ManageEngine
Powering IT ahead

EventLog Analyzer 7

Standalone/Managed Server - User Guide

www.eventloganalyzer.com

eventlog-support@manageengine.com

Table Of Contents

Introduction

Event log management is an important need in almost all enterprises. Logs need to be archived for the purpose of network auditing and more recently, to comply with various regulations such as HIPAA, GLBA, SOX, and PCI. It helps organizations meet host-based security information event management (SIEM) objectives. Apart from this, system administrators look at event logs as a critical source for troubleshooting performance problems on hosts and the network. Efficient event log analysis reduces system downtime, increases network performance, and helps tighten security policies in the enterprise.

What is EventLog Analyzer?

ManageEngine EventLog Analyzer is a web-based, real-time, event monitoring and management solution that improves security and reduces downtime of distributed servers and workstations on your enterprise network. It collects event logs from distributed Windows host and, syslogs from UNIX hosts, Routers & Switches, and other syslog devices using an agent-less architecture and generates graphs and reports that help in analyzing system problems with least impact on network performance.

This User Guide will help you install EventLog Analyzer on your machine, and get 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 eventloganalyzer-support@manageengine.com

About EventLog Analyzer

EventLog Analyzer collects, normalizes, and aggregates security, systems, directory service, dns server and application log data from enterprise-wide Windows, Linux, and UNIX hosts, and syslogs from Routers, Switches, and any other syslog devices.

The following are some of the key features of this release.

Feature	Description
Centralized event log management	Application, system, and security event data is collected from enterprise-wide and distributed Windows, UNIX, and Linux systems, and syslogs from Cisco Routers & Switches are stored in a central database (MySQL database bundled with the product).
Compliance reporting	Generate pre-defined compliance reports to meet HIPAA, GLBA, SOX, and PCI requirements.
Automatic alerting	Define alerts based on event, event category, event type, event ID, log message contents, host, or host groups.
Historical trending	View trends of system events on a particular host or host group. This is especially useful during performance analysis.
Security analysis	identify unauthorized and failed logins, and errant users. Such analysis helps to reduce the reaction time to unforeseen events.
Host grouping	group hosts based on business needs, and generate exclusive event reports and trend reports.
Pre-defined event reports	instantly generate reports on top events, top hosts, etc. across hosts, host groups, users, and even processes.
Customizable report profiles	build custom report profiles with specific event filters and report format options.
Report scheduling	automatically generate reports at specified time intervals and get them delivered via email.
Multiple report formats	generate and export reports in HTML, PDF, and CSV formats.

Release Notes

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

- 7.0.0 - Build 7000 (GA)

7.0.0 - Build 7000 - Standalone Edition

The general features available in this release include all the features of EventLog Analyzer Version 7.0.0 Build 7000 and

Features:

- Remote Agent - Optional agent for log collection across WAN/Firewalls
- Third party user authentication - RADIUS server authentication
- New reports for IBM AIX server - Logon and Logoff reports for SU, SSH and SFTP
- CSV report formatting issue fixed and further enhanced
- Support for MS SQL Cluster as back end database
- Provision to configure WMI Auth level
- Provision to control automatic syslog collection
- Provision to configure SMS modem connectivity baud rate

Bug Fixes:

- Fixed the migration issue occurred for MS SQL Cluster as back end database
- Fixed the issue in direct export option of trend reports
- Issue in compliance - summary/details report fixed
- Fixed the issue - Duplicate job creation on every scan in AS400
- Throwing exception while editing Host Details page - the issue has been fixed
- Fixed vulnerability - Apache Tomcat Single-Sign-On HTTP Cookie Exposure Vulnerability (CVE-2008-0128)
- Fixed the issue of non-listing of Windows Vista Event IDs in Predefined Alerts for Windows
- Fixed the issue in Active Directory user import (for AD authentication) in Windows Vista and Windows 2008 environment.
- Fixed the issue of listing all the Host Groups for the Operator user instead of listing Host Groups only assigned to the user in the Add New Hosts page
- Fixed the issue of displaying the count in decimal value in the PDF reports
- Fixed the issue of displaying the records for the Host Group even if a single host is selected, when drilled down to a particular event from a scheduled Top N Reports (Top Users by Login)
- Fixed the issue garbled Throw away report when MS SQL database is used
- Eventlog Analyzer Service not started at reboot in Windows 2008 server - this issue is fixed
- Fixed the issue of displaying wrong error message during MS SQL migration, when 64 bit bcp runs in 32 bit machine
- Fixed the following issue: 'No Data Available' error message is displayed, when

clicked on the event count for the name of the process containing special characters (e.g., COM+), in the **All Events** tab

- Issue in migration fixed, when MySQL database installed in a remote server was used.

Known Issues:

- The inbuilt MySQL database of EventLog Analyzer could get corrupted if other processes are accessing these directories. Kindly exclude the EventLog Analyzer installation directory 'ManageEngine' (it could be in *C:\ManageEngine* or *D:\ManageEngine*) from both the Backup process and Anti-Virus Scans.
- UAC need to be disabled for Remote Agents installation in an Windows Vista based machine
- 64 bit installations need to use in built batch file for troubleshooting syslog packets instead of UI based syslog viewer tool
- For converted Managed Server (in case of an Distributed installation) already processed application based logs will not be migrated. New logs will be automatically taken care
- Remote Agent will not support specific reporting of Oracle logs.

Installation and Setup

System Requirements

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

- Hardware Requirements
- MySql Performance Improvement Parameters
- Operating System Requirements
- Supported Platforms & Devices
- Supported Web Browsers

Hardware Requirements

For 32 Bit Installation

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

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

For 64 Bit Installation

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.

**The following table recommends the disk space and RAM size requirements of the system where EventLog Analyzer is installed. The disk space and RAM size requirements depends on the number of host sending log information to EventLog Analyzer, the number of host log records received per second or the host 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..*

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

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

Hardware RAM Size	MySQL Parameter Changes
1 GB	*Default configuration as given in startDB.bat/sh*
2 GB	*" --innodb_buffer_pool_size=**1200M** "*
3 GB	*" --innodb_buffer_pool_size=**1500M** "*
4 GB	*" --innodb_buffer_pool_size=**1500M** "*

Operating System Requirements

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

1. Windows™ 2000, XP, Vista, 7, 2000 Server, 2003 Server, 2008 Server & 2008 R2
2. Linux - RedHat 8.0/9.0, Mandrake/Mandriva, SuSE, Fedora, CentOS
3. Ability to run in VMware environment

Note: Note: If EventLog Analyzer is installed in SuSE Linux, then ensure that in the **mysql-ds.xml** file, present under *<EventLogAnalyzer_Home>/server/default/deploy* you replace *localhost* mentioned in the following line : *<connection-url>jdbc:mysql://localhost:33335/eventlog</connection-url>* with the corresponding IP Address or DNS resolvable name of the current system where EventLog Analyzer is installed.

Supported Platforms & Devices

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

1. Windows™ NT/2000/XP/Vista and 2000/2003/2008 Server
2. Linux - RedHat, Debian
3. UNIX - Solaris, HP-UX
4. IBM AS/400 - Variants V5R1, V5R2, V5R3, V5R4, V5R5 and V6R1
5. Cisco Switches and Routers
6. VMWare - Syslog of versions
7. DHCP - Windows and Linux
8. SNARE for Windows

The logs of the following applications can be processed:

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

- For analyzing logs from Windows NT machine, WMI core should have been installed in the Windows NT machine.
- Syslogs received from SNARE agents for Windows will be displayed as Windows hosts.

Supported Web Browsers

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

1. Internet Explorer 5.5 and later
2. Netscape 7.0 and later
3. Mozilla 1.5 and later
4. Firefox 1.0 and later

Prerequisites

Before setting up EventLog Analyzer in your enterprise, ensure that the following are taken care of.

In the non-NATed firewall setup, ensure DCOM is enabled on the host machine to be monitored. (DCOMCNFG > Default Properties > Enable Distributed COM).

In the NATed firewall, forward the logs in the syslog format using the third party utility like SNARE.

Ports to be freed

EventLog Analyzer requires the following ports to be free:

Port Number	Usage
8400	This is the default web server port. You will connect to the EventLog Analyzer from a web browser using this port number. You may change this port during installation
513, 514	These are the default listener ports. It is recommended that you configure hosts to send event logs to any one of these ports.
33335	This is the port used to connect to the MySQL database in EventLog Analyzer.

EventLog Analyzer will be using the following ports:

Port Number	Usage
135, 445, 139	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 (Non-SysLog mode).
1024-65534	Outgoing Traffic Ports - DCOM will use callback mechanism and uses random ports (1024-65534) and hence open the ports above >1024

EventLog Analyzer will be using the following ports:

Port Number	Usage
5000, 5001	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 to opened in the Firewall

For IBM AS/400

Port Number	Usage
446-449, 8470-8476, 9470-9476	Keep the mentioned ports opened to access IBM AS/400 machines.

	Look up Changing Default Ports for help on changing the default ports used by EventLog Analyzer

Recommended System Setup

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

- Run EventLog Analyzer on a separate, dedicated PC or server. The software is resource-intensive, and a busy processor may cause problems in collecting event logs.
- Use the MySQL pre-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 replace the existing MySQL parameters.

Changing Default Ports

Changing the default MySQL port:

1. Edit the **mysql-ds.xml** file present in the *<EventLogAnalyzer_Home>/server/default/deploy* directory.
2. Change the port number in the following line to the desired port number:
   `<connection-url>jdbc:mysql://localhost:33335/eventlog</connection-url>`
3. Save the file and restart the server.

Changing the default web server port:

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

Installing and Uninstalling

EventLog Analyzer is available for Windows and Linux platforms. It is available both in 32 Bit version and 64 Bit version.

Installation Procedure for various OS and CPU versions:

- Windows 64 Bit version
- Windows 32 Bit version
- Linux 64 Bit version
- Linux 32 Bit version

For more information on supported versions and other specifications, look up System Requirements.

Installing EventLog Analyzer

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.

Windows 64 Bit version:

The EventLog Analyzer Windows 64 Bit version download is available as an EXE file at http://www.eventloganalyzer.com/download.html

Windows 32 Bit version:

The EventLog Analyzer Windows 32 Bit version download is available as an EXE file at http://www.eventloganalyzer.com/download.html

Rest of the installation procedure remains same for both 64 Bit and 32 Bit versions.

Double-click the downloaded EXE file, and follow the instructions as they appear on screen. Once the installation is complete you will notice a tray icon, which provides you with the following options.

Option	Description
EventLog Server Status	This option provides you details like *Server Name*, *Server IpAddress* , *Server Port*, *Server Status*.
Start WebClient	This option will open up your default browser and connect you to the web login UI of EventLog Analyzer Server, provided the server has already been started
Shutdown Server	This option will shutdown the EventLog Analyzer Server.

The tray icon option is only available for Windows !

Linux 64 Bit version:

The EventLog Analyzer Linux 64 Bit version download is available as a BIN file at

http://www.eventloganalyzer.com/download.html

Linux 32 Bit version:

The EventLog Analyzer Linux 32 Bit version download is available as a BIN file at

http://www.eventloganalyzer.com/download.html

Rest of the installation procedure remains same for both 64 Bit and 32 Bit versions.

1. Download the BIN file, and assign **execute** permission using the command:
   chmod a+x <*file_name*>.bin
   where <*file_name*> is the name of the downloaded BIN file.
2. Execute the following command: ./<*file_name*>Bin

	During 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*>

Follow the instructions as they appear on the screen.

This will install EventLog Analyzer on the respective machine.

Uninstalling EventLog Analyzer

Uninstallation procedure remains same for both 64 Bit and 32 Bit versions.

Windows:

1. Navigate to the Program folder in which EventLog Analyzer has been installed. By default, this is **Start > Programs > ManageEngine EventLog Analyzer 6**.
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.

	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.

Starting and Shutting Down

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

Starting EventLog Analyzer

Windows Application:

Click on **Start > Programs > ManageEngine EventLog Analyzer 6 > 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 application as Windows Service, carry out the procedure to convert the application installation as Windows Service. After this, carryout the following procedure to start Windows Service.

- Go to the Windows **Control Panel**. Select **Administrative Tools > Services**.
- Right-click **ManageEngine EventLog Analyzer 6** and select **Start** in the menu.
- Alternatively, select **Properties**. The **<Service> Properties** screen opens up.
- In the **General** tab of the screen, check the **Service status** is "*Stopped*" and **Start** button is in enabled state and other buttons besides are grayed.
- 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 prompt window opens up showing startup information on several modules of EventLog Analyzer. Once all the modules have been successfully created, the following message is displayed:

```
Server started.

Please connect your client at http://localhost:8400
```

where `8400` is replaced by the port you have specified as the web server port during installation.

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 into the UI.

Linux Service:

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

/etc/init.d/eventloganalyzer start

Check the status of EventLog Analyzer service

/etc/init.d/eventloganalyzer status
ManageEngine EventLog Analyzer 6.0 is running (15935).

Shutting Down EventLog Analyzer

Follow the steps below to shut down the EventLog Analyzer server. Please 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:

1. Navigate to the Program folder in which EventLog Analyzer has been installed. By default, this is **Start > Programs > ManageEngine EventLog Analyzer 6**.
2. Select the option **Shut Down EventLog Analyzer**.
3. Alternatively, you can navigate to the <*EventLog Analyzer Home*>*bin* folder and invoke the **shutdown.bat** file.
4. You will be asked to confirm your choice, after which the EventLog Analyzer server is shut down.

Windows Service:

Ensure that the EventLog Analyzer application is installed as Windows Service. Carryout the following procedure to stop Windows Service.

- Go to the Windows **Control Panel**. Select **Administrative Tools > Services**.
- Right-click **ManageEngine EventLog Analyzer 6**, and select **Stop** in the menu.
- Alternatively, select **Properties**. The **<Service> Properties** screen opens up.
- In the **General** tab of the screen, check the **Service status** is "*Started*" and **Stop** button is in enabled state and other buttons besides are grayed.
- Click **Stop** button to stop the windows service.

Linux Application:

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

Linux Service:

/etc/init.d/eventloganalyzer stop
Stopping ManageEngine EventLog Analyzer 6.0...
Stopped ManageEngine EventLog Analyzer 6.0.

Check the status of the service again

/etc/init.d/eventloganalyzer status
ManageEngine EventLog Analyzer 6.0 is not running.

Accessing the Web Client

EventLog Analyzer is essentially an event log management tool that collects, stores, and reports on event logs from distributed servers and workstations on the network.

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

1. Open a supported web browser window
2. Type the URL address as ***http://<hostname>:8400*** (where <*hostname*> is the name of the machine on which EventLog Analyzer is running, and *8400* is the default web server port)
3. Log in to EventLog Analyzer using the default username/password combination of **admin/admin**.

EventLog Analyzer provides two more external authentication apart from the local authentication. They are **Active Directory** authentication and **Remote Authentication Dial-in User Service (RADIUS)** authentication. If you import users from Active Directory or if you add a RADIUS server details, you will find the **Options >>** link besides the **Login** button in the EventLog Analyzer Client UI Login screen. If you click the **Options >>** link, **Log on to** field will appear below the **Password** field. 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 avilable 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

Enter the **User Name** and **Password**. Select one of the three options in **Log on to** (**Local Authentication** or **Radius Authentication** or **Domain Name**). Click **Login** button to log in to EventLog Analyzer Client UI.

Once you log in, you can start collecting event logs, generate event reports, and more.

If you want to access the web client from the same machine on which EventLog Analyzer is installed, execute the **startClient.bat/.sh** file from the <*EventLog Analyzer Home*>/*bin* directory.

- On a Windows machine, you can also access the web client from the Start menu by clicking on **Start > Programs > ManageEngine EventLog Analyzer 7 > EventLog Analyzer Web Client**.
- On a Windows machine, you can also access the web client from the System Tray by right-clicking on **EventLog Analyzer Tray Icon > Start Web Client**.

License Information

After you log in to EventLog Analyzer, click the **Upgrade License** link present in the top-right corner of the screen. The License window that opens up, shows you 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

Upgrading your License

Before upgrading the current license, make sure you have the new license file from ZOHO Corp. saved on that system.

1. Browse for the new license file, and select it.
2. Click **Upgrade** to apply the new license file.

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

Getting Started

Once EventLog Analyzer has been successfully set up and started in your network, the next thing to do is to start collecting event logs from hosts on the network.

As soon as you log in, you will see the Dashboard. If no hosts are sending event logs to EventLog Analyzer, you will see a welcome screen with options to help you get started.

The options in the welcome screen will help you do the following tasks:

- Add a Windows/Unix-host/Any syslog device or Cisco device to collect event logs or syslogs.
- Simulate event logs

	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. To convert the message you have to use separate third party tool. Please mail us to eventlog-support@manageengine.com for the steps, if required.

Adding Hosts

In order to collect event logs from various hosts in the network, you need to add them to the list of hosts that EventLog Analyzer is currently collecting event logs from. The list of hosts currently monitored is shown in the Hosts table on the Dashboard view of the **Home** tab. You can add a new host by clicking the **New Host** link from the Dashboard, the sub tab, or the **Settings** tab.

	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.

	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.

Default listener ports of EventLog Analyzer are **513 & 514**. UNIX hosts already configured to send data to the EventLog Analyzer on either of these ports will be automatically added to the list of hosts.

- Adding Windows Host
- Adding Unix Host
- Adding IBM AS/400 Host
- Adding VMware Host
- 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

Adding Windows Host

1. From the Add New Host page, choose **Windows** 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. Click the **Pick Hosts** link to select hosts auto-discovered from domains scanned on the network.
    1. Select the **Login as Domain User** checkbox if you want to use the login credentials of the Domain Administrator.
    2. If you cannot find a specific host in the domain, click **Rescan the Domain** to rescan this domain alone
    3. If you cannot find a specific domain, click **Rescan the complete network** to rescan the entire network
3. Select the Host Group to which the hosts need to be added. Click the icon to create a new host group.

	You need to be logged in with Administrator rights to see the **Pick Hosts** option.

4. Enter the domain name of the host in the **Domain Name** field. However, the field is optional.

5. Enter the administrator **Login Name** and **Password** for the selected host. Click on **Verify Login** to ensure that the correct credentials are provided and you are able to authenticate to the host machine.

6. Select the **Monitoring Interval**. This is the time interval after which event logs will be collected from the host

7. Select the **Use Agent To Collect Logs** check box, if you want to use the agent in the network to collect the logs from the particular host. When the option is selected, the drop down list of available agents in the network becomes active. Choose the appropriate agent.

8. 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.

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.

Adding UNIX Host

1. From the Add New Host page, choose **Unix** 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. If you would like EventLog Analyzer to listen to a different **Syslog Listener Port**, other than the mentioned **514** port,then you need to enter the port number where the syslog or syslog-ng service is running on that particular (Cisco Device or UNIX or HP-UX or Solaris or IBM AIX) host.

While adding multiple hosts, the Syslog Listener Port number that you enter, is assumed as the port number of the syslog service for **all the hosts**.

5. 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 above steps for adding a UNIX host is also applicable for adding Cisco Device (switches and routers) or any other Syslog Device provided you select the **Host Type** as **Cisco Device** or **Syslog Device** or Custom Host Type. Before adding a Cisco Device or UNIX or HP-UX or Solaris host, you need to configure the syslog service on the Cisco Device or UNIX or HP-UX or Solaris host to send syslogs to EventLog Analyzer.

The Host Details page provides details regarding the added hosts.

Adding IBM AS/400 Host

1. From the Add New Host page, choose **IBM AS/400** as the **Host Type**.

	Keep the ports 446-449,8470-8476,9470-9476 opened to access IBM AS/400 machines.

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. Select the monitoring interval. This is the time interval after which event logs will be collected from the host.
6. Select the **Date Format** and the **Delimiter Date Format in the log**. This is the date format used in the event logs will be collected from the IBM AS/400 hosts.
7. 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 able to login to fetch History logs.

The Host Details page provides details regarding the added hosts.

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>;

	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 IBM AIX) **startsrc -s syslogd**

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.

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 by syslog. Changes to *Syslog.Remote.Port* only take effect if *Syslog.Remote.Hostname* is configured.

8. Click **OK**.

Adding Cisco Devices

The following configuration needs to be done in Cisco Devices (Switches and Routers), before adding them in EventLog Analyzer, for them to send syslogs to EventLog Analyzer and generate reports.

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
```

	**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 eventloganalyzer-support@manageengine.com if the syslog format of your cisco devices are different from the standard syslog format supported by EventLog Analyzer.

Analyzing Application Logs

EventLog Analyzer analyzes **Application Logs** and generates reports. The following applications logs can be analyzed. The applications logs are:

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

Applications logs in ASCII text format are only handled.

Importing Logs

Only imported logs are processed. However, EventLog Analyzer can be scheduled to import logs periodically from the application hosts. The logs are not received from application hosts in real time. In the case of Event logs and Syslogs, the logs are received in real time.

For to collecting Oracle logs, follow the configuration procedure given in the ELA Configuration page.

Processing Logs

When the log files are imported periodically, the processing of logs is carried out progressively. That is, only the new log entries added after the previous processing of the log file will be processed. Also the EventLog Analyzer will be able to handle Dynamic Filename change of application log files. That is, some of the applications may append the time stamp with the log file name daily and in turn changes the log file name.

Associating Logs to Host

The imported log files can be associated to one of the hosts listed. If the log file is not associated with a host, EventLog Analyzer associates the log file to dummy host.
The filtering, alerting, and archieving features are not available for Application logs.

Simulating Event Logs

The **Simulate** option lets you test EventLog Analyzer with sample event log data before setting it up for real-time analysis on your network. The sample data is taken from the **syslog_records.xml** file present in the *<EventLogAnalyzer_Home>/server/default/conf* directory on the server.

If EventLog Analyzer is running on a Windows machine, add the same machine as a Windows host before trying to simulate event logs. Otherwise you cannot view any reports for the simulated data.

When you click the **Simulate** link from the welcome screen or the **Settings** tab, the EventLog Analyzer server starts receiving the sample data as event logs. The server then analyzes this data and generates reports assuming this data to be actual event logs. As a result, you can view all the pre-defined event reports, create custom reports, and set up notifications just like you would when actual data is received.

At any time, click the **Stop Simulate** link from the **Settings** tab to stop sending the sample event logs to the server. However, data already sent to the server will be present until the database is reinitialized.

User Interface

Using the Dashboard

The Dashboard is shown when the **Home** tab is clicked. This is the one place from which important information about events and hosts can be seen.

Use the global calendar to set the time period for which the graph and table values are generated.

The **Total Events Per Host Group** graph shows the number of events generated in each host group. This includes standard, as well as custom created host groups. Color codes are used to differentiate between event severity's in each host group.

The **Total Events Per Event Type** graph shows the total number of events generated in the selected time period, grouped according to event category or type - Application, System, Directory Service, DNS Server, File Replication Service, Security, and any other custom event type. Color codes are used to differentiate between event severity's in each event category.

You can drill down from the above graphs to see more information about the hosts that generated the corresponding events, and the event message that was received. You can export this report to PDF and CSV formats. Click **Export to: PDF** icon or **CSV** icon on the right top corner of the report page.

The table below the graphs shows two tabs: Hosts and Applications. The first tab **Hosts** lists all the hosts that have been configured to send event/system logs to EventLog Analyzer, and the next tab **Applications** lists all application logs imported by the EventLog Analyzer.

Click the icon or the **Hosts** link to view the list of all hosts from which event logs are collected. Click the icon or the **Add New Host** link to add a new host.

The fields and icons present in the **Hosts** table are described below:

Field / Icon	Description
or or or or or or	This icon tells you whether this host is Linux/ Windows/ Cisco Routers / Switches/IBM AS/400.
	Click this icon to edit attributes for this host
or	Click this icon to enable or disable collecting event logs from this host
Host Name	The host name of the machine from which event logs are collected
Host Group	The host group to which this host belongs
	Click this icon to delete the host
Status	The status of log collection from this host. Hover over each icon to see the current status.
Error/ Warning/ Failure/ Others/ Total	The number of events generated with each severity. Click on the event count to see more information about the events generated with this severity.
	Click this icon to see the last ten events generated by this host

Field / Icon	Description
	Click this icon to search a host or a set of hosts.
	Click this icon to create and schedule Host Summary Report.

The status of log collection can be:

Status	Description
	event log collection started
	access is denied for event log collection or log does not exist
	event log collection is yet to start

The fields and icons present in the **Applications** table are described below:

Field / Icon	Description
Application Type	The application to which the imported log belongs to.
Error	The number of events generated with Error severity. Click on the event count to see information about the events generated with this severity. Clicking the count displays the time stamp and actual text message of the events.
Warning	The number of events generated with Warning severity.
Failure	The number of events generated with Failure severity.
Others	The number of events generated with severity other than the above three.
Total	The total number of events generated including all the severity.

In the **Applications** tab, the entries are based on Application type and not based on application hosts. Click on the Application type link in the individual entry. The <**Application Logs**> screen opens up. This screen displays the overview of log details and application hosts view drilled down to one level. This screen also displays the reports related to this application logs combined for all the hosts. Further you can drill down to one more level by clicking on the application host. The <**Application >> Application Host Logs**> screen opens up. This screen displays the log details of application hosts specific to the application. This screen also displays the reports related to this application logs specific to the selected host.

	The application logs should be associated to hosts while configuring import of logs. Otherwise the logs will be associated to dummy host.

Using The Sub Tab

The sub tab provides links to frequently accessed reports and tasks in EventLog Analyzer.

Show Listen Port Details

Click the icon to see the host name, IP address, listening ports, and server status details for the EventLog Analyzer server.

Syslog Viewer

You can view the Syslogs (Raw packets) in real time. Click the syslog viewer icon to view the details of the syslog packets like *source*, *destination*, syslog *port*, and the raw log *message* received by the EventLog Analyzer server from the various configured hosts.

If you would like to troubleshoot whether the syslog packets are being sent by the host (*source*) to the EventLog Analyzer (*destination*) at the configured port, you can mention the Host IP Address (by default it is *Any*) and syslog port of this hosts (by default it *513,514*) and click on **Apply Filter**. With the filter applied, you can find out whether the raw log packets are sent from the specific host to EventLog Analyzer server in real time.

The following tasks can be done by clicking the corresponding links in the sub tab:

Link	Action
New Host	A dd a new host from which event logs will be collected
New Alert Profile	Create a new alert profile to trigger alerts and send notifications
New Report	Create a new custom report
New Filter	Create new database filter, to filter out the unwanted events from your hosts, getting stored in the database
Import Logs	Click this link to import Windows Event Log files (type *.evt* format) (type *.evtx* format supported in **Windows Vista** and **2008** machines only) from the local machine or by FTP from remote machine.
AS/400 Alert/Filter/Report	Click **AS/400 > Alert** to create a new alert profile to trigger alerts and send notifications for AS/400 devices. Click **AS/400 > Filter** to create new database filter, to filter out the unwanted events from AS/400 hosts, getting stored in the database. Click **AS/400 > Report** to create a new AS/400 custom report. At least one AS/400 host should be added to EVentLog Analyzer, for this menu item in the sub-tab to be visible.

Bookmarks	Allows you to set a bookmark for the current page, and manage existing bookmarks

Advanced Search	Click this link to carry out Advanced Search of Formated logs and Raw logs. Use the result to create Report Profile. This will be useful for network trouble shooting and forensic analysis.

Using The Left Navigation Pane

The left navigation pane provides quick links to different tasks and reports in EventLog Analyzer. The components present in the left navigation pane depend on the tab that is currently selected.

The following is a list of all components found in the left navigation pane:

Component	Description
Dashboard Views	List all the custom dashboard views created by the user. 'All Groups' view is the default dashboard view.
Global Calendar	Allows you to select the time period for all reports from one place. By default, the current day's data is shown.

Component	Description
My Reports	Includes links to generate custom reports created using the **Add New Report** link.
Top N Reports	Includes links to generate event-based reports on top hosts, top processes, and more.
User Activity Reports	Includes links to generate reports for HIPAA, GLBA, SOX, and PCI compliance requirements.
Compliance Reports	Includes links to generate reports for HIPAA, GLBA, SOX, and PCI compliance requirements.
Trend Reports	Includes links to generate trend reports based on event logs received from hosts.

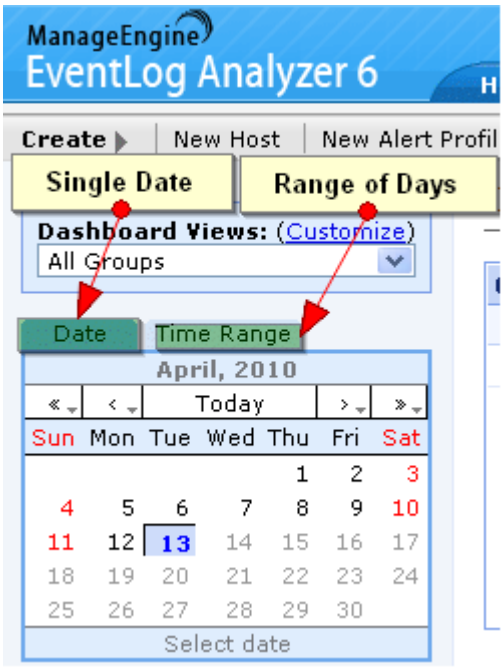
Most of the tasks in the left navigation pane can be done from the main tabs also, by clicking the corresponding links. The left navigation pane provides a quicker way to perform the same tasks.

Component	Description
Applications	Includes links to generate application-based reports on top hosts, top users, top file types, top Page URLs, and more. It also includes link to **Import Log File**.

Using Calendar

You can use the calendar to select a single date or range of days to view various details of the reports, alerts, and logs of the Firewalls.

There are two icons provided on top left corner of the calendar to select a single day or range of days. Refer the screen shot given below:



Dashboard View Customization

In the **Dashboard Views** section, you can see **Customize** link besides "*Dashboard Views:*" title to customize the dashboard view and a combo box listing all the available Dashboard Views with **All Groups** view on top.

To customize the dashboard view, click **Customize** link. **Dashboard View Customization** page appears. It lists all the dashboard views available to the user including **All Groups** view on top.

The dashboard view customization page lets users to:

- Create multiple dashboard views based on the groups assigned to the user. Each view can be configured to show a list of assigned groups. The created dashboard views are listed in the Dashboard Views combo box in the left hand side top of the Home tab.
- Edit any of the listed views, except the **All Groups** dashboard view.
- Set any one of the views as default dashboard view.
- Delete any of the listed views, except the **All Groups** view and the default dashboard view, if any of the created dashboard view is set as a default dashboard view.

To create a new group view

Click **Create Group View** link. The **Create Group View** screen pops-up. In that screen,

- Enter a name for the view in the **View Name** text box.
- Select the devices from the **Available Groups** list, and move it to the **Dashboard View Groups** list.
- Select the **Set this view as Default View** check box option to make this view as the default dashboard view upon user login.
- Click **Update** to create the device view and **Close** to close the screen.

Now you can see the new view created is listed in the **Dashboard View Customization** page.

To edit a device view

To edit a view, click the icon of the view to be edited. The **Edit Group View** screen pops-up. The procedure is same as that of create device view.

To set a device view as default view

Select any one of the listed views to be **Set as default**. The default dashboard view is indicated by the icon and all other views by the icon.

Click the icon of the view, which you want to set as default view. Now the icon changes to icon and in the previous default view, the icon changes to icon.

To delete a device view

To delete a view, click the icon of the view to be deleted.

	**Default View**: The default dashboard view is the one which appears in the **Home** tab, upon user login. By default **All Groups** view is set as default view. User can create and set any view as default view. Default view will appear automatically only when the user closes the client and re-logs in. User can view any of the listed dashboard views and traversing between the tabs will not change the view.

Generating Event Reports

EventLog Analyzer offers a rich set of pre-defined reports that help in analyzing event logs and understanding system behavior without spending a lot of time. On a broad level, EventLog Analyzer provides the following types of reports:

Report	Description
Top N Reports	view top hosts and top processes generating events of different severity
User Activity (PUMA) Reports	view overview of user activity and user wise reports of their activities
Trend Reports	view event trends based on event severity or event category, and alert trends
Compliance Reports	view instant reports for HIPAA, GLBA, SOX, and PCI requirements
Detailed Host Reports	view host-specific event summary for each host
Custom Reports (My Reports)	create custom reports based on specific reporting criteria
Application Reports	view pre-defined reports for three types of applications, namely, IIS W3C Web Server Logs, IIS W3C FTP Logs, and MSSQL Server Logs
IBM AS/400 Reports	view pre-defined reports for IBM AS/400 device

Generate Test Report

If you want to see a preview of report for the newly created rep rot profile, at the end of the Report Profile Creation wizard, click the **Generate Test Report** button.

All the above reports can be accessed from the **Reports** tab.

Customizing and Scheduling the EventLog Analyzer Reports

All the reports of EventLog Analyzer can be customized and scheduled as per your requirement. The pre-defined reports like Top N Reports, Trend Reports, and Compliance Reports can be customized to suit your requirements. Selectively filtered reports can be created from the pre-defined reports of the EventLog Analyzer. The default reports also will be available.

Procedure to customize and schedule pre-defined reports

On any of the pre-defined reports like Top N Reports, Trend Reports, and Compliance Reports, you will find the icon.

- Click on the icon, Create New Report wizard screen opens up.
- Create the new report as explained below. But, in this case you will be customizing the existing predefined report from which you clicked the icon.

Step 1:

In the **Create New Report** wizard first page, enter report details and select host.

1. Enter a unique name as the **Report Name**, for the new customized report.
2. Select the hosts or host groups to report on.
3. Click **Next** to continue.

Step 2:

In the **Create New Report** wizard final page, select the report generation schedule, configure to send the report by Email and generate test report.

1. If you want to schedule this report to run automatically, choose the time interval after which this report should be generated. Choose from hourly, daily, weekly, or monthly schedules, or choose to run this report only once. For Daily, Weekly, and Only once schedules, you can set the **TimeFilter** for **Custom** Hours, **Only Working Hours**, or **Only NonWorking Hours**.

   For the **Daily** schedules, if the option **Run on Week Days** is selected then the reports are run daily except on the weekends. For the **Weekly** or **Monthly** schedules, select the option **Generate Report only for Week Days** if you want to report on the events that occurred only on the week days and not report on events that occurred over the weekends.

	You can also add a schedule to this report later from the **My Reports** section

2. You can select the report format. Select the **Report Format**, **PDF** or **CSV** radio buttons.
3. You can select the summary or detailed report to be generated. Select the **Generate Report**, **Summary & Details** or **Only Summary** radio buttons.
4. If you want to email this report select the **Email This Report** checkbox

   - Enter the e-mail addresses as comma-separated values in the **Mail To** box
   - If the mail server has not been set up yet, an error message is shown below the **Mail To** box. Click the link inside the error message to configure the mail server settings in the popup window that is opened.

5. Click **Generate Test Report** to see a preview of how this report will look like, once it is set up. Click **Finish** to save the report. The report is now listed in the **My Reports** section.

Scheduled reports are generated and emailed in PDF or CSV formats.

Viewing Events for a Host

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.

	For Cisco devices, EventLog Analyzer supports reports for Important Events like: AccessList Hits, Configuration Changes, ISDN Disconnects, Link State Changes, and System Restarts.

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.

	Look up Database Filters to know more about setting up filters to store only specific events from a host or host group.

Viewing Top Hosts

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

This report shows the hosts with maximum number of successful logins, and the 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.

Using this report, you can decide if security policies need to be changed with respect to certain hosts, and even tighten security measures across the network.

Top Users by Login

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.

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

Top Interactive Login

In this case, 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.

Using this report, you can 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. This means that, at one glance, you can see which hosts have been generating maximum 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**.

Using this report, you can quickly see hosts that may be experiencing problems, thereby accelerating the troubleshooting process.

	Some event severities are applicable to Unix hosts only

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. This means that, at one glance, you can see which processes have been generating maximum 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**.

Using this report, you can investigate suspicious behavior on 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.

Viewing User Acitivity (PUMA) Reports

Under the User Activity Reports you have the following reports:

- **User Activity Overview**
- **Used Based Reports**

You can save these reports using **Save as: > Scheduled Report** link available right top corner of the reports.

User Activity Overview

This report lets you know the overall host wise user activity.

You can change the hosts using **Filter Criteria**.

Select **Filter Criteria: > Change 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.

The list of 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

Used Based Reports

This report lets you know the number of events of user wise activity.

You can change the hosts, users and reports using **Filter Criteria**.

Select **Filter Criteria: > Change Hosts** to view the overview graph of a selected hosts.
Select **Filter Criteria: > Change Users** to view the overview graph of a selected users.
Select **Filter Criteria: > Change Reports** to view the overview graph of a selected reports.

The report wise number of events (**Report vs Event Count**) are plotted in the graph.

The list of 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

Generating Compliance Reports

EventLog Analyzer lets you generate the following pre-defined reports to help meet the requirements of PCI-DSS, FISMA, HIPAA, GLBA, and SOX regulatory compliance acts:

- PCI Compliance
- FISMA compliance report
- HIPAA compliance report
- SOX compliance report
- GLBA compliance report

Click the **Compliance Reports** link to see the different reports available for each act. These reports are available under the **Compliance Reports** section in the **Reports** tab and the left navigation pane.

Click the **Compliance Reports** link to view the details and descriptions of the default compliance and the selected list of reports, configure new or existing compliance. You can find this link on the **Reports** menu of the sub-tab. Clicking the **Compliance Reports** link opens the **Compliance Reports** page. On the right side top of the page, **+ New Compliance** link is present. With the **+ New Compliance** link, you can add a new compliance and select a set of reports for the compliance. With **Edit Compliance** link, you can edit the default compliance available in the EventLog Analyzer. The **Compliance Reports** page displays the default and custom compliance reports with description and the respective sections/controls of the act covered. Click the Compliance report of your choice.

The chosen Compliance Report page displays the overview of the Compliance in pi graph format, its description and the report details.

You can click on the graph to get one level drill down of number of events information of reports of the group. In the next level drill down click the number of events link of the reports in the group to get the exact raw logs

It provides **Change Report** instant menu option on top of overview itself, to change the Compliance or the specific report of interest to be displayed.

It provides **Change Host** instant menu option on top of overview itself, to change the Host Group or the specific host of interest to be displayed.

It provides **Schedule Report** instant menu option on top of overview itself, to schedule the displayed compliance report. You also have **Export to: PDF, CSV** icons to export the report currently being viewed to the selected format.

EventLog Analyzer Support for adding more reports to the existing list of default reports with **More Reports? Tell us here** link, all the reports selected for the compliance and their description. Clicking on the compliance report, displays all the selected reports of the compliance in the **<Compliance Name> Compliance Report** page. Clicking on the individual report under a compliance, displays the selected report of the compliance in the **<Compliance Name> Compliance Report** page.

PCI Compliance Reports

Requirement 10 of Payment Card Industry Data Security Standard (PCI-DSS) requires payment service providers and merchants to track and report on all access to their network resources and cardholder data through system activity logs.

EventLog Analyzer provides the following reports under various groups to help organizations to comply with the PCI regulations. The following reports cover Requirements 10.1, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.6, 10.2.7

- **Object Access**
  - Object Accessed
  - Object Created
  - Object Modified
  - Object Deleted
  - Object Handle
- **Logon**
  - Successful User Logons
  - Successful User Logoffs
  - Unsuccessful User Logons
  - Terminal Service Session
- **Policy Changes**
  - User Policy Changes
  - Domain Policy Changes
  - Audit Policy Changes
- **System Events**
  - System Logs
  - Audit Logs Cleared
- **User Access**
  - Individual User Action

All these reports are accessible from the PCI Compliance Reports section.

FISMA Compliance Reports

Federal Information Security Management Act (FISMA) mandates minimum security requirements for the federal government and related agencies. The requirements are covered in FIPS Publication 200, Minimum Security Requirements for Federal Information Systems in seventeen security-related areas. Federal agencies must meet the requirements as defined herein through the use of the security controls in accordance with NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, as amended. The following controls are covered in the reports:

- Audit and Accountability (AU)
- Certification, Accreditation, and Security Assessments (CA)
- Contingency Planning (CP)
- Access Control (AC)
- Identification and Authentication (IA)
- Configuration Management (CM)

EventLog Analyzer provides the following reports under various groups to help comply with the FISMA regulation controls:

- **Audit and Accountability (AU)**
  - Object Handle
  - Object Created
  - Object Modified
  - Object Deleted
  - Object Accessed

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

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

- **Access Control (AC)**
  - Terminal Service Session
  - Unsuccessful User Logons
  - Successful User Logoffs
  - Successful User Logons

- **Identification and Authentication (IA)**
  - Individual User Action

- **Configuration Management (CM)**
  - Anti-malwares
  - Other Software
  - Windows Software Updates

All these reports are accessible from the **FISMA Compliance Reports** section.

HIPAA Compliance Reports

The Health Insurance Portability And Accountability (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.

As part of the requirements, 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 . In other words being able to monitor, report and alert on attempted or successful access to systems and applications that contain sensitive patient information.

EventLog Analyzer provides the following reports under various groups to help comply with the HIPAA regulations:

- **Object Access**
  - Object Accessed
  - Object Created
  - Object Modified
  - Object Deleted
  - Object Handle

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

- **System Events**
  - System Logs
  - Audit Logs Cleared

- **Account Logon**
  - Successful User Account Validation
  - Unsuccessful User Account Validation

All these reports are accessible from the **HIPAA Compliance Reports** section.

Sarbanes-Oxley Compliance Reports

Section 404 of the Sarbanes-Oxley (SOX) act describes specific regulations required for publicly traded companies to document the management s Assessment of Internal Controls over security processes.

Although the exact requirements of Sarbanes-Oxley are a bit vague, as part of the requirements, it can be assumed 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. In other words, being able to monitor, report and alert on attempted or successful access to systems and applications that contain sensitive financial information.

EventLog Analyzer provides the following reports under various groups to help comply with the SOX regulations:

- **Object Access**
  - Object Accessed
  - Object Created
  - Object Modified
  - Object Deleted
  - Object Handle
- **Logon**
  - Successful User Logons
  - Successful User Logoffs
  - Unsuccessful User Logons
  - Terminal Service Session

- **Policy Changes**
  - User Policy Changes
  - Domain Policy Changes
  - Audit Policy Changes
- **System Events**
  - System Logs
  - Audit Logs Cleared
- **Process Tracking**
  - Process Access
- **Account Logon**
  - Successful User Account Validation
  - Unsuccessful User Account Validation
- **User Access**
  - Individual User Action
- **Account Management**
  - User Account Changes
  - Computer Account Changes
  - User Group Changes

All these reports are accessible from the **SOX Compliance Reports** section.

GLBA Compliance Reports

Section 501 of the GLBA documents specific regulations required for financial institutions to protect “non-public personal information”.

As part of the GLBA requirements, 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 provides the following reports under various groups to help comply with the GLBA regulations:

- **Logon**
  - Successful User Logons
  - Successful User Logoffs
  - Unsuccessful User Logons
  - Terminal Service Session
- **System Events**
  - System Logs
  - Audit Logs Cleared

All these reports are accessible from the **GLBA Compliance Reports** section.

Adding New Compliance

EventLog Analyzer lets you to create reports for any/new regulatory compliance act. This can be created either from **Compliance Reports** or **System Settings > Compliance Settings**.

Compliance Reports page

Click the **Compliance Reports** link in the left navigation pane or clicking the **Compliance Reports [View All]** link under the **Compliance Reports** section in the **Reports** tab, opens the **Compliance Reports** page. On the right side top of the page, **Add New** link is present. With the **Add New** link, you can add a new compliance and select a set of reports for the compliance.

Compliance Settings page

Click the **Compliance Reports** link to configure new or existing compliances. You can find this link on the **System Settings** section of the **Settings** tab. Clicking the **Compliance Reports** link opens the **Compliance Settings** page. On the right side top of the page, **Add new Compliance** link is present. With the link, you can add a new compliance and select a set of reports for the compliance.

Viewing Event Trends

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.

You can monitor trends of events generated across hosts, based on event severity, or event type. You can also view trends of alerts triggered. All the trend reports in EventLog Analyzer show the current trend, and compare this with the historical trend, with the time period split into one hour, and one day.

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

Event Severity Trend Reports

This type of trend report lets you see how events of different severities 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 type of 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.

Look up Setting up Notifications to know more about creating alert profiles

Generating Application Log Reports

The **Application Reports** provide different reports available for each application. These reports are available under the **Detailed Application Reports** section in the **Reports** tab and the left navigation pane.

The **Detailed Application Reports** section lists the **Log Type**, **Report Description** and **View Report** columns of the reports of the application logs.
The supported log types are:

- IIS W3C Web Server Logs
- IIS W3C FTP Logs
- DHCP Windows Logs
- DHCP Linux Logs
- MS SQL Server Logs
- Oracle Audit Logs

View Report column contains links to open the various reports of the selected application log.

Reports for IIS W3C Web Server Logs

Clicking the **View Report** link opens the **Reports for IIS W3C 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 lets you generate the following pre-defined reports for web server application logs:

- Hosts Report
- Users Report
- File Type Report
- Page URLs Report
- Browser Usage Report
- OS Usage Report
- HTTP Error Status Code Report
- Malicious URL Report

Hosts Report

EventLog Analyzer provides the following details for hosts report:

- Client IP Address
- Hits
- Page Views
- Bytes Sent
- Events

Users Report

EventLog Analyzer provides the following details for users report:

- Username
- Hits
- Page Views
- Bytes Sent
- Events

File Type Report

EventLog Analyzer provides the following details for file type report:

- File Type
- Hits
- Percentage
- Bytes Sent
- Events

Page URLs Report

EventLog Analyzer provides the following details for page URLs report:

- URI Stem
- Hits
- Page Views
- Bytes Sent
- Events

Browser Usage Report

EventLog Analyzer provides the following details for browser usage report:

- Browser
- Hits
- Percentage
- Events

OS Usage Report

EventLog Analyzer provides the following details for OS usage report:

- OS
- Hits
- Percentage
- Events

HTTP Error Status Codes Report

EventLog Analyzer provides the following details for browser usage report:

- HTTP Status
- Hits
- Percentage
- Events

Malicious URL Report

EventLog Analyzer provides the following details for malicious URL report:

- URI Stem
- Hits
- Percentage
- Events

Reports for IIS W3C FTP Logs

Clicking the **View Report** link opens the **IIS W3C FTP 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 lets you generate the following pre-defined reports for FTP server application logs:

- Hosts Report
- Users Report
- File Type Report
- Server Services Report

- Server IPs Report
- Source Port Report

Hosts Report

EventLog Analyzer provides the following details for FTP server application hosts report:

- Client IP Address
- Bytes Sent
- Bytes Received
- Events

Users Report

EventLog Analyzer provides the following details for FTP server application users report:

- Username
- Bytes Sent
- Bytes Received
- Events

File Type Report

EventLog Analyzer provides the following details for FTP server application file type report:

- File Type
- File Transfers
- Bytes Sent
- Bytes Received
- Events

Server Services Report

EventLog Analyzer provides the following details for FTP server application server services report:

- Server Service
- File Transfers
- Bytes Sent
- Bytes Received
- Events

Server IPs Report

EventLog Analyzer provides the following details for FTP server application server IPs report:

- Server IP Address

- File Transfers
- Bytes Sent
- Bytes Received
- Events

Source Ports Report

EventLog Analyzer provides the following details for FTP server application server ports report:

- Server Port
- File Transfers
- Bytes Sent
- Bytes Received
- Events

Reports for DHCP Windows Logs

Clicking the **View Report** link opens the **Reports for DHCP Windows 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 lets you generate the following pre-defined reports for web server application logs:

- Lease Report
- BOOTP lease report
- DNS dynamic update report
- Rogue server detection report
- IP-Event report
- MAC-Event report

Lease Report

EventLog Analyzer provides the following details for lease report:

- Lease Report
- Events

BOOTP lease Report

EventLog Analyzer provides the following details for BOOTP lease report:

- Events

DNS dynamic update Report

EventLog Analyzer provides the following details for DNS dynamic update report:

- DNS update details
- Events

The DNS update details are:

- DNS dynamic update request
- DNS dynamic update successful

Rogue server detection Report

EventLog Analyzer provides the following details for Rogue server detection report:

- Events

IP-Event Report

EventLog Analyzer provides the following details for IP-Event report:

- IP Address
- Events

MAC-Event Report

EventLog Analyzer provides the following details for MAC-Event report:

- MAC Address
- Events

Reports for DHCP Linux Logs

Clicking the **View Report** link opens the **Reports for DHCP Linux 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 lets you generate the following pre-defined reports for web server application logs:

- Operations Report
- MAC Address Report
- Client Gateway Report
- IP Report
- Single page summary

Operations Report

EventLog Analyzer provides the following details for operations report:

- Operation
- Events

The operations are:

- DHCPREQUEST
- DHCPNAK
- DHCPDISCOVER
- DHCPOFFER
- DHCPACK
- DHCPINFORM
- if IN
- delete
- DHCPRELEASE
- Abandoning IP

MAC Address Report

EventLog Analyzer provides the following details for MAC Address report:

- MAC Address
- Events

Client Gateway Report

EventLog Analyzer provides the following details for Client Gateway report:

- Gateway
- Events

IP Report

EventLog Analyzer provides the following details for IP report:

- IP Address
- Events

Single Page Summary Report

EventLog Analyzer provides the following details for single page summary report:

- Logging device
- Operation
- IP Address
- MAC Address
- Gateway
- Events

Reports for MS SQL Server Logs

Clicking the **View Report** link opens the **MS SQL 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 lets you generate the following pre-defined reports for MS SQL server application logs:

- Successful Trusted Logins
- Successful Non-Trusted Logins
- Failed User Logins
- Insufficient Resources Events

Successful Trusted Logins Report

EventLog Analyzer provides the following details for MS SQL server application Successful Trusted Logins report:

- Username
- Events

Successful Non-Trusted Logins Report

EventLog Analyzer provides the following details for MS SQL server application Successful Non-Trusted Logins report:

- Username
- Events

Failed User Logins Report

EventLog Analyzer provides the following details for MS SQL server application Failed User Logins report:

- Username
- Events

Insufficient Resources Events Report

EventLog Analyzer provides the following details for MS SQL server application Insufficient Resources Events report:

- Events

Reports for Oracle Audit Logs

Clicking the **View Report** link opens the **Oracle 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. There are delete icon links against each host to delete the host.

The **Report** section at bottom of the page displays the various reports generated in the **Report** column of the table. The total events count of each report are listed in the **Total Counts** columns.

EventLog Analyzer lets you generate the following pre-defined reports for Oracle server application Audit logs:

- Create Table
- Drop Table
- Alter Table
- Alter User
- Alter System
- Create User
- Drop User
- Logon
- Logoff
- Connect
- Shutdown
- Startup
- All Logs - This is created only as a custom report and is not available as a pre-built report.

Create Table Report

EventLog Analyzer provides the following details for Oracle server application Create Table report:

- SESSIONID
- ENTRYID
- USERID
- USERHOST
- TERMINAL
- RETURNCODE
- OBJ$CREATOR
- OBJ$NAME
- Time

Drop Table Report

EventLog Analyzer provides the following details for Oracle server application Drop Table report:

- SESSIONID
- ENTRYID
- USERID
- USERHOST
- TERMINAL
- RETURNCODE
- OBJ$CREATOR
- OBJ$NAME
- Time

Alter Table Report

EventLog Analyzer provides the following details for Oracle server application Alter Table report:

- SESSIONID
- ENTRYID
- USERID
- USERHOST
- TERMINAL
- RETURNCODE
- OBJ$CREATOR
- OBJ$NAME
- Time

Alter User Report

EventLog Analyzer provides the following details for Oracle server application Alter User report:

- SESSIONID
- ENTRYID
- USERID

- USERHOST
- TERMINAL
- RETURNCODE
- OBJ$NAME
- Time

Alter System Report

EventLog Analyzer provides the following details for Oracle server application Alter System report:

- SESSIONID
- ENTRYID
- USERID
- USERHOST
- TERMINAL
- RETURNCODE
- Time

Create User Report

EventLog Analyzer provides the following details for Oracle server application Create User report:

- SESSIONID
- ENTRYID
- USERID
- USERHOST
- TERMINAL
- RETURNCODE
- OBJ$NAME
- Time

Drop User Report

EventLog Analyzer provides the following details for Oracle server application Drop User report:

- SESSIONID
- ENTRYID
- USERID
- USERHOST
- TERMINAL
- RETURNCODE
- OBJ$NAME
- Time

Logon Report

EventLog Analyzer provides the following details for Oracle server application Logon report:

- SESSIONID
- ENTRYID
- USERID
- USERHOST
- TERMINAL
- RETURNCODE
- Time

Logoff Report

EventLog Analyzer provides the following details for Oracle server application Logon report:

- SESSIONID
- ENTRYID
- USERID
- USERHOST
- TERMINAL
- RETURNCODE
- Time

Connect Report

EventLog Analyzer provides the following details for Oracle server application Connect report:

- DATABASE USER
- PRIVILEGE
- CLIENT USER
- CLIENT TERMINAL
- Status
- Time

Shutdown Report

EventLog Analyzer provides the following details for Oracle server application Shutdown report:

- DATABASE USER
- PRIVILEGE
- CLIENT USER
- CLIENT TERMINAL
- Status
- Time

Startup Report

EventLog Analyzer provides the following details for Oracle server application Startup report:

- DATABASE USER
- PRIVILEGE
- CLIENT USER
- CLIENT TERMINAL
- Status
- Time

All Logs

This is created only as a custom report and is not available as a pre-built report.
In this report all actions and severity events will be available.

Viewing IBM AS/400 System History Log Reports

The history logs of IBM AS/400 contains 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.

You can view the reports of the history logs in EventLog Analyzer.

Select the **Home** tab. In the **Dashboard**, below the events graph, you will find the **Hosts** and **Applications** tabs. 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

Creating Custom Reports

Custom reports in EventLog Analyzer let you monitor specific events and hosts exclusively. Custom report profiles can be scheduled to run automatically during selected time intervals, and also e-mailed to recipients as PDF or CSV reports.

Custom reports are listed under the **My Reports** section, found in the **Reports** tab, and the left navigation pane.

The **My Reports** section lists all the custom reports created so far, the hosts that are reported on, and scheduling options. Click on the report name to view the report. The page contains a menu bar and the menu bar contains the following menu:

- **Add New Report** - Click this menu to create a new custom report.
- **Delete Report** - Select the check boxes of custom reports to be deleted and click the **Delete Report** link to delete report(s).
- **Export Profiles** - Select the check boxes of report profiles to be exported and click this menu. The profile will be downloaded as an XML file (**EventLogAnalyzer_Profiles.xml**), through your browser into your client machine.
- **Import Profiles** - Click this menu to import report profiles. On clicking the menu, **Import Profiles** screen pops-up. In that, you will find **File Location** text box and **Browse** button besides. Enter the location of the XML file (**EventLogAnalyzer_Profiles.xml**) or use the browse button to locate the XML file. Click **Import** button to import the profiles in to EventLog Analyzer server and **Cancel** button to cancel the import profiles operation. If the report already exist in EventLog Analyzer, clicking **Import** button will list **Failed To Import** option and the existing reports with check boxes and you will find **Over Write** button and **Cancel** button to cancel the import profiles operation. Select the check boxes of report profiles to overwrite and click **Over Write** button.

There will be no hosts configured for the imported report profiles. You have to edit the report profile to configure the hosts.

Click the icon to edit the corresponding custom report configuration details. If the report profile has no schedules associated with it, the icon is displayed. Click this icon to schedule the report profile. If the report profile already has a schedule associated with it, the icon is displayed. Click this icon to create another schedule for this report profile.

Creating a New Custom Report

Click the **Add New Report** link to create a new custom report. You can find this link on the sub tab, and the **My Reports** section in the left navigation pane, and the **Reports** tab.

Click the **Add New Report** link opens the **Create New Report** wizard with three/two pages.

Step 1:

In the **Create New Report** wizard first page, enter report details and select host.

1. Enter a unique name as the **Report Name**, for the new custom report.
2. Select one of the three report types given as tabs:

a. Select **Custom Report with Event Filters** tab, if the report is meant to monitor specific events on specific hosts
b. Select **Compliance Report for Windows and Syslog Devices** tab, to generate compliance reports for specific Windows or Linux/Unix hosts. Enter the **Compliance Type** in the text box or click the **Select** link. On clicking the link, **Select Reports to Include** window pops-up. In that select the **Compliance Type** in the combo box. From the **Schedule Report for *<HIPAA/SOX/GLBA/PCI>* Compliance** list, select the check boxes for **Check All** or **Clear All** or select check boxes of individual reports of selected compliance.

   - Successful User Logons
   - Successful User Logoffs
   - Logon Attempts
   - Audit Logs Cleared
   - Object Access
   - System Events
   - Host Session Status
   - Successful User Account Validation
   - Failed User Account Validation

   Click **Done** button to save selection and close window. Click **Cancel** to cancel the operation. *(Step 2 will be skipped in this case)*

c. Select **Application Report for Application Logs** tab, to generate application reports for a specific application of a host. Select the **Application Type** in the text box or click the **Select** link. On clicking the link, **Select Reports to Include** window pops-up. In that select the **Application Type** (Oracle Logs) in the combo box. From the **Available Reports** list, select the check boxes for **Check All** or **Clear All** or select check boxes of individual reports of selected application type.

   The available reports for '**Application Type: Oracle Logs**' are:

   - Create Table
   - Drop Table
   - Alter Table
   - Alter User
   - Alter System
   - Create User
   - Drop User
   - Logon
   - Logoff
   - Connect
   - Shutdown
   - Startup
   - All Logs - This is created only as a custom report and is not available as a pre-built report.

   The available reports for '**Application Type: IIS W3C Web Server Logs**' are:

   - Hosts Report
   - Users Report

- File Type Report
- Page URLs Report
- Browser Usage Report
- OS Usage Report
- HTTP Error Status Code Report
- Malicious URL Report

The available reports for '**Application Type: IIS W3C FTP Logs**' are:

- Hosts Report
- Users Report
- File Type Report
- Server services Report
- Server IPs Report
- Source Port Report

The available reports for '**Application Type: DHCP Windows Logs**' are:

- Lease Report
- BOOTP lease report
- DNS dynamic update report
- Rogue server detection report
- IP-Event report
- MAC-Event report

The available reports for '**Application Type: DHCP Linux Logs**' are:

- Operations Report
- MAC Address Report
- Client Gateway Report
- IP Report
- Single page summary

Click **Done** button to save selection and close window. Click **Cancel** to cancel the operation. *(Step 2 will be skipped in this case)*

3. Select the hosts or host groups to report on
4. Click **Next** to continue.

Step 2:

In the **Create New Report** wizard second page, select the event filters and message filters. There are two set of event type/severity lists, one list of filters for Windows hosts and the other list of filters for Syslog hosts.

1. Select the filters for the events generated by the hosts or host groups selected. Choose event type and event severity depending on the specific events that need to be collected for Windows and/or UNIX hosts.
2. You have two options (**Basic Options** and **Advanced**) to filter the messages under two tabs.

   a. **Basic Options** tab

   In the basic option, when multiple values are entered, all the values are considered for filtering events.
   - You will find **Drop the Logs containing** text box to drop the logs containing the message(s).

- You will find **Except** text box to exclude an event with a specific event log message.
- You will find **Event Source** text box to filter out events received from a specific event log source.
- You will find **User** text box to filter out events received for a specific user. This field is effective only for Security (Important) events..

Multiple values can be entered in the text boxes separated by commas..

b. **Advanced** tab

In the advanced option, when multiple values are entered, any of the values or all the values are considered for filtering events depending up on the selection of **Match Any** or **Match All** radio buttons.

- You will find **Match Any** and **Match All** radio buttons for **Drop the Logs containing** text box to drop the logs containing the message(s).
- You will find **Match Any** and **Match All** radio buttons for **Except** text box to exclude events with a specific event log message, from filtering out.
- You will find **Event Source** text box to filter out events received from a specific event log source.
- You will find **User** text box to filter out events received for a specific user. This field is effective only for Security (Important) events..

Multiple values can be entered in the text boxes separated by commas.

3. For Windows hosts, you can also filter events using **Event ID**. Choose the **Event ID** checkbox. With this, the text box and **Event ID** link get enabled and the **Event Type / Event Severity** filter selection gets disabled. Enter the Event IDs for which the events need to be collected. If you do not know the Event IDs, click the **Event ID** link besides the text field. This pops up a window with textual equivalents for the Event IDs. Select the required text entries. Selecting the entry fills the Event IDs in the text field. Unselecting the text entries, removes the Event IDs in the text field. If the **Event ID** filtering is not selected, the **Event Type / Event Severity** filter selection gets enabled. Select the types of events for which the report needs to be generated, from the list of events under **Event Type** column.

   The event types are:

   1. Application
   2. Security
   3. System
   4. DNS Server
   5. File Replication Service
   6. Directory Service

   Select the severity of events for which the report needs to be generated, from the list of severity in the **Event Severity** row.

   The event severity are:

   1. Information
   2. Success
   3. Error
   4. Failure
   5. Warning

Any combination of event type and severity is possible and select the appropriate check boxes provided in a matrix format.

The unselected event type and severity will be excluded from the report.

Ensure you copy/enter the exact string as shown in the Windows Event Viewer. e.g., **Logon Name:<tab/blank spaces>John**

3. For Unix hosts (i.e., Syslog), you can filter events using the **Event Type / Event Severity** filter selection. Select the types of events for which the report needs to be generated, from the list of events under **Event Type** column.

The event types are:

a. kernel
b. user
c. mail
d. daemon
e. auth
f. syslog
g. lpr
h. news
i. uucp
j. cron1
k. authpriv
l. ftp
m. ntp
n. logAudit
o. logAlert
p. cron2
q. local0
r. local1
s. local2
t. local3
u. local4
v. local5
w. local6
x. local7

Select the severity of events for which the report needs to be generated, from the list of severity in the **Event Severity** row.

The event severity are:

a. Emergency
b. Alert
c. Critical
d. Error
e. Warning
f. Notice
g. Information
h. Debug

Any combination of event type and severity is possible and select the appropriate check boxes provided in a matrix format.

The unselected event type and severity will be excluded from the report.

4. Click **Next** to continue.

Step 3:

In the **Create New Report** wizard final (**Select Schedule**) page, select the report generation schedule, configure to send the report by Email and generate test report.

1. If you want to schedule this report to run automatically, choose the time interval after which this report should be generated. Choose from hourly, daily, weekly, or monthly schedules, or choose to run this report only once.

Schedule	Generate Report On	Generate Report For
Hourly	Generate report hourly starting from the below specified time Generate report on: _ Hrs _ Min	Previous Hour Last 60 Minutes
Daily	Generate report daily at the below specified time Generate report on: _ Hrs _ Min	Previous Day Last 24 Hours
Weekly	Generate report on the following days at the specified time Generate report on: _ Day _ Hrs _ Min	Previous Week Last 7 Days
Monthly	Generate report on the following months at the specified time Generate report on: _ Date _ Hrs _ Min	Previous Month Last 30 Days
Only Once	Generate report only once at the specified time Generate report at: Select date using Calendar	Previous Hour Last 60 Minutes Previous Day Last 24 Hours Previous Week Last 7 Days Previous Month Last 30 Days

For Daily and Weekly schedules, you can set the **TimeFilter** for **Custom** Hours, **Only Working Hours**, or **Only NonWorking Hours**.

For the **Daily** schedules, if the option **Run on Week Days** is selected then the reports are run daily except on the weekends. For the **Weekly** or **Monthly** schedules, select the option **Generate Report only for Week Days** if you want to report on the events that occurred only on the week days and not report on events that occurred over the weekends.

You can also add a schedule to this report later from the **My Reports** section

2. You can select the report format. Select the **Report Format**, **PDF** or **CSV** radio buttons.
3. You can select the summary or detailed report to be generated. Select the **Generate Report**, **Summary & Details** or **Only Summary** radio buttons.
4. If you want to email this report, select the **Mail To** check box.

a. Enter the e-mail addresses as comma-separated values in the **Mail To** text box.
b. If the mail server has not been set up yet, an error message is shown below the **Mail To** box. Error message: "**Mail Server is not configured. Click here to configure the Mail Server.**" Click the link inside the error message to configure the mail server settings in the popup window that is opened. If the mail server has been configured already and you want to reconfigure click the link in **Reconfigure the Mail Server here** message and reconfigure the mail server settings in the popup window that is opened.

5. Click **Generate Test Report** to see a preview of how this report will look like, once it is set up. Click **Finish** to save the report. The report is now listed in the **My Reports** section.

Scheduled reports are generated and emailed in PDF or ZIP format.

Creating Custom Reports for AS/400 Hosts

Custom reports in EventLog Analyzer let you monitor specific events and hosts exclusively. Custom report profiles can be scheduled to run automatically during selected time intervals, and also e-mailed to recipients as PDF or CSV reports.

Custom reports are listed under the **My Reports** section, found in the **Reports** tab, and the left navigation pane.

The **My Reports** section lists all the custom reports created so far, the hosts that are reported on, and scheduling options. Click on the report name to view the report. The page contains a menu bar and the menu bar contains the following menu:

- **Add New Report** - Click this menu to create a new custom report.
- **Delete Report** - Select the check boxes of custom reports to be deleted and click the **Delete Report** link to delete report(s).
- **Export Profiles** - Select the check boxes of report profiles to be exported and click this menu. The profile will be downloaded as an XML file (**EventLogAnalyzer_Profiles.xml**), through your browser into your client machine.
- **Import Profiles** - Click this menu to import report profiles. On clicking the menu, **Import Profiles** screen pops-up. In that, you will find **File Location** text box and **Browse** button besides. Enter the location of the XML file (**EventLogAnalyzer_Profiles.xml**) or use the browse button to locate the XML file. Click **Import** button to import the profiles in to EventLog Analyzer server and **Cancel** button to cancel the import profiles operation. If the report already exist in EventLog Analyzer, clicking **Import** button will list **Failed To Import** option and the existing reports with check boxes and you will find **Over Write** button and **Cancel** button to cancel the import profiles operation. Select the check boxes of report profiles to overwrite and click **Over Write** button.

There will be no hosts configured for the imported report profiles. You have to edit the report profile to configure the hosts.

Click the icon to edit the corresponding custom report configuration details. If the report profile has no schedules associated with it, the icon is displayed. Click this icon to schedule the report profile. If the report profile already has a schedule associated with it, the icon is displayed. Click this icon to create another schedule for this report profile

Creating a New Custom Report for AS/400

Click the **Report** link to create a new custom report for AS/400. You can find this link (**AS/400 > Report**) on the sub tab below the main tabs.

Click the **Add New Report** link opens the **Create New Report** wizard with three pages.

Step 1:

In the **Create New Report** wizard first page, enter report details and select host.

1. Enter a unique name as the **Report Name**, for the new custom report.
2. Select the hosts or host groups to report on.
3. Click **Next** to continue.

Step 2:

In the **Create New Report** wizard second page, select the event filters.

1. You have two options (**Basic Options** and **Advanced**) to filter the messages under two tabs.
   a. **Basic Options** tab
      In the basic option, when multiple values are entered, all the values are considered for filtering events.

      - You will find **Drop the Logs containing** text box to drop the logs containing the message(s).
      - You will find **Except** text box to exclude an event with a specific event log message.
      - You will find **Event Source** text box to filter out events received from a specific event log source.
      - You will find **User** text box to filter out events received for a specific user. This field is effective only for Security (Important) events.

      Multiple values can be entered in the text boxes separated by commas.
   b. **Advanced** tab
      In the advanced option, when multiple values are entered, any of the values or all the values are considered for filtering events depending up on the selection of **Match Any** or **Match All** radio buttons.

      - You will find **Match Any** and **Match All** radio buttons for **Drop the Logs containing** text box to drop the logs containing the message(s).
      - You will find **Match Any** and **Match All** radio buttons for **Except** text box to exclude events with a specific event log message, from filtering out.
      - You will find **Event Source** text box to filter out events received from a specific event log source.
      - You will find **User** text box to filter out events received for a specific user. This field is effective only for Security (Important) events.

   Multiple values can be entered in the text boxes separated by commas.
2. Select the severity of events which needs to be filtered, from the list of severity in the **Severity** row.
   The event severity are:
   a. Emergency
   b. Alert
   c. Critical
   d. Error
   e. Warning
   f. Notice
   g. Information
   h. Debug

   Any combination of event severity is possible and select the appropriate check boxes provided.
   The unselected event severity will be dropped.
3. Enterthe message ID of AS/400 host error message to be filtered, in the **Message ID** field.
4. Enterthe name of the IBM AS/400 job for which the error message to be filtered, in the **Job Name** field.
5. Click **Next** to continue.

Step 3:

In the **Create New Report** wizard final page, select the report generation schedule, configure to send the report by Email and generate test report.

1. If you want to schedule this report to run automatically, choose the time interval after which this report should be generated. Choose from hourly, daily, weekly, or monthly schedules, or choose to run this report only once. For Daily, Weekly, and Only once schedules, you can set the **TimeFilter** for **Custom** Hours, **Only Working Hours**, or **Only NonWorking Hours**.

   For the **Daily** schedules, if the option **Run on Week Days** is selected then the reports are run daily except on the weekends. For the **Weekly** or **Monthly** schedules, select the option **Generate Report only for Week Days** if you want to report on the events that occurred only on the week days and not report on events that occurred over the weekends.


You can also add a schedule to this report later from the **My Reports** section

2. You can select the report format. Select the **Report Format**, **PDF** or **CSV** radio buttons.
3. You can select the summary or detailed report to be generated. Select the G**enerate Report**, **Summary & Details** or **Only Summary** radio buttons.
4. If you want to email this report, select the **Mail To** check box.

   a. Enter the e-mail addresses as comma-separated values in the **Mail To** text box.
   b. If the mail server has not been set up yet, an error message is shown below the **Mail To** box. Error message: "**Mail Server is not configured. Click here to configure the Mail Server.**" Click the link inside the error message to configure the mail server settings in the popup window that is opened. If the mail server has been configured already and you want to reconfigure click the link in **Reconfigure the Mail Server here** message and reconfigure the mail server settings in the popup window that is opened.
5. Click **Generate Test Report** to see a preview of how this report will look like, once it is set up. Click **Finish** to save the report. The report is now listed in the **My Reports** section.


Scheduled reports are generated and emailed in PDF or ZIP format.

Editing Custom Reports

Custom reports are listed under the **My Reports** section, found in the **Reports** tab, and the left navigation pane.

The **My Reports** section lists all the custom reports created so far, the hosts that are reported on, and scheduling options. Click on the report name to view the report. Click the icon to delete a report. Click the icon to edit the corresponding custom report configuration details.

Editing an existing Custom Report

Click the icon to edit an existing custom report. You can find this icon besides the report listed in the **My Reports** section in the left navigation pane, and the **Reports** tab.

Clicking the icon opens the **Edit Custom Report** page.

In the **Edit Custom Report** page, edit the host and criteria in the **Edit Host** and **Edit Criteria** tabs.

1. Select the **Edit Host** tab to edit the hosts or host groups to report on.
2. Select the **Edit Criteria** tab to edit the event filters and message filters. There are two set of event type/severity lists, one list of filters for Windows hosts and the other list of filters for Syslog hosts.
   a. Edit the filters for the events generated by the hosts or host groups selected. Edit event type and event severity depending on the specific events that need to be collected for Windows and/or UNIX hosts.
   b. You have two options (**Basic Options** and **Advanced**) to filter the messages under two tabs.
      a. **Basic Options** tab
      In the basic option, when multiple values are entered, all the values are considered for filtering events.

      - You will find **Drop the Logs containing** text box to drop the logs containing the message(s).
      - You will find **Except** text box to exclude an event with a specific event log message.
      - You will find **Event Source** text box to filter out events received from a specific event log source.
      - You will find **User** text box to filter out events received for a specific user. This field is effective only for Security (Important) events.

      Multiple values can be entered in the text boxes separated by commas.

      b. **Advanced** tab

      In the advanced option, when multiple values are entered, any of the values or all the values are considered for filtering events depending up on the selection of **Match Any** or **Match All** radio buttons.

      - You will find **Match Any** and **Match All** radio buttons for **Drop the Logs containing** text box to drop the logs containing the message(s).
      - You will find **Match Any** and **Match All** radio buttons for **Except** text box to exclude events with a specific event log message, from filtering out.

- You will find **Event Source** text box to filter out events received from a specific event log source.
- You will find **User** text box to filter out events received for a specific user. This field is effective only for Security (Important) events.

Multiple values can be entered in the text boxes separated by commas.

c. For Windows hosts, you can also filter events using **Event ID**. Choose the **Event ID** checkbox. With this, the text box and **Event ID** link get enabled and the **Event Type / Event Severity** filter selection gets disabled. Enter the Event IDs for which the events need to be collected. If the **Event ID** filtering is not selected, the **Event Type / Event Severity** filter selection gets enabled. Select the types of events for which the report needs to be generated, from the list of events under **Event Type** column.

The event types are:

d. Application
e. Security
f. System
g. DNS Server
h. File Replication Service
i. Directory Service

Select the severity of events for which the report needs to be generated, from the list of severity in the **Event Severity** row.

The event severity are:

j. Information
k. Success
l. Error
m. Failure
n. Warning

Any combination of event type and severity is possible and select the appropriate check boxes provided in a matrix format.

The unselected event type and severity will be excluded from the report.

o. For Unix hosts (i.e., Syslog), you can filter events using the **Event Type / Event Severity** filter selection. Select the types of events for which the report needs to be generated, from the list of events under **Event Type** column.

The event types are:

p. kernel
q. user
r. mail
s. daemon
t. auth
u. syslog
v. lpr
w. news
x. uucp
y. cron1
z. authpriv

aa. ftp
bb. ntp
cc. logAudit
dd. logAlert
ee. cron2
ff. local0
gg. local1
hh. local2
ii. local3
jj. local4
kk. local5
ll. local6
mm. local7

Select the severity of events for which the report needs to be generated, from the list of severity in the **Event Severity** row.

The event severity are:

1. Emergency
2. Alert
3. Critical
4. Error
5. Warning
6. Notice
7. Information
8. Debug

Any combination of event type and severity is possible and select the appropriate check boxes provided in a matrix format.
The unselected event type and severity will be excluded from the report.

4. Click **Save** to save the edited report. Click **Cancel** button to cancel the edit operation.

Using Advanced Search

EventLog Analyzer provides advanced search feature. Advanced Search, offers numerous options for making your searches more precise and getting more useful results. It allows you to search from the Raw Logs. Using this feature, you will be able to save the search results as Report Profiles. This provides a simplified means to create very precise, selectively filtered and narrowed down Report Profiles.

- Advanced Search
- Using Advanced Search to create Report Profiles

Advanced Search

In Advance Search, you can search the logs for the selected hosts, from the aggregated logs database or raw Host/Application logs, and define matching criteria.

1. To carry out advanced search, click **Advanced Search** link in the Sub Tab. **Advanced Search** screen opens up and there will be **Search Criteria** section. **Search Criteria** has two sub-sections.
   - Select Hosts
   - Select Criteria

Select Hosts

In this sub-section, you can choose the hosts for which you want the logs to be searched. If no host is selected or you want to change the list of selected hosts, select the hosts.

a. Click **Click to Select** link.
b. **Select Hosts** window pops-up. In that window, Select All Groups with selection check box and all the available host groups with individual hosts with selection check boxes are listed. By default, the Default Group and the hosts with selection check boxes are displayed in the screen
c. Select the host groups or individual hosts in the groups by selecting the check boxes as per your requirement. Click **Done** to select the hosts and close the window or click **Cancel** to cancel the operation and close the window.

The selected groups and hosts are displayed in this section.

Select Criteria

In this sub-section, you can define the criteria listed below to search the event database for incidents:

Criteria	Description
Type	Refers to major and particular event types. Major event types are: EventLog Types, Syslog Types
Severity	Refers to the following event severity listed: Emergency, Alert, Critical, Error, Warning, Information, Notice, Debug, Success, Failure
User Name	Refers to the User Name of the user associated with the log events
Event ID	Refers to the Event ID of the log events
Source	Refers to the source host name or IP address from which the events originated
Message	Refers to the log message texts stored in the database

Type Sub-Criteria

If no event type is selected or you want to change the selected event types, select the event types.

i. Click **Click to Select** link.
ii. **Select Event Types** window pops-up. In that window, EventLog Types and Syslog Types and individual event types are listed with selection check boxes. Selecting EventLog Types check box will select all the event types listed under EventLog Types. Same is applied for Syslog Types.
iii. Select the complete lists or individual event types in the lists by selecting the check boxes as per your requirement. Click **Done** to select the event types and close the window or click **Cancel** to cancel the operation and close the window.

The list of event types under **Eventlog Types** are:

1. Application
2. Security
3. System
4. DNS Server
5. File Replication Service
6. Directory Service
7. OSession

The list of event types under **Syslog Types** are:

1. kernel
2. user
3. mail
4. daemon
5. auth
6. syslog
7. lpr
8. news
9. uucp
10. cron1
11. authpriv
12. ftp
13. ntp
14. logAudit
15. logAlert
16. cron2
17. local0
18. local1
19. local2
20. local3
21. local4
22. local5
23. local6
24. local7

2. Select any combination of the following criteria: **Type**, **Severity**, **User Name**, **Event ID**, **Source**, and **Message**.
3. After selecting the Host(s) and Criteria, click **Search** or click **Cancel** to cancel the operation.
4. Clicking **Search** will display the results in the **Search Results** section below the **Search Criteria** section.

The **Search Results** screen displays the following:

- Save as Report Profile link,
- Time frame (From, To)

- Number of rows displayed (1 to x of y) with navigation buttons
- View per page (5, [10], 20, 25, 50, 75, 100, 250, 500)
- and following columns:
  - Host Name
  - Source
  - Type
  - Severity
  - UserName
  - EventId
  - Message
  - Time
- By default, the search is carried out for the time period selected in the Global Calendar present in the left pane of the UI.
- You can also search within the search results. Fill the text boxes below the column headers and click the icon to carry out search within search.


If the search string exists then the search result will be intelligently displayed based on the report category in which it occurred.

Using Advanced Search to create Report Profile

To generate users reports:

- Click **Advanced Search** link in the Sub Tab.
- Select appropriate Hosts.

  In the **Criteria** section, enter **Duration** *isn't* **'0'**.

  - Click **Search** and click **Configure Columns** to change reports columns.

  In the **Criteria** section, select **Match all of the following** or **Match any of the following** to match all the criteria set or any of the criteria set and add or remove additional criteria using **Add Criteria** and **Remove Criteria** links and select **Protocol** *is* **'HTTP'**.

  - Click **Search**. Search results provide the *Reports related to your search <for time period from beginning of the day to current time>*.
  - Select the required reports by selecting the individual reports or by selecting the **Add Criteria** to select all the reports. These will form the criteria for the Report Profile.
- To save the search result as report profile, click **Save as Report Profile** link.
- Enter a **Report Profile Name**.
- Schedule the report, if required.
- Select the **Report Format**: **PDF** or **CSV**.
- Select the **Mail To:** check box if you want the report to be auto delivered. Enter the Email ID(s). If more than one Email ID, separate them with a comma.
- Click **Finish** button. A new report profile is added. Click **Cancel** button if you want to cancel the operation.

Alert Notifications

Creating an Alert Profile

An alert is triggered whenever an event matching a specific criteria is generated. An alert profile lets you define such specific criteria, and also notify you by email, when the corresponding alert is triggered.

Creating a New Alert Profile

Click the **New Alert Profile** link to create a new alert profile. You can find this link on the sub tab below the main tabs, or in the **Alerts** box present on the left side navigation in the **Alerts** tab.

1. Provide an **Alert Profile Name**
2. Choose the **Criticality**. Criticality can be High, Medium, or Low. This is a value that you set for the alert, for your reference.
3. In the **Select Host/Group** section, you can select multiple hosts or groups of hosts from the list, if you want to create an alert profile for multiple hosts or a groups of hosts. This includes both default, and user-created host groups.

Alerts will not work for those listed hosts from which logs have been imported. You need to Add the host to EventLog Analyzer for alerts to work.

In the **Define Criteria** section you will find three tabs with radio buttons to choose the type of alert.

Choose **Predefined Alert** tab, if you want to set alert criteria based on predefined alerts.

Field	Description
Predefined Alert	Select the event description for which the alert has to be triggered. It is easier to identify an event by its description, which indicates what could be the reason the event was generated.
Severity / Event ID	Depending on the type of predefined alert selected, this field displays either the event severity or the event ID.
Log Type	The log type for the selected pre-defined alert is displayed.
Message	If you want the alert to be triggered when an event with a specific event log message is generated, type the log message here.
Number of occurrences	Enter the number of times the event has to be generated before triggering this alert.
Occurring within	Enter the time interval between events, in minutes, after which this alert should be triggered.

6. Choose **Compliance Alert** tab, if you want to set alert criteria based on compliance violation. Compliance alerts are available only for logs received from Windows hosts.You can choose to be notified of HIPAA, GLBA, SOX, and PCI compliance violation by selecting the corresponding checkbox. Alerts will be triggered, for each of these compliance violations like **Failed Logon Attempts**, **Policy Changes**, **Account Changes**, and **Audit Logs Cleared**, based on the below mentioned criteria.

Field	Description
Log Type	Edit the log type for which the alert has to be triggered from the types listed in the combo box.
Severity / Event ID	Depending on the type of Compliance alert selected, this field displays the appropriate event IDs.
Log message contains	If you want the alert to be triggered when an event with a specific event log message is generated, type the log message here.
Except	If you want that the alert should not be triggered when an event with a specific event log message is generated, type the log message here.
Number of occurrences	Edit the number of times the event has to be generated before triggering this alert.
Occurring within	Edit the time interval between events, in minutes, after which this alert should be triggered.

7. Choose **Custom Alert** tab, if you want to set alert criteria based on syslog log type.

- Select the LogType from the **LogType** combo box.
  - Any
  - Application
  - Security
  - System
  - DNS Server
  - File Replication Service
  - Directory Service
  - Auth
  - AuthPriv
  - Cron1
  - Cron2
  - Daemon
  - FTP
  - Kernel
  - Local0
  - Local1
  - Local2
  - Local3
  - Local4
  - Local5
  - Local6
  - Local7
  - LogAudit
  - LogAlert
  - LPR
  - Mail
  - News
  - NTP
  - Syslog
  - User
  - UUCP
- For the log message criteria part, you have the advanced option. Click the **Advanced Option** link. Above the **Log Message Contains** and **Except** criteria text boxes, **Match Any** and **Match All** options with buttons will appear. With **Match Any** and **Match All** options, you will be able to carry out ***and*** or ***or*** operation on the multiple **Log Message Contains** and **Except** criteria.
- If the criteria is based on **Severity**, then the following fields will be available for creating the alert profile.

Field	Description
Log Type	Select the log type of the event for which the alert has to be triggered. The log types that are listed depend on the platform of the host or host group selected. Click on **More** to add additional log type, you can add a **maximum of 5** Log Type. Click on **Remove** to remove the log type.
Severity	Select the severity of the event for which the alert has to be triggered. Click on **More** to add additional severity, you can add a **maximum of 5** severities. Click on **Remove** to remove the severity.
Log Message Contains	If you want the alert to be triggered when an event with a specific event log message is generated, type the log message here. Use comma ',' to separate multiple log message texts.
Except	If you **do not** want the alert to be triggered when an event with a specific event log message is generated, type the log message here. Use comma ',' to separate multiple log message texts.
Event Source	If you want that alert should be generated for events received from specific host sources, mention the same in this text box. The alert will be generated for events received from the host(s) you have entered.
User	If you want that alert should be generated for events received for a specific user, enter the user names in this text box. The alert will be generated for events received for the user(s) you have entered. This field is effective only for Security (Important) events.
Number of occurrences	Enter the number of times the event has to be generated before triggering this alert.
Occurring within	Enter the time interval between events, in minutes, after which this alert should be triggered.

- If the criteria is based on **Event ID**, then the following fields will be available for creating the alert profile.

Field	Description
Log Type	Select the log type of the event for which the alert has to be triggered. The log types that are listed depend on the platform of the hosts or host groups selected.
Event ID	If you want the alert to be triggered for a particular Event ID, mention the Event ID here. Use comma ' **,** ' to separate multiple event id's. You can also specify range of event id's.
Log Message Contains	If you want the alert to be triggered when an event with a specific event log message is generated, type the log message here. Use comma ',' to separate multiple log message texts.
Except	If you **do not** want the alert to be triggered when an event with a specific event log message is generated, type the log message here. Use comma ',' to separate multiple log message texts.
Event Source	If you want that alert should be generated for events received from specific host sources, mention the same in this text box. The alert will be generated for events received from the host(s) you have entered.
User	If you want that alert should be generated for events received for a specific user, enter the user names in this text box. The alert will be generated for events received for the user(s) you have entered. This field is effective only for Security (Important) events.
Number of occurrences	Enter the number of times the event has to be generated before triggering this alert.
Occurring within	Enter the time interval between events, in minutes, after which this alert should be triggered.

7. In the **Notify by:** section, you will find three tabs to choose the notification mechanism.

8. Choose the **E-mail** tab to receive an e-mail every time an alert matching this alert profile is triggered. Fill in the recipient e-mail address in the **To** box. Emails can be sent to more than one email address by separating the email addresses using a comma ' **,** '. Enter the subject of alert in the **Subject** text box. You can select the following arguments from the **Select Arguments** combo box.
   - **Source** - Source of the log
   - **HostName** - Host generating the log
   - **AlertName** - Name of the alert profile.

   You can concatenate the arguments with your own text as subject of alert notification. Enter the text of alert notification in the **Add Notes** text box. You can enter up to 250 characters.

You will have to configure the Mail Server Settings in EventLog Analyzer before sending e-mails from the server.

9. Choose the **Run Program** tab to execute custom scripts when an alert is generated. Specify the location of the script in the **Location** field or click the **Browse** button to get the location of the script/program. Select the parameters to be passed as arguments to the script in the **Arguments** field. The following details from the log can be passed as arguments to the script by clicking the appropriate option under **Select Arguments**.
   - **Source** - Source of the log
   - **Hostname** - Host generating the log
   - **Criticality** - Criticality of the alert

Apart from this, you can also specify other arguments as required.

Notify Alerts using SNMP

You can notify the alerts by **SNMP Traps** by running a program **sendtrap.bat** available in *<EventLog Analyzer Home>/tools* directory. You have to configure the SNMP host and if required SNMP trap port in the batch file.

10. Choose the **SMS** tab to receive an SMS in your mobile phone, every time an alert matching this alert profile is triggered. Fill in the recipient mobile phone number in the **Mobile Number** text box. Enter the SMS message of alert in the **Message** text box. You can select the following arguments from the **Select Arguments** combo box.

    - **Source** - Source of the log
    - **HostName** - Host generating the log
    - **AlertName** - Name of the alert profile
    - **Criticality** - Criticality of the alert
    - **NoOfOccurences** - Number of occurences of the event
    - **Message** - Message of the event

    You can concatenate the arguments with your own text as SMS message of alert notification. You can enter up to 250 characters.

11. Finally click **Add Alert Profile** to save and activate this alert profile. Click **Cancel** to return to the previous page.

Creating Alert Profile for AS/400 Hosts

An alert is triggered whenever an event, matching a specific criteria, is generated. An alert profile lets you define such specific criteria, and also notify you by email, when the corresponding alert is triggered.

Click the **Alert Profiles** option in the **Settings** tab, to trigger an alert for occurance of event with a matching criteria. Clicking the option will open the **Alert Profile Details** page. The page contains a menu bar and list of alert profiles available.

The menu bar contains the following menu:

- **New Alert Profile** - Click this menu to create a new Alert Profile.
- **Delete Alert** - Select the check boxes of Alert Profiles to be deleted and click this menu.
- **Export Profiles** - Select the check boxes of Alert Profiles to be exported and click this menu. The profile will be downloaded as an XML file (**EventLogAnalyzer_Profiles.xml**), through your browser into your client machine.
- **Import Profiles** - Click this menu to import filter profiles. On clicking the menu, **Import Profiles** screen pops-up. In that, you will find **File Location** text box and **Browse** button besides. Enter the location of the XML file (**EventLogAnalyzer_Profiles.xml**) or use the browse button to locate the XML file. Click **Import** button to import the profiles in to EventLog Analyzer server and **Cancel** button to cancel the import profiles operation. If the filter already exist in EventLog Analyzer, clicking **Import** button will list **Failed To Import** option and the existing filters with check boxes and you will find **Over Write** button and **Cancel** button to cancel the import profiles operation. Select the check boxes of filters to overwrite and click **Over Write** button.

	There will be no hosts configured for the imported filter profiles. You have to edit the filter profile to configure the hosts.

Managing Alert Profiles

The **Alert Profiles** option lists all the Alert Profiles created so far, with the option to add more. Click the  icon to disable the Alert Profile. This is a toggle icon, so click it again to enable the Alert Profile. Click the  icon to *Edit the Alert Profile*. Click the  icon to delete the filter. The list also shows the filter type, hosts and host groups for which the filter has been set up.

Creating a New Alert Profile for AS/400

Click the **Alert** link to create a new alert profile for AS/400. You can find this link (**AS/400 > Alert**) on the sub tab below the main tabs.

1. Provide an **Alert Profile Name**
2. Choose the **Criticality**. Criticality can be High, Medium, or Low. This is a value that you set for the alert, for your reference.
3. In the **Select Host/Group** section, you can select multiple hosts or groups of hosts from the list, if you want to create an alert profile for multiple hosts or a groups of hosts. This includes both default, and user-created host groups.

	Alerts will not work for those listed hosts from which logs have been imported. You need to Add the host to EventLog Analyzer for alerts to work.

In the **Define Criteria** section you have to define the criteria for Alert generation. For the log message criteria part, you have the advanced option. Click the **Advanced Option** link. Above the **Log Message Contains** and **Except** criteria text boxes, **Match Any** and **Match All** options with buttons will appear. With **Match Any** and **Match All** options, you will be able to carry out ***and*** or ***or*** operation on the multiple **Log Message Contains** and **Except** criteria.

- If the criteria is based on **Severity**, then the following fields will be available for creating the alert profile.

Field	Description
Severity	Select the severity of the event for which the alert has to be triggered. The severity list is: Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug
Message ID	The message ID of AS/400 host error message.
JobName	The name of the IBM AS/400 job for which the error message was generated.
Log Message Contains	If you want the alert to be triggered when an event with a specific event log message is generated, type the log message here. Use comma ',' to separate multiple log message texts.
Except	If you **do not** want the alert to be triggered when an event with a specific event log message is generated, type the log message here. Use comma ',' to separate multiple log message texts.
Event Source	If you want that alert should be generated for events received from specific host sources, mention the same in this text box. The alert will be generated for events received from the host(s) you have entered.
User	If you want that alert should be generated for events received for a specific user, enter the user names in this text box. The alert will be generated for events received for the user(s) you have entered. This field is effective only for Security (Important) events.
Number of occurrences	Enter the number of times the event has to be generated before triggering this alert.
Occurring within	Enter the time interval between events, in minutes, after which this alert should be triggered.

7. In the **Notify by:** section, you will find three tabs to choose the notification mechanism.
8. Choose the **E-mail** tab to receive an e-mail every time an alert matching this alert profile is triggered. Fill in the recipient e-mail address in the **To** box. Emails can be sent to more than one email address by separating the email addresses using a comma ' **,** '. Enter the subject of alert in the **Subject** text box. You can select the following arguments from the **Select Arguments** combo box.
   - **Source** - Source of the log
   - **HostName** - Host generating the log
   - **AlertName** - Name of the alert profile.

You can concatenate the arguments with your own text as subject of alert notification. Enter the text of alert notification in the **Add Notes** text box. You can enter up to 250 characters.

	You will have to configure the Mail Server Settings in EventLog Analyzer before sending e-mails from the server.

9. Choose the **Run Program** tab to execute custom scripts when an alert is generated. Specify the location of the script in the **Location** field or click the **Browse** button to get the location of the script/program. Select the parameters to be passed as arguments to the script in the **Arguments** field. The following details from the log can be passed as arguments to the script by clicking the appropriate option under **Select Arguments**.
   - **Source** - Source of the log
   - **Hostname** - Host generating the log
   - **Criticality** - Criticality of the alert

Apart from this, you can also specify other arguments as required.

Notify Alerts using SNMP

You can notify the alerts by **SNMP Traps** by running a program **sendtrap.bat** available in *<EventLog Analyzer Home>/tools* directory. You have to configure the SNMP host and if required SNMP trap port in the batch file.

10. Choose the **SMS** tab to receive an SMS in your mobile phone, every time an alert matching this alert profile is triggered. Fill in the recipient mobile phone number in the **Mobile Number** text box. Enter the SMS message of alert in the **Message** text box. You can select the following arguments from the **Select Arguments** combo box.
    - **Source** - Source of the log
    - **HostName** - Host generating the log
    - **AlertName** - Name of the alert profile
    - **Criticality** - Criticality of the alert
    - **NoOfOccurences** - Number of occurences of the event
    - **Message** - Message of the event

    You can concatenate the arguments with your own text as SMS message of alert notification. You can enter up to 250 characters.

11. Finally click **Add Alert Profile** to save and activate this alert profile. Click **Cancel** to return to the previous page.

Viewing 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  icon against an alert profile indicates that an email notification has been setup. The  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  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 on  Alerts link on the left navigation pane or click the **Alert Profiles** link in the **Settings** tab.

Editing an Alert Profile

From Alert Profile Details page click the edit alert icon to edit an already existing alert profile. Edit Alert Profile page lets you edit an already created alert profile.

Editing an Alert Profile

1. Edit the Criticality. Criticality can be High, Medium, or Low. This is a value that you set for the alert, for your reference.
2. In the Select Host/Group section, you can select multiple hosts or groups of hosts from the list, if you want to edit an alert profile for multiple hosts or a groups of hosts. This includes both default, and user-created host groups.

	Alerts will not work for those listed hosts from which logs have been imported. You need to Add the host to EventLog Analyzer for alerts to work.

In the **Modify Criteria** section you will find the details to edit, depending upon the type of alert.

If it is a **Predefined Alert** profile, edit alert criteria of predefined alerts.

Field	Description
Log Type	The log type for the selected pre-defined alert is displayed.
Severity / Event ID	Depending on the type of predefined alert selected, this field displays either the event severity or the event ID.
Log message contains	If you want the alert to be triggered when an event with a specific event log message is generated, type the log message here.
Except	If you want that the alert should not be triggered when an event with a specific event log message is generated, type the log message here.
Number of occurrences	Edit the number of times the event has to be generated before triggering this alert.
Occurring within	Edit the time interval between events, in minutes, after which this alert should be triggered.

6. If it is **Compliance Alert** profile,editalert criteria of compliance violation. Compliance alerts are available for logs received from Windows host only. You can choose to be notified of HIPAA, GLBA, SOX, and PCI compliance violation by selecting the corresponding checkbox. Alerts will be triggered, for each of these compliance violations like **Failed Logon Attempts**, **Policy Changes**, **Account Changes**, and **Audit Logs Cleared**, based on the below mentioned criteria.

Field	Description
Log Type	Edit the log type for which the alert has to be triggered from the types listed in the combo box.
Severity / Event ID	Depending on the type of Compliance alert selected, this field displays the appropriate event IDs.
Log message contains	If you want the alert to be triggered when an event with a specific event log message is generated, type the log message here.
Except	If you want that the alert should not be triggered when an event with a specific event log message is generated, type the log message here.
Number of occurrences	Edit the number of times the event has to be generated before triggering this alert.
Occurring within	Edit the time interval between events, in minutes, after which this alert should be triggered.

7. If it is a **Custom Alert** profile,editalert criteria of syslog log type.

- Select the LogType from the **LogType** combo box.
  - Any
  - Application
  - Security
  - System
  - DNS Server
  - File Replication Service
  - Directory Service
  - Auth
  - AuthPriv
  - Cron1
  - Cron2
  - Daemon
  - FTP
  - Kernel
  - Local0
  - Local1
  - Local2
  - Local3
  - Local4
  - Local5
  - Local6
  - Local7
  - LogAdit
  - LogAlert
  - LPR
  - Mail
  - News
  - NTP
  - Syslog
  - User
  - UUC
- For the log message criteria part, you have the advanced option. Click the **Advanced Option** link. Above the **Log Message Contains** and **Except** criteria text boxes, **Match Any** and **Match All** options with buttons will appear. Additionally, **Event Source** text box will appear below the **Except** criteria text box. With **Match Any** and **Match All** options, you will be able to carry out ***and*** or ***or*** operation on the multiple **Log Message Contains** and **Except** criteria.
- If the Select Criteria is based on **Severity**, then the following fields will be available for creating the alert profile.

Field	Description
Log Type	Edit the log type of the event for which the alert has to be triggered. The log types that are listed depend on the platform of the host or host group selected. Click on **More** to add additional log type, you can add a **maximum of 5** Log Type. Click on **Remove** to remove the log type.
Severity	Edit the severity of the event for which the alert has to be triggered. Click on **More** to add additional severity, you can add a **maximum of 5** severities. Click on **Remove** to remove the severity.
Log Message Contains	If you want the alert to be triggered when an event with a specific event log message is generated, type the log message here. Use comma ',' to separate multiple log message texts.
Except	If you **do not** want the alert to be triggered when an event with a specific event log message is generated, type the log message here. Use comma ',' to separate multiple log message texts.
Number of	Edit the number of times the event has to be generated before triggering

Field	Description
occurrences	this alert.
Occurring within	Edit the time interval between events, in minutes, after which this alert should be triggered.

- If the Select Criteria is based on **Event ID**, then the following fields will be available for creating the alert profile.

Field	Description
Log Type	Edit the log type of the event for which the alert has to be triggered. The log types that are listed depend on the platform of the hosts or host groups selected.
Event ID	If you want the alert to be triggered for a particular Event ID, mention the Event ID here. Use comma ' **,** ' to separate multiple event id's. You can also specify range of event id's.
Log Message Contains	If you want the alert to be triggered when an event with a specific event log message is generated, type the log message here. Use comma ',' to separate multiple log message texts.
Except	If you **do not** want the alert to be triggered when an event with a specific event log message is generated, type the log message here. Use comma ',' to separate multiple log message texts.
Number of occurrences	Edit the number of times the event has to be generated before triggering this alert.
Occurring within	Edit the time interval between events, in minutes, after which this alert should be triggered.

7. In the **Notify by:** section, you will find three tabs to choose the notification mechanism.
8. Select the **E-mail** tab to edit it is selected to receive an e-mail every time an alert matching this alert profile is triggered. Editthe recipient e-mail address in the **To** box. Emails can be sent to more than one email address by separating the email addresses using a comma ' **,** '. Editthe subject of alert in the **Subject** text box. You can select the following arguments from the **Select Arguments** combo box.
   - **Source** - Source of the log
   - **HostName** - Host generating the log
   - **AlertName** - Name of the alert profile.

You can concatenate the arguments with your own text as subject of alert notification. Editthe text of alert notification in the **Add Notes** text box. You can enter up to 250 characters.

You will have to configure the Mail Server Settings in EventLog Analyzer before sending e-mails from the server.

9. Select the **Run Program** tab to edit if it is selected to execute custom scripts when an alert is generated.Editthe location of the script in the **Location** field or click the **Browse** button to get the location of the script/program.Editthe parameters to be passed as arguments to the script in the **Arguments** field. The following details from the log can be passed as arguments to the script by clicking the appropriate option under **Select Arguments**.
   - **Source** - Source of the log
   - **Hostname** - Host generating the log
   - **Criticality** - Criticality of the alert
10. Apart from this, you can also specify other arguments as required.

Select the **SMS** tab to edit if it is selected to receive an SMS in your mobile phone, every time an alert matching this alert profile is triggered.Editin the recipient mobile phone number in the **Mobile Number** text box. Enter the SMS message of alert in the **Message** text box. You can select the following arguments from the **Select Arguments** combo box.

- **Source** - Source of the log
- **HostName** - Host generating the log
- **AlertName** - Name of the alert profile
- **Criticality** - Criticality of the alert
- **NoOfOccurences** - Number of occurences of the event
- **Message** - Message of the event

You can concatenate the arguments with your own text as SMS message of alert notification. You can enter up to 250 characters.

11. Finally click **Save Alert Profile** to save the edited alert profile. Click **Cancel** to return to the previous page.

Configuring System Settings

The **Settings** tab lets you configure several system settings for the server running EventLog Analyzer, as well as other settings.

The **Simulate** option generates sample event logs so that you can view reports without having to collect actual event logs. At any time click the **Stop Simulate** link to stop sending the sample data to EventLog Analyzer

The following is the the list of configuration options available under the **System Settings** section:

Setting	Description
Add New Host	Click this link to add a host from which event logs need to be collected
Host Groups	Click this link to add, edit, or delete host groups
Host Details	Click this link to view device details for each host from which event logs are collected
Alert Profiles	Click this link to view the alert profiles set up so far
Database Filters	Click this link to set up database filters for storing event logs
Schedule Listing	Click this link to view the list of reports scheduled
Archived Files	Click this link to configure archiving intervals, or load an archived file into the database
Imported Log Files	Click this link to import Windows Event Log files (type *.evt* format) from the local machine or by FTP from remote machine
Rebranding ELA Web Client	To customize EventLog Analyzer Web Client to suit the needs of Managed Security Service Providers (MSSPs) or large enterprises
Compliance Reports	Click this link to configure a new compliance type with required reports from the set of default reports and customize the existing compliance type with required reports.
Working Hour	Click this link to configure Working and Non-Working hour event log collection pattern of the organization.

The following is the the list of configuration options available under the **Administration Settings** section:

Setting	Description
External Authentication Settings	Click this link to import AD users details, import AD users details periodically, use AD authentication.
User Management	Click this link to add, edit, or delete users in EventLog Analyzer
ELA Configurations	Click this link to save the EventLog Analyzer configurations to restore when you restart the server.
Mail Server Settings	Click this link to configure the mail server
Alert Me	Click this link to configure Email alert for EventLog Analyzer failure
Account Settings	Click this link to change the default password and e-mail address set for the user account. This applies to only for users with **Guest** or **Operator** access level
Database Console	Click this link to access the database and execute queries
Server Diagnostics	Click this link to view system-related information
SMS Settings	Click this link to configure the SMS settings in order to get SMS alert notifications in your cellular phone.

Apart from this, the left navigation pane includes the **DB Storage Options** box. The **Current Storage Size** value is used to define the number of days for which event logs collected, will be retained in the database. The default value is 32 days, after which the oldest values are deleted.

You can change the **Current Storage Size** value to reflect the storage settings required for your setup. Once done, click **Update** to save your changes.

Creating Host Groups

EventLog Analyzer lets you group hosts from which event logs are collected. Host groups let you define which hosts you want to analyze event logs from. You can also create custom reports to report on event logs collected from this host group alone.

Click the **Host Groups** link from the **Settings** tab to perform operations on host groups.

By default, Windows hosts are grouped under the **WindowsGroup**, and UNIX hosts are grouped under the **UnixGroup**. All other hosts are grouped under the **DefaultGroup**.

Creating a New Host Group

Click the **New Host Group** link. In the popup window that opens, enter the following details:

1. Enter a unique **Group Name** to identify the host group
2. Give a meaningful **Description** to explain the purpose of the host group
3. Select the hosts to be included in this group from the list of **Available Host(s)** and transfer > them to the **Selected Host(s)**.

Once you are done, click **Add** to create this host group. Click **Cancel** to quit without creating any host group.

Click on the **Number of Hosts** link to list the hosts belonging to the corresponding group. Click on icon to edit the group. To delete a particular group, select the group from the list of groups and click on the delete icon. You cannot delete the **WindowsGroup**, **UnixGroup**, and **DefaultGroup**.

Editing a Host Group

Here you can add new hosts, or remove the existing hosts from this group.
To **add new hosts to this group**, select the hosts to be added from the list of **Available Host(s)** and transfer > them to the **Selected Host(s)**.
To **remove existing hosts from this group**, select the hosts to be removed from the **Selected Host(s)** and transfer < them to the list of **Available Host(s)**.

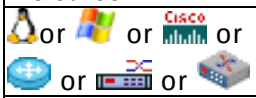
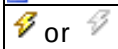
Click **Save** . Click **Cancel** to quit without editing the host group.

Viewing Host Details

Click the **Host Details** link to view the details on the EventLog Server and also the details of the hosts from which EventLog Analyzer is currently collecting event logs.

The **Add New Host** link lets you add a new host to this list. Select multiple hosts and click the **Delete Host** link to delete them all in a single click. There is a **Search** option to search a particular host from the list of hosts available.

The **Hosts Details** table lists all the hosts from which event logs are being collected.

Field/Icon	Description
	This icon tells you whether this host is Linux/ Windows/ Cisco Routers / Switches.
	Click this icon to edit attributes for this host
	Click this icon to enable or disable collecting event logs from this host
HostName	The host name of the machine from which event logs are collected
HostIPAddress	The IP Address of the host.
Delete	Click the icon to delete this host . To delete more than one host, use the check-box to select the host.
Status	The status of log collection from this host. Hover over each icon to see the current status.
NextScanOn	Provides the time at which the next scan is scheduled. This is set while adding the host, where the field **Monitor Interval in minutes** decides the next schedule of the scan, the default being 10 minutes. The status of the hosts and performing unscheduled scans using the **ScanNow** link, impacts the next scanning schedule.
LastMessageOn	Displays the last time at which the host sent an event log to the server.
Action	The *ScanNow* link provides an option to do an unscheduled scan for Windows and AS/400 machines. Until the scan is complete, Scanning in progress icon is displayed. The *PingNow* link pings the Unix/Linux machines to ascertain connectivity is intact.

Editing Host Details

Click the icon next to the host to edit the log collection details for that host. Depending on the type of host, the following details can be edited:

Host Type	Host Detail	Description
Windows	Display Name	The name that is displayed for the host.
	Login Name/ password	The login details (credentials) needed to collect event logs from this host. You need to have Administrator privileges, and for applying the change of credentials to all the hosts in the particular domain, displayed in the field Domain Name, you need to select the option **Apply login name and password changes to all domain(displayed below) authenticated hosts**.

Host Type	Host Detail	Description
	Domain Name	The default domain name to which the host belongs is displayed and it is non-editable. The field is optional. Select the check box **Domain Name**, the domain name field becomes editable and the option **Apply authentication to all hosts in this domain** with selction check box appears below the field. Enter the domain name of the host in the **Domain Name** field. If you want to use the host credentials to all the hosts in the domain to access the hosts and collect logs, select the check box.
	Host Group	Select the Host Group to which the hosts need to be changed to. Click the icon to create a new host group. The option **Apply authentication to all hosts in this Group** with selction check box is available below the field. If you want to use the host credentials to all the hosts in this host group to access the hosts and collect logs, select the check box.
	Monitor Interval	The number of minutes after which the host will be polled for new event logs
Unix / Cisco Device / Any Syslog Device	Display Name	The name that is displayed for the host.
	Host Type	Select the Host Type to which the hosts need to be changes to. Click the icon to create a new host type.
	Display Icon	Click on the **Change Image** link to change the icon that is displayed. You can select from a list of icons or or or or or . You can also add your own icon using the Add New Icon link. If you need to apply the changes to all the host belonging to this Host Group, you need to select the option **Apply to all hosts in Group**.
	Host Group	Select the Host Group to which the hosts need to be changed to. Click the icon to create a new host group.
	Syslog Listener Port	The listener port on which EventLog Analyzer is listening for event logs from this host. This is also the same port on which this host is forwarding event logs to EventLog Analyzer.

Once you have made the changes, click **Save Host Details** to save the new settings for this host


When a host is deleted, it is removed from the database, meaning all host-related data is permanently deleted.

Click on any host to view the event summary for that host.

The **Host Details** link also lists the ports on which EventLog Analyzer is listening for event logs. By default, **Listening Ports** 513 and 514 is added. When you add a UNIX host, and specify a different port other than 513 or 514 to collect logs, that port is automatically added to this list.


Any newly added syslog port will be displayed under Listening Ports only after a couple of minutes.

Managing Alert Profiles

Click the **Alert Profiles** link in the **Settings** tab, to manage all the alert profiles set up so far. Clicking the option will open the **Alert Profile Details** page. The page contains a menu bar and list of alert profiles available.

The menu bar contains the following menu:

- **New Alert Profile** - Click this link to create a new alert profile.
- **Delete Alert** - Select the check boxes of alert profiles to be deleted and click the **Delete Alert** link to delete alert profile(s).
- **Export Profiles** - Select the check boxes of alert profiles to be exported and click this menu. The profile will be downloaded as an XML file (**EventLogAnalyzer_Profiles.xml**), through your browser into your client machine.
- **Import Profiles** - Click this menu to import alert profiles. On clicking the menu, **Import Profiles** screen pops-up. In that, you will find **File Location** text box and **Browse** button besides. Enter the location of the XML file (**EventLogAnalyzer_Profiles.xml**) or use the browse button to locate the XML file. Click **Import** button to import the profiles in to EventLog Analyzer server and **Cancel** button to cancel the import profiles operation. If the alert profile already exist in EventLog Analyzer, clicking **Import** button will list **Failed To Import** option and the existing alert profiles with check boxes and you will find **Over Write** button and **Cancel** button to cancel the import profiles operation. Select the check boxes of alert profiles to overwrite and click **Over Write** button.

There will be no hosts configured for the imported alert profiles. You have to edit the alert profile to configure the hosts.

The Alert Profiles table lists all the alert profiles set up so far, along with all the details selected when the alert profile was created, such as log type, Severity/EventID, Criticality, Occurrences, etc. Click on an alert profile to see the corresponding list of alerts triggered. The toggle icon lets you enable or disable an alert profile and correspondingly start or stop triggering alerts for the same. You can edit the alert profile by clicking on the edit alert icon.

The icon lets you delete an alert profile. Once deleted, the alerts associated with this profile are also deleted from the database. The icon indicates that an e-mail notification has been set up for this alert profile.

Defining Database Filters

You can use the database filters, to filter out the unwanted events from your hosts, from getting stored in the database. By this you can save the hard drive space.

For example, if you want to reject/ filter out the events with the Event ID 1001, in the database filters, choose the **Event ID:** box and enter 1001. If you are not aware of the Event ID(s), kindly uncheck the events that you do not want to get stored. For example, if you do not want the *Information* type of events, unselect the *Information* check box. This will reject all the *Information* type of events for the host(s) that you choose in the database filters wizard.

Click the **Database Filters** option in the **Settings** tab, to apply specific event filters on the data collected and stored in the database. With this option, you can store only the necessary event logs in the database, making it easier to search for particular events, and optimizing the capacity of the database. Clicking the option will open the **Filter Details** page. The page contains a menu bar and list of filters available.

The menu bar contains the following menu:

- **New Filter** - Click this menu to create a new database filter.
- **Delete Filter** - Select the check boxes of filters to be deleted and click this menu.
- **Export Profiles** - Select the check boxes of filter profiles to be exported and click this menu. The profile will be downloaded as an XML file (**EventLogAnalyzer_Profiles.xml**), through your browser into your client machine.
- **Import Profiles** - Click this menu to import filter profiles. On clicking the menu, **Import Profiles** screen pops-up. In that, you will find **File Location** text box and **Browse** button besides. Enter the location of the XML file (**EventLogAnalyzer_Profiles.xml**) or use the browse button to locate the XML file. Click **Import** button to import the profiles in to EventLog Analyzer server and **Cancel** button to cancel the import profiles operation. If the filter already exist in EventLog Analyzer, clicking **Import** button will list **Failed To Import** option and the existing filters with check boxes and you will find **Over Write** button and **Cancel** button to cancel the import profiles operation. Select the check boxes of filters to overwrite and click **Over Write** button.

There will be no hosts configured for the imported filter profiles. You have to edit the filter profile to configure the hosts.

Managing Database Filters

The Database Filters option lists all the filters created so far, with the option to add more. Click the  icon to disable the filter. This is a toggle icon, so click it again to enable the filter. Click the  icon to Edit the Database Filter. Click the  icon to delete the filter. The list also shows the filter type, hosts and host groups for which the filter has been set up.

Creating a New Database Filter

Click on **New Filter** to create a new database filter.

1. Provide a **Filter Name**.
2. You have two options (**Basic Options** and **Advanced**) to filter the messages under two tabs.

a. **Basic Options** tab

In the basic option, when multiple values are entered, all the values are considered for filtering events.

- You will find **Drop the Logs containing** text box to drop the logs containing the message(s).
- You will find **Except** text box to exclude an event with a specific event log message.
- You will find **Event Source** text box to filter out events received from a specific event log source.
- You will find **User** text box to filter out events received for a specific user. This field is effective only for Security (Important) events.

Multiple values can be entered in the text boxes separated by commas.

b. **Advanced** tab

In the advanced option, when multiple values are entered, any of the values or all the values are considered for filtering events depending up on the selection of **Match Any** or **Match All** radio buttons.

- You will find **Match Any** and **Match All** radio buttons for **Drop the Logs containing** text box to drop the logs containing the message(s).
- You will find **Match Any** and **Match All** radio buttons for **Except** text box to exclude events with a specific event log message, from filtering out.
- You will find **Event Source** text box to filter out events received from a specific event log source.
- You will find **User** text box to filter out events received for a specific user. This field is effective only for Security (Important) events.

Multiple values can be entered in the text boxes separated by commas.

3. Select the **Windows** tab for the Windows Hosts Filters and **Syslog** tab for Unix Hosts Filters.

a. **Windows** tab

- If you would like to filter based on Windows Event ID, then select the **By Event ID** option and provide the Event ID's (Use comma ',' to separate multiple Event ID's).
- If you would like to filter based on **Event Type** and **Event Severity**, then select the **By Type / Severity** option. Select the types of events which needs to be filtered, from the list of events under **Event Type** column. The event types are:
  i. Application
  ii. Security
  iii. System
  iv. DNS Server
  v. File Replication Service
  vi. Directory Service

  Select the severity of events which needs to be filtered, from the list of severity in the **Event Severity** row.

The event severity are:

vii. Information
viii. Success
ix. Error
x. Failure
xi. Warning

Any combination of event type and severity is possible and select the appropriate check boxes provided in a matrix format.

The unselected event type and severity will be dropped.

b. **Syslog** tab

- Unselect the types of events which needs to be filtered, from the list of events under **Event Type** column.
  The event types are:
  i. kernel
  ii. user
  iii. mail
  iv. daemon
  v. auth
  vi. syslog
  vii. lpr
  viii. news
  ix. uucp
  x. cron1
  xi. authpriv
  xii. ftp
  xiii. ntp
  xiv. logAudit
  xv. logAlert
  xvi. cron2
  xvii. local0
  xviii. local1
  xix. local2
  xx. local3
  xxi. local4
  xxii. local5
  xxiii. local6
  xxiv. local7

  Unselect the severity of events for which needs to be filtered, from the list of severity in the **Event Severity** row.

  The event severity are:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Information
- Debug

Any combination of event type and severity is possible and select the appropriate check boxes provided in a matrix format.

4. Click **Next**.
5. Choose the hosts and/or host groups on which the filter needs to be applied.
6. Click **Finish** to create and activate this database filter.

Editing Database Filters

In the **Edit Hosts** tab you can add or remove hosts from this DB Filter. In the **Edit Criteria** tab you can modify the **Event Type**, **Event Severity**, **Event ID,** or **Message Filters** for the **Filters for Windows Hosts** and/or **Filters for Unix Hosts**. Click **Save** once the required modifications have been done in **Edit Hosts** tab or **Edit Criteria** tab or in both tabs.

Defining Database Filters for AS/400 hosts

You can use the database filters, to filter out the unwanted events from your hosts, from getting stored in the database. By this you can save the hard drive space.
For example, if you want to reject/ filter out the messages with the Message ID CPF8902, in the database filters, enter *CPF8902* in the **Message ID:** field. If you do not want the *Information* severity of messages, unselect the *Information* check box. This will reject all the *Information* severity messages for the AS/400 host(s) that you choose in the database filters wizard.

Click the **Database Filters** option in the **Settings** tab, to apply specific event filters on the data to be stored in the database. With this option, you can store only the necessary event logs in the database, making it easier to search for particular events, and optimizing the capacity of the database. Clicking the option will open the **Filter Details** page. The page contains a menu bar and list of filters available.

The menu bar contains the following menu:

- **New Filter** - Click this menu to create a new database filter.
- **Delete Filter** - Select the check boxes of filters to be deleted and click this menu.
- **Export Profiles** - Select the check boxes of filter profiles to be exported and click this menu. The profile will be downloaded as an XML file (**EventLogAnalyzer_Profiles.xml**), through your browser into your client machine.
- **Import Profiles** - Click this menu to import filter profiles. On clicking the menu, **Import Profiles** screen pops-up. In that, you will find **File Location** text box and **Browse** button besides. Enter the location of the XML file (**EventLogAnalyzer_Profiles.xml**) or use the browse button to locate the XML file. Click **Import** button to import the profiles in to EventLog Analyzer server and **Cancel** button to cancel the import profiles operation. If the filter already exist in EventLog Analyzer, clicking **Import** button will list **Failed To Import** option and the existing filters with check boxes and you will find **Over Write** button and **Cancel** button to cancel the import profiles operation. Select the check boxes of filters to overwrite and click **Over Write** button.

There will be no hosts configured for the imported filter profiles. You have to edit the filter profile to configure the hosts.

Managing Database Filters

The Database Filters option lists all the filters created so far, with the option to add more. Click the  icon to disable the filter. This is a toggle icon, so click it again to enable the filter. Click the  icon to Edit the Database Filter. Click the  icon to delete the filter. The list also shows the filter type, hosts and host groups for which the filter has been set up.

Creating a New Database Filter for AS/400

Click the **Filter** link to create a new database filter for AS/400. You can find this link (**AS/400 > Filter**) on the sub tab below the main tabs.

1. Provide a **Filter Name**.
2. You have two options (**Basic Options** and **Advanced**) to filter the messages under two tabs.

a. **Basic Options** tab

In the basic option, when multiple values are entered, all the values are considered for filtering events.

- You will find **Drop the Logs containing** text box to drop the logs containing the message(s).
- You will find **Except** text box to exclude an event with a specific event log message.
- You will find **Event Source** text box to filter out events received from a specific event log source.
- You will find **User** text box to filter out events received for a specific user. This field is effective only for Security (Important) events.

Multiple values can be entered in the text boxes separated by commas.

b. **Advanced** tab

In the advanced option, when multiple values are entered, any of the values or all the values are considered for filtering events depending up on the selection of **Match Any** or **Match All** radio buttons.

- You will find **Match Any** and **Match All** radio buttons for **Drop the Logs containing** text box to drop the logs containing the message(s).
- You will find **Match Any** and **Match All** radio buttons for **Except** text box to exclude events with a specific event log message, from filtering out.
- You will find **Event Source** text box to filter out events received from a specific event log source.
- You will find **User** text box to filter out events received for a specific user. This field is effective only for Security (Important) events.

Multiple values can be entered in the text boxes separated by commas.

3. Select the severity of events which needs to be filtered, from the list of severity in the **Severity** row.
   The event severity are:
   a. Emergency
   b. Alert
   c. Critical
   d. Error
   e. Warning
   f. Notice
   g. Information
   h. Debug
   Any combination of event severity is possible and select the appropriate check boxes provided.
   The unselected event severity will be dropped.
4. Enterthe message ID of AS/400 host error message to be filtered, in the **Message ID** field.
5. Enterthe name of the IBM AS/400 job for which the error message to be filtered, in the **Job Name** field.
6. Click **Next**.
7. Choose the IBM AS/400 hosts and/or host groups on which the filter needs to be applied.
8. Click **Finish** to create and activate this database filter.

Editing Database Filters

In the **Edit Hosts** tab you can add or remove hosts from this DB Filter. In the **Edit Criteria** tab you can modify the **Event Type**, **Event Severity**, **Event ID,** or **Message Filters** for the **Filters for Windows Hosts** and/or **Filters for Unix Hosts**. Click **Save** once the required modifications have been done in **Edit Hosts** tab or **Edit Criteria** tab or in both tabs.

Scheduling Reports

Once you have created a custom report profile, you can set up schedules to run the report automatically at specified time intervals. You can also configure EventLog Analyzer to automatically email the report once it runs.

	Scheduled reports are generated and emailed only in PDF

Click the **Schedule Listing** link under the **Settings** tab to see the list of reports that have been scheduled so far. The list shows all the schedules that have been set up so far, along with the report profile they are associated with, the type of schedule, and options to delete the schedule.

Click the icon to delete a schedule. The report profile associated with this schedule will no longer be generated automatically at the specified time interval.

The icon against a schedule is a toggle icon used to enable or disable a schedule. When the icon is displayed, the schedule is enabled, and reports will be generated automatically for that schedule. Click the icon to disable the schedule. The icon is displayed indicating that the schedule is currently disabled. Reports will not be generated automatically for this schedule.

Creating a New Schedule

Click the icon or the **New Schedule** link to add a new schedule. In the Add New Schedule page that comes up, enter the following details:

Attribute	Description
Schedule Name	Enter a unique name to identify this schedule
Profile Name	Choose the report profile to which this schedule has to be applied. All the report profiles that have been created are listed.
Mail Id	The first time a schedule is associated with a report profile, you need to enter the e-mail address to which the report has to be sent. Enter multiple e-mail addresses separated by a comma(,).
Hourly*	If you want to schedule this report to run every hour, enter the date and time after which this report has to run every one hour
Daily*	If you want to schedule this report to run every day, enter the date and time after which this report has to run every one day
Weekly*	If you want to schedule this report to run every week, enter the date and time after which this report has to run every one week
Monthly*	If you want to schedule this report to run every month, enter the date and time after which this report has to run every one month
Once only*	If you want to run this report only once, enter the date and time when the report has to be generated

**Choose from any one of these options*

For Daily, Weekly, and Only once schedules, you can set the **TimeFilter** for **Custom** Hours, **Only Working Hours**, or **Only NonWorking Hours**.

For the **Daily** schedules, if the option **Run on Week Days** is selected then the reports are run daily except on the weekends. For the **Weekly** or **Monthly** schedules, select the option **Generate Report only for Week Days** if you want to report on the events that occurred only on the week days and not report on events that occurred over the weekends.

Once you have chosen all the required values click **Save Schedule** to save and activate the new schedule. Click **Cancel** to return to the Schedule Listing page.

Archiving Log Files

EventLog Analyzer archives the event logs received from each host, and zips them in regular intervals. The **Archived Files** page lists the files that have been archived for each host, along with options to load the file into the database, and delete the file.

All Imported Log Files will automatically get listed on the Archived Files page.

Archived Files List

The **Archived Files** page lists the files that have been zipped for each host, along with the archived time, file size, and archiving status.

The columns, in the Archived Files table, are described below:

Attribute	Description
Host Name	The name of the host machine for which the log file is archived.
Start Time	The starting time of the log file archiving process.
Archived Time	The completion time of the log file archiving process.
File Size	The file size of the archived logs.
Status	You can view the log file archiving status in this column. The status values are: *All*, *Loaded*, *Loading*, *Not Loaded*, *Verified* and *Tampered*. The appropriate status value will be displayed, denoting the file archiving status. While loading Archived Files, if the archived file is tampered, it will not be loaded and marked as **Tampered**. If it is not tampered, it will be marked as **Verified**.
Action	You can carry out the following actions on the archived log files. The Actions are: **Load & Search**, **Search** and **DropDB**. The Actions are discussed below.

Search for Archived Files

You can search for the archive log file of your interest using the **Search** icon. Click the **Search** icon, the search option boxes will appear below every column. The **Search** icon will change to **Hide Search Options** icon.
Besides the option boxes of **Start Time** and **Archived Time**, **Calendar** icons will appear for selection.
The options for **File Size** are as given here: The file size is in KB or MB or GB. The file size is displayed as > or = <Upper limit of file size>
The options for **Status** are as given here: The status values are: *All*, *Loaded*, *Loading*, *Not Loaded*, *Verified* and *Tampered*.

Action on Archived Files

Loading of Archived Files

To load an archived file into the database, click the **Load & Search** link against the host for which you need to see archived data. Once the file is fully loaded into the database, The **Load & Search** link will change to **Search** | **DropDB** links and you can search for data in the archives, and view specific information. Click **Search** link to search the archived file which is loaded in to the database. Click **DropDB** link to

drop the table created for corresponding archived file from the database. You can once again load the archived file into the database by clicking the **Load & Search** link.

Click the icon against the archived files you would like to delete. **Once deleted, the archived data cannot be retrieved**.

Viewing Data from Archived Files

Once the archive is fully loaded into the database, click the **Search** link to search for specific data in the archive. In the popup window that opens, carry out the following: Select '**Match any of the following**' or '**Match all of the following**' for using the criteria. You can enter a maximum of four criteria. Enter the criteria for the data, such as the **Source**, **Severity**, **Message**, **Event ID** and **Type**.

Choose the time interval for which you want to see the data that meets all the criteria. Click **Generate Report** to view the records that match the criteria that you have specified.

You can export this report to PDF and CSV formats. Click **Export to: PDF** icon or **CSV** icon on the right top corner of the report page.

Changing Archive Settings

Click the **Archive Settings** link to change the archiving intervals, to disable archiving and also to change the archive location. In the popup window that opens, there will be two sections, **Log Archiving** section and **Log Indexing** section.

In the **Log Archiving** section, there is a **Enable Archiving** checkbox. Select the check box to enable log file archiving and unselect to disable log file archiving.

The archiving options available are described below:

Attribute	Default Value	Description
File Creation Interval	12 hours	The time interval after which a log file is created for each host from which event logs are collected.
Zip Creation Interval	96 hours	The time interval after which log files created for each host are zipped to save disk space.
Encrypt Archive Data	Disable	EventLog Analyzer comes with a feature to encrypt the archive data. To enable encryption of archive data, select the **Enable** radio button and to disable, select **Disable** radion button.
Archive Timestamping	Disable	EventLog Analyzer comes with a feature to timestamp the archive data. To enable time stamping of archive data, select the **Enable** radio button and to disable, select **Disable** radion button.
Retain Archive Logs for	Forever	You can retain the archive log data as per the compliance audit requirement or internal audit policy requirement. The options available are: *Forever*, *1 Year*, *6 Months*, *3 Months*, *1 Month* and *1 Week*. Select the option that suits your requirement.
Archive Location	*<EventLog Analyzer Home>\archive* directory	By default the Archive Location for the event logs and syslogs in EventLog Analyzer is *<EventLog Analyzer Home>\archive* directory, you can change this location by clicking the **Edit** link and providing the location as per your requirement.

In the **Log Indexing** section, the indexing options available are described below:

Attribute	Default Value	Description
Index Location	*<EventLog Analyzer Home>\server\default\indexes* directory	By default the Index Location for the event logs and syslogs in EventLog Analyzer is *<EventLog Analyzer Home>\server\default\indexes* directory, you can change this location by clicking the **Edit** link and providing the location as per your requirement.

Click **Zip Now** to create a zipped file with the currently available log files. Click **Save** to save the archiving options, if you have changed them. Click **Close** to close the Archive Settings box.

Importing Log Files

The **Imported Log Files** link lets you import a windows event log file (type *.evt* format) (type *.evtx* format supported in **Windows Vista** and **2008** machines only) from the local machine or remotely, through FTP.

You can import the following log files:

- Windows Event Log
- IIS W3C Web Server Logs
- IIS W3C FTP Server Logs
- MSSQL Server Logs
- DHCP Windows logs
- DHCP Linux logs
- IBM AS/400 Logs
- Syslog
- EventLog Analyzer Archive

Importing Event Log and Application Log files are explained below.

Importing Event Log File

1. Select the **Settings** tab. In the **System Settings** section, click the **Imported Log File** link.
2. Select the **Event Log Imports** / **Application Log Imports** tab, and click the **Import Log File** link on the right side, to import a new event/application log file. The procedure to import the log files for both Event Logs and Application Logs remain same.
3. Choose **Local Host** if the event log files are present in the local machine from where you are accessing the EventLog Analyzer server.
   a. Select the log format from the **Choose Log Format** combo box (*Windows EventLog, IIS W3C Web Server Logs, IIS W3C FTP Logs, MSSQL Server Logs, DHCP windows logs, DHCP linux logs, IBM AS/400 Logs, Syslog, EventLog Analyzer Archive)*.
   b. Select the **Time Interval** (*Import Once, Import Every Hour, Import Every Day*). Select *Import Every* option and enter __ *Min* after which EventLog Analyzer should retrieve new log files.
   c. Enter the **File Location** in the text box or click **Browse** to locate the log file.
   d. Select the **Log Type** (*Application, Directory Service, DNS Server, File Replication Service, Security, System*) based on the type of event log you are importing.
   e. Select the option **Want to Specify Time Criteria?** if you want to import log file during a specific time period. Select the **From** and **To** dates using the **Calendar** icon besides the fields.
   f. Select the option **Create Throw Away Reports** if you do not want to store the imported event log file for more than 2 days. After 2 days the Throw Away reports are automatically removed from the Imported Log File listing page.
   g. Finally click **Import** to import the log file into the database. The time taken to import a log file depends on its file size.

4. Choose **Remote Host** if you need to import the event log files from a remote location on the network.

   a. Select the log format from the **Choose Log Format** combo box (*Windows EventLog, IIS W3C Web Server Logs, IIS W3C FTP Logs, MSSQL Server Logs, DHCP windows logs, DHCP linux logs, IBM AS/400 Logs, Syslog, EventLog*

Analyzer Archive).

b. Select the **Time Interval** (*Import Once, Import Every Hour, Import Every Day*). Select *Import Every* option and enter __ *Min* after which EventLog Analyzer should retrieve new log files.
c. Click **Select Remote File** link to locate the log file. Enter the remote host's hostname or IP address, and the FTP user name and password. Select the **Protocol** to be used from the combo box: **FTP** or **SFTP/SSH**. Enter the remote host's FTP Port (Default port for **FTP** will be **21** and for **SFTP/SSH** will be **22**). You can click the **List Files** link to locate the file on the remote computer. Select the location on the remote machine where the log file or the entire directory containing the log files is present.
d. Select the **Log Type** (*Application, Directory Service, DNS Server, File Replication Service, Security, System*) based on the type of event log you are importing.
e. Select the option **Want to Specify Time Criteria?** if you want to import log file during a specific time period. Select the **From** and **To** dates using the **Calendar** icon besides the fields.
f. Select the option **Create Throw Away Reports** if you do not want to store the imported event log file for more than 2 days. After 2 days the Throw Away reports are automatically removed from the Imported Log File listing page.
g. Finally click **Import** to import the event log file into the database. The time taken to import a log file depends on its file size.

If you importing an event log file which is much older than the configured **DB Storage option**, then such imported event log files are automatically considered as Throw Away Reports

Importing Application Logs

- You can associate the application logs with the existing hosts. Enter the host name in the **Associate To Host** text box. Alternatively, click the **Existing Host** link besides the text box. Clicking the link will pop-up **List of Existing Hosts** screen. On the top there is a provision to search hosts. The hosts are listed below the search option. Select the host and click **Select** button. Click **Cancel** button to cancel the associating to host operation.

- Some Applications create log file with new name (with time stamp appended) everyday. If the Application log files are to be imported from remote machines, you do not have to change the filename daily, instead select the **Does filename change periodically?** option while importing the logs. Selecting the option displays the the **Filename Pattern:** combo box to select the time stamp pattern that the server appends when the server creates the log file daily. You can also enter new pattern using the '*blue plus*' icon. Select the pattern as required. A help tip icon displays, (when you click the icon) the mapping of the *Timestamp in Filename* to the *Pattern to be given*.

Automatic FTP Scheduling:

Importing of logs with periodic name changing of log files from both local and remote sources can be automated.

- In the **System Settings > Import Log Files**, carryout the following step: Select or select & enter the **Time Interval** (*Import Once, Import Every Hour, Import Every Day, Import Every __ Min*) after which EventLog Analyzer should retrieve new log files.
- Also some Applications create log file with new name (with time stamp appended) everyday. EventLog Analyzer takes care of the dynamic file name change also. If the Application log files are to be imported from remote machines, you do not have to change the filename daily, instead select the **Does filename change periodically?** option while importing the logs. Selecting the option displays the the **Filename Pattern:** combo box to select the time stamp pattern that the server appends when the server creates the log file daily. You can also enter new pattern using the '*blue plus*' icon. Select the pattern as required. A help tip icon displays, (when you click the icon) the mapping of the *Timestamp in Filename* to the *Pattern to be given*.

The **Imported Log Files** listing page shows you the list of windows event log files imported, along with details such as the following for each imported event log file.

Column Head	Description
FileName	Name of the imported event log file. Click on the icon to know the details of errors while importing the event log files.
HostName	Host which generated the event logs.
LogType	The event log type can be **Application, Security, System, Directory Service, DNS Server, or File Replication Service**.
ImportType	Whether the event log file has been imported from the local machine or remotely (remote machine name or ip) through FTP.
ImportedTime	Timestamp at which the event log file was imported.
LogRecord StartTime	Time stamp of the first collected log record in the imported event log file.
LogRecord EndTime	Time stamp of the last collected log record in the imported event log file.
Report Type	The type of custom report that will be generated. The report type can be **Active** or **Throw Away**.
Action	Click on the *Load & Search* link to load the event log file into the EventLog Analyzer database. (MySQL/MSSQL)
	Click on the Search link to search through the DB for matching criteria. The search criteria can be *Source*, *Severity*, *Message*, *Event ID*, *Type* (or *Facility*)
	Click on the Dr opDB link to drop the imported log file table..

Importing Application Log File

The **Application Log Imports** tab of the **Imported Log Files** listing page shows you the list of application log files imported, along with details such as the following for each imported application log file.

Column Head	Description
File Name	Name of the imported application log file. Click on the icon to know the details of errors while importing the application log files..
Format Description	The log format is indicated here
Remote Host	Remote Host from where the application log file has been imported
Status	Indicates the status of file import. Various status are listed below.
Imported Time	The time stamp at which the application log file was imported.
Size	The size of the imported application log file.
Time Taken	The time taken to import the application log file.
Action	Click on the Load & Search *Load & Search* link to load the event log file into the inbuilt MySQL DB
	Click on the Load & Search Search link to search through the DB for matching criteria. The search criteria can be *Source*, *Severity*, *Message*, *Event ID*, *Type* (or *Facility*).
	Click on the Drop Tables DropDB link to drop the imported log file table.

Viewing Data from Imported Files

Once the imported is fully loaded into the database, click the **Search** link to search for specific data in the archive. In the popup window that opens, carry out the following

Select '**Match any of the following**' or '**Match all of the following**' for using the criteria. You can enter a maximum of four criteria. Enter the criteria for the data, such as the **Source**, **Severity**, **Message**, **Event ID** and **Type**.

Choose the time interval for which you want to see the data that meets all the criteria. Click **Generate Report** to view the records that match the criteria that you have specified.

You can export this report to PDF and CSV formats. Click **Export to: PDF** icon or **CSV** icon on the right top corner of the report page. You can also export the Throw Away reports to PDF and CSV formats.

Status of File Import

- Received log file for import
- Continuing to parse log file from last update...
- File received, loading the file into DB
- Import of log file completed
- Import of log file failed!
- The file has not been modified since last update
- Import task enabled!
- Import task disabled!
- Import task already disabled!
- Import task already enabled!
- Import task not available!
- Processing request

	All Imported Log Files will automatically get listed on the Archived Files page, except Application Logs.

Rebranding EventLog Analyzer Web Client

To customize the EventLog Analyzer Web Client follow the steps given below:

1. In the EventLog Analyzer web client, select the **Settings** tab.
2. In **Settings** screen, select the **System Settings > Rebranding ELA Web Client** link. Rebranding **EventLog Analyzer Web Client** page appears.

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).

The rebranding screen contains two sections. At the top you have the **Customize Images** section. In this section, you can customize logos and images. At the bottom you have the **Customize Strings/Links** section. In this section, you can customize strings and links.

Customize Images

Replace the default images with your company/enterprise images

Client Logos & Images	Where it is used	Image Size & Thumbnail	New Image
Company Logo	Login Page	129*39 pixels	
Product Logo	Login Page	289*59 pixels	
Top Band Image	Client Header	232*47 pixels	
PDF Cover Image	PDF Cover Page	612*820 pixels	
PDF Footer Image	PDF Footer	547*37 pixels	
Server Status Image	Tray Icon [Windows]	400*60 pixels	

Customize Strings/Links

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

Client Strings & Links	Where it is used	Existing String/Link	New String/Link
Company Name	Login Page	ZOHO Corp.	
Brand Name	Login Page	ManageEngine	
Company Website	Login Page	www.manageengine.com	
Product Website	Login Page	www.eventloganalyzer.com	
Support E-Mail	Login Page	eventloganalyzer-support@manageengine.com	
Sales E-Mail	About Popup	sales@manageengine.com	
Toll Free	Support Page	+1-888-720-9500	

Click **Update** to update the customized images/logos and strings/texts. Click **Cancel** to cancel the customizing the web client operation.

- 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**

Configuring Compliance Reports Settings

EventLog Analyzer provides a framework that lets you configure a new compliance type with required reports from the set of default reports. There are 11 default report groups available to choose. These reports are derived based on the Event IDs. The framework provides required default reports for four regulatory compliance acts and allows you to modify the default list of reports as per your requirement.

The four regulatory compliance acts are:

1. PCI
2. FISMA
3. HIPAA
4. GLBA
5. SOX

Configuring Compliance Reports Settings

Compliance Settings page

Click the **Compliance Reports** link to configure new or existing compliances. You can find this link on the **System Settings** section of the **Settings** tab. Clicking the **Compliance Reports** link opens the **Compliance Settings** page. On the top of the page, **+ New Compliance** link is present. The page lists the default compliances, with pre-selected reports provided by EventLog Analyzer, in the **Compliance List** section of the page. The **Edit Compliance** section lists the compliance and the number of reports selected for each compliance from the 11 default report groups provided by EventLog Analyzer.

The details of the four default compliances and the pre-selected reports are given below:

- PCI compliance report
- FISMA compliance report
- HIPAA compliance report
- SOX compliance report
- GLBA compliance report

You can add a new compliance and select a list of reports, for the new compliance, from the 11 default report groups provided by EventLog Analyzer. To add a new compliance, click the **+ New Compliance** link is present on the right side top of the **Compliance Settings** page.

PCI Compliance Reports

EventLog Analyzer provides the following report groups to help organizations to comply with the PCI regulations. The following reports cover Requirements 10.1, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.6, 10.2.7

- **Object Access**
  - Object Accessed
  - Object Created
  - Object Modified
  - Object Deleted
  - Object Handle

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

- **Policy Changes**
  - User Policy Changes
  - Domain Policy Changes
  - Audit Policy Changes

- **System Events**
  - System Logs
  - Audit Logs Cleared

- **User Access**
  - Individual User Action

All these reports are accessible from the **PCI Compliance Reports** section.

By default, EventLog Analyzer provides 5 report groups. You have the option to modify the list of reports. You can select a report from the available reports and add it to the list or remove a report from the list. You can configure the description of the reports specific to this compliance.

FISMA Compliance Reports

EventLog Analyzer provides the following reports to help organizations to comply with the FISMA controls. The following controls are covered in the reports:

- Audit and Accountability (AU)
- Certification, Accreditation, and Security Assessments (CA)
- Contingency Planning (CP)
- Access Control (AC)
- Identification and Authentication (IA)
- Configuration Management (CM)

The reports under various groups for the FISMA compliance are:

- **Object Access**
  - Object Accessed
  - Object Created
  - Object Modified
  - Object Deleted
  - Object Handle

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

- **Security Assessment**
  - Windows Services

- **Contigency Planning**
  - Windows Backup
  - Windows Restore
- **User Access**
  - Individual User Action

- **Configuration Management**
  - Windows Software Updates
  - Anti-malwares
  - Other Softwares

All these reports are accessible from the **FISMA Compliance Reports** section.

By default, EventLog Analyzer provides 7 report groups. You have the option to modify the list of reports. You can select a report from the available reports and add it to the list or remove a report from the list. You can configure the description of the reports specific to this compliance.

HIPAA Compliance Reports

EventLog Analyzer provides the following reports under various groups to help comply with the HIPAA regulations:

- **Object Access**
  - Object Accessed
  - Object Created
  - Object Modified
  - Object Deleted
  - Object Handle

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

- **System Events**
  - System Logs
  - Audit Logs Cleared

- **Account Logon**
  - Successful User Account Validation
  - Unsuccessful User Account Validation

All these reports are accessible from the **HIPAA Compliance Reports** section.

By default, EventLog Analyzer provides 4 report groups. You have the option to modify the list of reports. You can select a report from the available reports and add it to the list or remove a report from the list. You can configure the description of the reports specific to this compliance.

Sarbanes-Oxley Compliance Reports

EventLog Analyzer provides the following reports under various groups to help comply with the SOX regulations:

- **Object Access**
  - Object Accessed
  - Object Created
  - Object Modified
  - Object Deleted
  - Object Handle
- **Logon**
  - Successful User Logons
  - Successful User Logoffs
  - Unsuccessful User Logons
  - Terminal Service Session
- **Policy Changes**
  - User Policy Changes
  - Domain Policy Changes
  - Audit Policy Changes
- **System Events**
  - System Logs
  - Audit Logs Cleared
- **Process Tracking**
  - Process Access
- **Account Logon**
  - Successful User Account Validation
  - Unsuccessful User Account Validation
- **User Access**
  - Individual User Action
- **Account Management**
  - User Account Changes
  - Computer Account Changes
  - User Group Changes

All these reports are accessible from the **SOX Compliance Reports** section.

By default, EventLog Analyzer provides all the 8 report groups. You have the option to modify the list of reports. You can remove a report from the list. You can configure the description of the reports specific to this compliance.

GLBA Compliance Reports

EventLog Analyzer provides the following reports under various groups to help comply with the GLBA regulations:

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

- **System Events**
  - System Logs
  - Audit Logs Cleared

All these reports are accessible from the **GLBA Compliance Reports** section.

By default, EventLog Analyzer provides 2 report groups. You have the option to modify the list of reports. You can select a report from the available reports and add it to the list or remove a report from the list. You can configure the description of the reports specific to this compliance.

Adding a New Compliance

Click the **+** icon to configure a new compliance and the required reports. You can find this icon present on the right side of the **Compliance Report** in the left navigation pane of the client UI dashboard. Alternatively, select the **Settings** tab, **System Settings > Compliance Settings** link.

Click the **+ New Compliance** link opens the **New Compliance** page.
In the **Enter Compliance Details** section, enter the name of the new compliance in the **Name** field.
Enter the description of the compliance in the **Description** field.
In the **Select Group** sub-section, all the 11 default report groups, with relevant report for each group, provided by EventLog Analyzer are listed, with check boxes to select. Select the report groups and/or reports as required. The select group sub-section has **Check All**, **Clear All** links to select or unselect all the reports under all the reports groups.

You can also edit the description of various report groups by clicking on the report group link.

Click **Save** button to save the new compliance and **Cancel** button to cancel the adding new compliance operation.

Editing the Compliance / Report Group Description

Click on the **custom compliance / report groups** to edit the description of the custom compliance/report group for this compliance policy. Edit the existing or enter the new description and click **Save** button to save the description and **Cancel** button to cancel the edit description operation.

Click **+ New Compliance** link to add the new compliance and its reports and **Cancel** to cancel the add new compliance operation.

The new compliance report will be listed under the **Compliance List** section below the default compliances.

Adding New Default Report

If you to add more reports to the existing list of default reports, **Want more reports? Tell us here** link is provided at the bottom of the **New Policy** page. Clicking **Tell us here** link opens the **Add Report in New Compliance** window. This window collects the details and sends out a mail to EventLog Analyzer Support.

The details are given below:

- **Your Name**
- **Email ID**
- **To** *eventlog-support@manageengine.com*
- **Compliance Report**
- **Your Report for above compliance**
- **Description**

Enter the details and click **Send** button to send the details as mail to EventLog Analyzer Support. Click **Close** button to close the window.

Working Hour Configuration

Here you can configure the Working and Non-Working hour patterns of your enterprise. This will help you to distinguish between the working and non-working hour event log trends. By default, 10 - 20 Hours are considered as Working Hours and the remaining hours are considered as Non working Hours.

Two options are provided for configuring the working hour patterns.

- **General**

  Here you can mention the **Start Time** and **End Time** for your official working hours, and all hours outside the given range is considered as non-working hours.

  Advanced

  This option provides more customized working hours classification. For example, you may mention intermittent working hours like 8-12, 15-18, 19, 20, 21 Hours. Which means your non-working hour are 12-15 Hours and 21-8 Hours.

Agent Administration

EventLog Analyzer lets you to deploy agents to collect the logs of Windows hosts. The agent can be installed in any server in the network/sub-net. You can assign a number of Windows hosts to the agent for log collection. The agent remote, real-time, uninterrupted transfer of logs from the hosts to the EventLog Analyzer server. Agent pre-processes the logs before transfer to the server. The agent is installed as a service. Each agent supports up to 25 hosts.

Once an agent is installed and assign hosts to it, the agent will start collecting the logs automatically and forwarded to the EventLog Analyzer server. You can install agent from the **Agent Adminstration** page of **Settings** tab. If automatic agent installation fails, you can manually install the agent in that particular machine. You can assign host(s) to an agent from the **Agent Adminstration** page of **Settings** tab. You can also assign and reassign a host to an agent from the **Add New Host** menu and **Edit Host** menu respectively.

If the machine containing the Agent is deleted from EventLog Analyzer server or the agent is uninstalled, the log collection of all the hosts assigned to the agent will be switched over to default EventLog Analyzer server log collection process. If an assigned host is removed from an agent, the log collection of the host will be switched over to default EventLog Analyzer server log collection process.

Click the **Agent Administration** link from the **Settings** tab to manage the EventLog Analyzer Agents.

The **Agent Administration** page opens up and it lists all the sgents istalled in the **Agents Installed** table. On the right extreme, you will find the **Install Agent** button to install new agents.

The **Agents Installed** table will contain the following details. There are **Edit** and **Delete** icons for each agent.

Colums	Description
Agent Name	The name of the machine in which the EventLog Analyzer agent is installed.
Status	The status of the agent. If the agent service is installed successfully the status will be as 'Agent Installed Successfully.' There are two links Restart and Stop besides the status. With the links you can restrat and stop the agent service. If the agent service is running the status will be as 'Service is running.' There are two links Restart and Stop besides the status. With the links you can restrat and stop the agent service. If the agent service is not running the status will be as 'Service is not running.' There is a link Start besides the status. With the link you can strat the agent service.
IP Address	The IP address of the host machine in which the EventLog Analyzer agent is installed.
Hosts Assigned	The number of hosts assigned are displayed as 'x Hosts assigned'. There is a link Add More besides the hosts assigned message. With the link you can assign more hosts to the agent for log collection.

Add More Hosts

You can assign more hosts to an agent using the link **Add More** besides the hosts assigned message. Use the procedure given below.

Click the **Add More** link. The **Assign Hosts** window pops up. In that window, select the hosts to be assigned to this agent from the list of **Available Host(s)** and transfer > them to the **Selected Host(s)**.

Once you are done, click **Apply** to assign the host(s). Click **Cancel** to cancel assign host action.

Editing the Agent

Click the **Edit** icon on the left side against each EventLog Analyzer Agent listed in the **Installed Agents** table.

The **Edit Agent Details** page opens up. Enter the details of the machine(s) in which the agent need to be installed.

The details are:

Colums	Description
Agent Name	The name of the machine in which the EventLog Analyzer agent is installed. The field cannot be edited
Host IP	The IP address of the host machine in which the EventLog Analyzer agent is installed. The field cannot be edited
Domain Name	The domain name of the machine selected for installing the agent
Login Name	The login name of the machine, with Admin user privileges, in which the EventLog Analyzer agent to be installed
Password	The password of the Admin user with the above login name

Edit the Administrator **Login Name** and **Password** for the selected machine
Click on **Verify Login** to ensure that the correct credentials are provided and you are able to authenticate to the host machine.

Once you are done, click **Save Agent Details** to modify the agent details. Click **Cancel** to cancel the edit agent details.

Delete Agent

To delete a particular agent, click the delete icon of the respective agent. You will find a confirmation message '**The agent will be uninstalled. Proceed?**' poping up. Click **OK** to uninstall the agent from the particular machine. Click **Cancel** to cancel the delete agent operation.

Install Agent

Click the **Install Agent** link on the right extreme of the **Agent Administration** page to install new EventLog Analyzer Agents.

The **Install Agent** page opens up. Enter the details of the machine(s) in which the agent need to be installed.

The details are:

Colums	Description
Agent Name	The name of the machine(s) in which the EventLog Analyzer agent is installed. You can enter multiple machine names separated by commas. Alternatively, you can click the Pick Hosts link to get the machine(s), using the network domain or work group, in which the agent need to be installed.
Domain Name	The domain name of the machine(s) selected for installing the agent
Login Name	The login name of the machine(s), with Admin user privileges, in which the EventLog Analyzer agent to be installed
Password	The password of the Admin user with the above login name

Enter the Administrator **Login Name** and **Password** for the selected machine(s)
Click on **Verify Login** to ensure that the correct credentials are provided and you are able to authenticate to the host machine(s).

Once you are done, click **Save** to install agents. Click **Cancel** to cancel the installation.
Pick Hosts

The procedure to pick hosts from the domains/workgroups for agent installation is given below.

Click the **Pick Hosts** link to select machines auto-discovered from domains/work groups scanned on the network. The **Pick Hosts** screen pops up.

Select the **Domain / Workgroup** from the drop down list discovered from the network
Use the **Select All** check box to select all the machines of the selected domain/ workgroup

Use the **Search** box to select the required machines of the selected domain/workgroup
Select the **Login as Domain User** checkbox if you want to use the login credentials of the Domain Administrator.

If you cannot find a specific machine in the domain, click **Rescan the <selected> Domain** to rescan this domain alone

If you cannot find a specific domain, click **Rescan the complete network** to rescan the entire network

If you are done, click **Update** to add the machine(s) and click **Close** to return to the **Install Agents** page.

Configuring Admin Settings

Configuring External Authentication Settings

EventLog Analyzer provides two more external authentication apart from the local authentication. They are **Active Directory** authentication and **Remote Authentication Dial-in User Service (RADIUS)** authentication. If you import users from Active Directory or if you add a RADIUS server details, you will find the **Options >>** link besides the **Login** button in the EventLog Analyzer Client UI Login screen. If you click the **Options >>** link, **Log on to** field will appear below the **Password** field. 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 avilable 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

Enter the **User Name** and **Password**. Select one of the three options in **Log on to** (**Local Authentication** or **Radius Authentication** or **Domain Name**). Click **Login** button to log in to EventLog Analyzer Client UI.

Active Directory Configuration Settings

Users in the AD (Active Directory) can be imported into EventLog Analyzer server. You have to select the required OUs (Organizational Units) under the Listed domains. You can re scan the network to find domains. Login to individual servers of the domain to get the OUs listed and select the OUs as per your requirement. Use the server credentials (User Name & Password) to login to the server. For the first time, all the users will be imported into EventLog Analyzer. On subsequent or periodic imports, only the new user added to the AD will be imported.

	The imported users will be added in the EventLog Analyzer server with the following constraints: **Access Level** as *Operator* and will have access to all the EventLog devices.

Procedure to configure AD settings

Click the **External Authentication Settings** link under the **Settings** tab to configure the AD user details import, periodic import, and to enable user authentication usage. On clicking the **Active Directory** tab, the **Active Directory Configurations** page opens up. In that page, you will find the following sections:

- Import users from Active Directory
- Schedule
- Authentication

Import users from Active Directory

In this section, you will find **Import Users** button. Click the button and **Import users from Active Directory** screen pops-up.
In that screen, you will find the following items:

- **Domain Name** combo box & **Rescan Network** link

  Domain Name combo box will list all the available domains in the network. Besides the combo box, you will find the **Rescan Network** link. Clicking the link will re scan the network to find out all the available domains. Select the domain from the combo box as per requirement.

- **Server Name**

  If you want to list the OUs of a particular server, enter the server name in the text box.

- **User Name**

- **Password**

  If you want to access a server and get list of (Organizational Units) OUs, enter the user name and password of the server in the text boxes.

- **Login & List OUs** button

  After entering the server name to be accessed and the credentials for server access, click this button to get the list of (Organizational Units) OUs.

- **Cancel** button

  If you want to cancel the access to server and get list of OUs operation canceled, click this button.

Schedule

In this section, you will find a check box to schedule the import of users periodically from AD and a Save button.

Select the "**Schedule AD import once in every __ days**" check box. Enter the periodicity of user import in days.

Click **Save** button to save the changes.

Authentication

In this section, you will find the status (**Status: Disabled**) of the AD authentication to be used for users imported from AD and Enable button.

Click **Enable** button to use AD authentication for the users imported from AD. On clicking the button the status will change to **Enabled** (**Status: Enabled**) and the **Enable** button will change to **Disable**.

RADIUS Server Configuration Settings

You can also leverage the RADIUS authentication for user access bypassing the local authentication provided by EventLog Analyzer.
In the RADIUS server authentication the users credentials are sent to the RADIUS server. The server checks for the user credentials and sends the authentication successful message to EventLog Analyzer server.

	Note: If the user has only RADIUS server authentication, create the user in EventLog Analyzer with dummy password. On user logging in with RADIUS server authentication, the dummy password in the local server is ignored and the user credentials are sent to RADIUS server for authentication. Refer the procedure given in the Adding Users document to add a new user with dummy passowrd.

You can make EventLog Analyzer work with RADIUS server in your environment. This section explains the configurations involved in integrating RADIUS server with EventLog Analyzer.

Procedure to configure RADIUS server settings

To configure RADIUS server in EventLog Analyzer, provide the following basic details about RADIUS server and credentials to establish connection:
Click the **External Authentication Settings** link under the **Settings** tab to configure the RADIUS server configuration. On clicking the **Radius Server** tab, the configuration fields are displayed. In that page, you will find the following fields:

RADIUS Server Settings	Description
Radius Server IP	The IP Address of the machine in which the RADIUS server is running. Enter the IP address of the host where RADIUS server is running
Radius Server Authentication Port	The port used by the RADIUS server for authenticating users. Enter the port used for RADIUS server authentication. By default, RADIUS has been assigned the UDP port 1812 for RADIUS Authentication.
Radius Server Protocol	The protocol used by the RADIUS server for authenticating users. Select the protocol that is used to authenticate users. Choose from four protocols: • **PAP** - Password Authentication Protocol • **CHAP** - Challenge-Handshake Authentication Protocol • **MSCHAP** - Microsoft Challenge-Handshake Authentication Protocol • **MSCHAP2** - Version 2 of Microsoft Challenge-Handshake Authentication Protocol
Radius Server Secret	The secret string used for connecting RADIUS client (EventLog Analyzer) with the server. Enter the RADIUS secret used by the server for authentication
Authentication Retries	The number of retries the RADIUS server to permit for authenticating users. Select the number of times you wish to retry authentication in the event of an authentication failure

Adding Different Users

Click the **User Management** link to create and manage the different users who are allowed to access the EventLog Analyzer server. You can also import users from Active Directory listing.

The different types of users and their respective privileges are described in the table below:

User	Description
Administrator	This user can do all operations including adding hosts/applications, setting up file archiving, adding additional users, and more.
Operator	This user can do all operations **except** adding new users, managing existing users, and importing Alert/Report/Filter profiles.
Guest	This user can only view real time logs and archives.

By default, an Administrator user with username as **admin** and password as **admin**, and a Guest user with username **guest** and password **guest** are already created.

If you have logged in as an Administrator user, the **User Management** page lists all the users created so far.

You can view the users based on user type. Select the user type from the **Select User Type** combo box. The three user types listed are: *Administrator*, *Operator*, and *Guest*.

You can view the users alphabet wise. **All** option and the alphabets are listed above the user list. Select **All** option or the alphabet under which the user login name will be available.

Viewing Login Details

If you have logged in as an Administrator user, click the User Audit **View** link against a user to view the corresponding user audits. The **User Audit** page shows the remote host IP address from which the user logged on, the timestamp of the login, and the duration of the session.

The description the user details available in the user list table are explained below:

User Detail	Description
User Name	The user's login name
No. of HostGroups	The number of host group(s) to which the user will be having access
Access Level	The access level privilege of the user
Domain Name	The domain in the network to which the user belongs to
User Audit	The corresponding user audits information

Delete

Select all users check box if you want to delete all the users and individual user(s) check boxes to delete the selected users. There is a check box against each user below the all user check box. Click **Delete** button to delete all the or selected user(s) from the list of users accessing EventLog Analyzer.

Assign Role

Select the users for whom the host group(s) need to be assigned/re-assigned. Select the

access level of the user from the **Access Level** combo box. The three access levels listed are: *Guest*, *Operator*, and *Administrator*. Click **OK** to save the new changes. Click **Cancel** to cancel assigning the role operation.

Assign Group(s)

Select the users for whom the host group(s) need to be assigned/re-assigned. Select the host group to which the user will be having access. All the available host groups are listed in the **Available HostGroup(s)** list. Select the host groups and click right arrow. The selected host groups are displayed in the **Selected HostGroup(s)** list. If you want to remove any host group from the **Selected HostGroup(s)** list, select the host groups and click left arrow. The removed host groups will be listed back in the **Available HostGroup(s)** list.

Adding a New User

- Click the Add New User link to add another user to access EventLog Analyzer.
- Enter the new user's login name in the User Name text box. The user name should be unique. If you want the user name as password, select the Use Login Name as Password check box.
- Enter the user's password in the Password text box. The password should be of 5 to 20 characters long.
- Re-enter the user's password in the Verify Password text box.
- Select the access level of the user from the Access Level combo box. The three access levels listed are: *Guest*, *Operator*, and *Administrator*.
- Enter default e-mail address the user in the Email Address text box.
- Select the host group to which the user will be having access. All the available host groups are listed in the Available HostGroup(s) list. Select the host groups and click right arrow. The selected host groups are displayed in the Selected HostGroup(s) list. If you want to remove any host group from the Selected HostGroup(s) list, select the host groups and click left arrow. The removed host groups will be listed back in the Available HostGroup(s) list.
- Click Add User to add this user to the list of users accessing EventLog Analyzer. Click Cancel to cancel the adding user operation.

Import AD Users

- Click the Import AD Users link to import the users from Active Directory in to EventLog Analyzer. On clicking the link Import users from Active Directory window pops up.
- In that window, select the Domain Name. If domains are not available rescan the network for domains by clicking the Rescan Network link.
- Enter AD server name in the Server Name field.
- Enter the user name of the AD server in the User Name field.
- Enter the password of the AD server in the Password field.
- Click Login and List OUs to fetch the Organizational Units from the domain. Click Cancel to cancel the operation.
- Choose the Organizational units from which you want to import.

Users will be imported with the following default values:
- **Access Level**: *Operator*

Host Group: *Windows Group*

To add AD users to the list of users accessing EventLog Analyzer.

Editing User Details

If you have logged in as an Administrator user, the **User Management** page lists all the users created so far.

- Click the **Edit** link to edit the user details. You can change the access level, password, and optionally, the default e-mail address for this user.
- You can edit the host groups associated with the user. Select the host group to which the user will be having access. All the available host groups are listed in the **Available HostGroup(s)** list. Select the host groups and click right arrow. The selected host groups are displayed in the **Selected HostGroup(s)** list. If you want to remove any host group from the **Selected HostGroup(s)** list, select the host groups and click left arrow. The removed host groups will be listed back in the **Available HostGroup(s)** list.
- Once you are done, click **OK** to save the new changes. Click **Cancel** to cancel editing the user operation.

OR

If you have logged in as an Operator or Guest user, click on the **Account Settings** link to change your password and default e-mail address.

Once you are done, click **OK** to save the new changes. Click **Cancel** to cancel editing the user operation.

Changing Account Settings

This option is visible only for users with **Guest** or **Operator** access level

Click the **Account Settings** link under the **Settings** tab to change the default password and e-mail address set for this account. You cannot change the account's user name or access level.

Once you have made the required changes, click OK **to save the changes. Click** Cancel **to return to the default** Settings **tab.**

EventLog Analyzer Configurations

EventLog Analyzer provides a facility to save the server and client configurations to use it for future restart.

This option is enabled only for users with **Admin** access level and not for **Operator** or **Guest** access level

Click the **ELA Configurations** link under the **Settings** tab to change the configured values or restore the default values and save the settings for future use.

Configurations	Default Values	Value Options	Description
View Per Page:	10	5, 10, 20, 25, 50, 75, 100, 150, 200	You can select the number of hosts to be displayed in the web client pages.
Low Disk Space Alert:	5 GB		You can enable or disable the Low Disk Space Alert. If you enable, an alert will be generated when the disk space availability of EventLog Analyzer Archive Logs and Log data falls below the set threshold. You can set the threshold value.
Direct Export Report Limit:	20000		The maximum number of records to be included in a directly exported report
Rows in Top N Reports:	10		You can set the number of rows to be displayed for reports under Top N Reports section.
Custom Report Record Limit	1000		The maximum number of records to be included in a Scheduled Custom Report
Compliance Report Record Limit:	500		The maximum number of records to be included in a Scheduled Compliance Report
Report Time Out:	25 mins		You can set the maximum time allowed to generate a report.
Attach Report As:	ZIP Report	PDF/CSV Report, ZIP Report	You can select the report format to be attached in Email.
Daily Mail Limit:	500		You can set the maximum permissible number of Email to be sent per day. You can enable or disable mail limit alert by selecting the **Enable / Disable Mail Limit Alert** check box.
Daily SMS Limit:	50		You can set the maximum permissible number of SMS messages to be sent per day.
Reporting Mode:	Send Mail	Send Mail, Save To Folder, Send Mail & Save To Folder	With this configuration you can configure the reports saved in any folder in the machine

Configurations	Default Values	Value Options	Description
			and/or send them as mail attachements. For **Save To** and **Send Mail & Save To Folder** options, you have to enter the location to save reports, in the text box besides the option combo box.

Click the **[Fill with default values]** link to restore the default value for the above configurations.

Once you have made the required changes, click **Save** button to save the settings changes. Click **Cancel** to return to the default **Settings** tab.

Configure Oracle Hosts in EventLog Analyzer

Configure hosts for which you want to monitor oracle logs under **Settings** > **ELA Configurations** > **Configure Oracle Hosts**. Enter the Oracle host name in the **Add Host** text box and click the save icon to save the Oracle host. Below the text box, the existing Oracle hosts will be listed.

After Configuring Hosts in EventLog Analyzer, carry out the configuration given below in Oracle server

For Oracle server installed in Windows platform

connect to sqlplus

- Change audit parameter using below query
  ALTER SYSTEM SET AUDIT_TRAIL=*OS* **SCOPE**=*SPFILE;*
- Restart the Oracle server to get the changes effected.

For Oracle Server installed in Unix platform

To enable Oracle syslog auditing, follow the procedure given below:

1. Assign a value of OS to the **AUDIT_TRAIL** initialization parameter, as described in '**Enabling or Disabling the Standard Audit Trail**'
   For example: **ALTER SYSTEM SET AUDIT_TRAIL**=*OS* **SCOPE**=*SPFILE*;;
2. Manually add and set the **AUDIT_SYSLOG_LEVEL** parameter to the initialization parameter file, **initsid.ora**.

   Set the **AUDIT_SYSLOG_LEVEL** parameter to specify a facility and priority in the format *AUDIT_SYSLOG_LEVEL=facility.priority*.

   facility: Describes the part of the operating system that is logging the message. Accepted values are user, local0–local7, syslog, daemon, kern, mail, auth, lpr, news, uucp, and cron.

   The local0–local7 values are predefined tags that enable you to sort the syslog message into categories. These categories can be log files or other destinations that the syslog utility can access. To find more information about these types of tags, refer to the syslog utility MAN page.

priority: Defines the severity of the message. Accepted values are notice, info, debug, warning, err, crit, alert, and emerg.
The syslog daemon compares the value assigned to the facility argument of the **AUDIT_SYSLOG_LEVEL** parameter with the **syslog.conf** file to determine where to log information.

For example, the following statement identifies the facility as local1 with a priority level of warning:
AUDIT_SYSLOG_LEVEL=*local1.warning*

See Oracle Database Reference for more information about **AUDIT_SYSLOG_LEVEL**.

3. Log in to the machine that contains the syslog configuration file, **/etc/syslog.conf**, with the superuser (root) privilege.

4. Add the audit file destination to the syslog configuration file **/etc/syslog.conf**.

   For example, assuming you had set the **AUDIT_SYSLOG_LEVEL** to *local1.warning*, enter the following:

   local1.warning /var/log/audit.log

   This setting logs all warning messages to the **/var/log/audit.log** file.

5. Restart the syslog logger:
   $/etc/rc.d/init.d/syslog restart

   Now, all audit records will be captured in the file **/var/log/audit.log** through the syslog daemon.
6. Restart the Oracle server so that changes are effected.

Reference:

http://download.oracle.com/docs/cd/B28359_01/network.111/b28531/auditing.htm#CEGBIIJD

Setting up the Mail Server

You need to configure the mail server in order to email alert notifications and scheduled reports.

Click the **Mail Server Settings** link to edit the mail server settings. Enter the following details:

Field	Description
Outgoing Server Name	Enter the name of the SMTP server on your network which is used for outgoing emails.
Port	Enter the port used by the SMTP server. Usually this is 25.
Authenticate for every Login	If your SMTP server requires you to authenticate yourself before sending an email, check this option. Otherwise leave it unchecked. *The below two fields are active only when this checkbox is checked.
User Name*	Enter the user name used to authenticate email sending from this machine.
Password*	Enter the corresponding password for the typed user name.
Use Secure Connection	Select the **TLS** button to secure the connection between mail server and ELA server. Select **No** button if secure connection is not required.
Sender Address	Enter the Sender or From Address which needs to be mentioned in the outgoing emails. By default, *eventlogreport@localdomain.com* will be mentioned as the sender address.
Send a test message	The **Send a test message** button is for testing the mail server configurations. You can give your email-id in the "To" field, which comes-up when you click Send a test message, and click **Send**. If the mail server configurations have been given correctly you will receive a Test Mail. You will receive two test mails. One mail with Test.zip as attachment (this is to test whether the mail server allows zip file attachments) and other mail is plain without attachment.

After all the details have been filled in, click **Save** to save the mail server settings.

- If you want to send secured emails, you can use the **Use Secure Connection** option. The **Transport Layer Security (TLS)** option uses public key encryption to send the email to untrusted networks. For more information on Transport Layer Security (TLS) refer the URL: http://en.wikipedia.org/wiki/Transport_Layer_Security. Also refer the link to know about TLS http://technet.microsoft.com/en-us/library/cc784450%28WS.10%29.aspx
- If the mail server has not been configured, you will see an error message next to the **Mail To** box wherever e-mail options are available. Click the link inside the error message to enter the same details as above in the popup window that is opened.

Setting up SMS Port

The SMS setting is similar to Mail Server setting. You need to configure the SMS settings in order to get SMS alert notifications in your cellular phone.

	This option is enabled only for users with **Admin / Operator** access privileges.

Click the 

SMS Settings link under the **Settings** tab to configure the port in which the SMS equipment is connected and mobile phone number to test the functioning of port.

On clicking the link, SMS Settings screen open up on the right hand side.

In that you will see **GSM Communication Port Name** text box and **Test Port** button.

- Enter the communication port name (For example: **COM1**) in the text box.
- Click the **Test Port** button.
- On clicking the button, a window pops-up to enter phone number to test port.
- Enter mobile phone number with '+' sign and country code (For example: +19259249500).
- Click **OK** button. If the port & SMS equipment is functioning properly, you will get a test message on the phone. Click **Cancel** button to abort the testing.

Once you have entered the required port number and tested it, click **Save Changes** to save the changes. Click **Cancel** to return to the default **Settings** tab.

	The phone number entered in the pop-up screen is meant only for testing the SMS port. Phone numbers to which the Alerts are to be SMS notified need to be configured in individual Alert profiles.

Viewing Server Diagnostics

Click the **Server Diagnostics** link to see server-specific device information. This information will be useful while troubleshooting the server or reporting a problem.

The various information boxes on this page are described in the table below:

Box	Description
License Information	This box shows details about the license that is currently applied.
System Information	This box shows device information for the EventLog Analyzer server
Installation Information	This box shows details about the EventLog Analyzer installation on the server machine
JVM Memory Information	This box shows statistics on the amount of memory used by the JVM

Configuring Email Alert for EventLog Analyzer Failure

This option is enabled only for users with **Admin/Operator** access privileges.

EventLog Analyzer lets you configure Email alert to user(s), in case of (Log Collector) EventLog Analyzer goes down. Email alert can be configured to multiple Email IDs. You can also configure Email alert to user(s), in case of EventLog Analyzer not receiving logs from specific host(s).

EventLog Analyzer comes with a new feature to get all the logs which were not collected during the log collector application down time.

Configuring Email Alert for EventLog Analyzer Failure

Click the **Alert Me** link to configure Email alert. You can find this link on the **Admin Settings** section of the **Settings** tab.

1. On clicking the **Alert Me** link, the **Alert when EventLog Analyzer stops collecting data** window pops-up.
    a. Enter the subject of Email in the **Subject** field.
    b. Enter the e-mail address in the **MailID** field. Enter multiple Email IDs as comma-separated values.
2. Click **Submit** to set up the Email alert. Click **Close** to close the window.
3. You can disable this alert. After clicking the **Submit** button or if the alert is already configured, the **Disable this alert** check box appears below the **E-Mail** field. Select the check box.
4. If you have not yet configured the mail, the '*Mail Server is not configured*' message along with the **Configure Mail Server** link appears. Click the link to configure the mail server settings in the popup window that is opened.
5. If the mail server has been already set up, the mail server settings are displayed and you can reconfigure the mail server settings by click the **Reconfigure the Mail Server** link in the popup window that is opened.

Configure Alert on failure to receive logs from hosts

Click the **Alert** link to configure Email alert. You can find this link in the **Alert Me** screen of **Admin Settings** section of the **Settings** tab.

1. On clicking the **Alert** link, the **Configure Alert on failure to fetch logs from hosts** window pops-up.
    a. Select the host or host group from the **Select Host/Group:** section.
    b. Enter the time interval of alert generation in the **Interval** field and select the time unit (**minutes/Hrs/Days**) from the combo box besides.
    c. Enter the subject of Email in the **Subject** field.
    d. Enter the e-mail address in the **MailID** field. Enter multiple Email IDs as comma-separated values.
2. Click **Submit** to set up the Email alert. Click **Close** to close the window.

3. You can disable this alert. After clicking the **Submit** button or if the alert is already configured, the **Disable this alert** check box appears below the **Email**

Address field. Select the check box.

4. If you have not yet configured the mail, the '*Mail Server is not configured*' message along with the **Configure Mail Server** link appears. Click the link to configure the mail server settings in the popup window that is opened.
5. If the mail server has been already set up, the mail server settings are displayed and you can reconfigure the mail server settings by click the **Reconfigure the Mail Server** link in the popup window that is opened.

Accessing the Database

EventLog Analyzer lets advanced users access the in-built database and run standard queries.

2. Click the **Database Console** link to open the Database Console window. In the prompt window displayed, enter the query to be executed.
3. Click **Execute Query** button. The **only** database queries allowed are: *SELECT* and *SHOW*.
4. Click **Close** button to close the Database Console window.

Remember the following when executing a query:

5. Table names and Table column names are **Case sensitive**
6. Set Row limit between 1 and 500 for select queries.
7. Default Row limit is set to 10.

Tips and Tricks

Frequently Asked Questions

For the latest list of Frequently Asked Questions on EventLog Analyzer, visit the FAQ on the website or the public user forums.

General Product Information [Show / Hide All]

1. What is the difference between the Free and Professional Editions?

   The Free Edition of EventLog Analyzer is limitehd to handling event logs from a maximum of five hosts (only hosts and no applications), whereas the Professional Edition can handle event logs from any number of hosts/applications, you have purchased license for. There is no other difference between the two editions, with respect to features or functionality.

2. Is a trial version of EventLog Analyzer available for evaluation?

   Yes, a 30-day free trial version of EventLog Analyzer Premium Edition, can be downloaded from the website at http://www.eventloganalyzer.com/

3. Does the trial version have any restrictions?

   The trial version is a fully functional version of EventLog Analyzer Premium Edition. When the trial period expires, EventLog Analyzer automatically reverts to the Free Edition.

4. Do I have to reinstall EventLog Analyzer when moving to the fully 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.

5. 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 from Windows and Unix hosts. If installed on a Unix machine, EventLog Analyzer can collect event logs only from Unix hosts. Also Windows Event Logs can be collected in this case as SysLog forwards like Snare.

6. I don't want to collect or report on actual event logs. Can I still use this product?

   You can still use EventLog Analyzer to simulate event logs and see how reports will look like when real-time data is used. Click the **Simulate** link in the **Settings** tab to begin sending sample event logs to EventLog Analyzer.

7. 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.

8. 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.

9. Can EventLog Analyzer collect logs if dcom is disabled on remote systems?

   No. EventLog Analyzer cannot collect logs if dcom is disabled on remote systems.You need to ensure that dcom is enabled in remote windows servers for the logs to get collected and shown in EventLog Analyzer.

10. How do I buy EventLog Analyzer?

    You can buy EventLog Analyzer directly from the ZOHO Corp. Online Store, or from a reseller near your location or send a mail to ManageEngine Sales Team. Please see the website at http://www.eventloganalyzer.com/ for more information on purchasing options.

11. 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. To convert the message you have to use separate third party tool. Please mail us to eventlog-support@manageengine.com for the steps, if required.

Installation [Show / Hide All]

1. What are the recommended 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
   * Disk Space - 100MB

   - RAM - 512MB
     * Operating System - Windows 2000/XP/Vista, 2003 Server, 2008 Server, Linux 8.0/9.0
     * Web Browser - Internet Explorer 5.5 and later, Netscape 7.0 and later, Mozilla 1.5 and later

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

2. 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.

3. 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.

4. 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 collected, follow the procedure given below:

   For MySQL: You can run the database backup utility, **BackupDB.bat / .sh** present in the <*EventLog Analyzer_Home*>/*troubleshooting* directory.

   For MSSQL: You can use appropriate third party application.

5. How to take database backup?

   MySQL database

   To take a backup of the existing EventLog Analyzer **MySQL database**, 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:

   a. 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
```

6. 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\eventlog_log.LDF**) 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:

8. Stop the EventLog Analyzer application.
9. Execute the following command in the command prompt window in the *<EventLog Analyzer Home>\bin* directory.

   service.bat -i

10. 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:

11. Stop the EventLog Analyzer application.
12. Execute the following command:

    sh configureAsService.sh -i

13. 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

1. **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 isrunning, and that it is using the same port number specified here.)

2. 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** page. Click the **View** link under User Audit against each user to view the active session information and session history for that user. Look up User Management for more information on users in EventLog Analyzer.

3. 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.

4. 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.
   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 process manually if any 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\`
      - The folder, `Archive` located under `EventLog Analyzer Home\archive`

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

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

7. In the newly installed EventLog Analyzer machine/server, rename the folder **MySQL** located under `EventLog Analyzer Home\` as **OldMySQL**.

8. 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.

9. Copy the **StartDB.bat** file, which is located under `EventLog Analyzer Home\bin`, from the old machine/server to the newly installed Eventlog Analyzer machine/server.

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

In-case of any issues while performing the above steps, please do not continue any further and contact eventloganalyzer-support@manageengine.com to assist you better.
How to monitor Oracle Audit Logs?

14. Add the host (in which the Oracle server is installed) to ELA server.
15. If Oracle is installed in Linux, configure to forward syslogs to ELA server.
16. Carryout the configuration as given in the link below:
Configure Oracle Hosts in EventLog Analyzer

Reporting

1. **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. If otherwise, check the event filters applied. If no event logs are generated with the specified event filters, graphs will not show any data.

2. 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. Reports that are scheduled to run automatically, or be emailed automatically, are generated as CSV or PDF files.

Troubleshooting Tips

For the latest Troubleshooting Tips on EventLog Analyzer, visit the Troubleshooting Tips on the website or the public user forums.

General

1. 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.

2. I find that EventLog Analyzer keeps crashing or all of a sudden stops collecting logs. What could be the reason?

   Make sure that the EventLog Analyzer installation folder 'ManageEngine' is not accessed by other applications. Kindly exclude the 'ManageEngine' directory (it could be in *C:\ManageEngine* or *D:\ManageEngine*) from both the Backup process and Anti-Virus Scans. It is possibile that the inbuilt mysql database of EventLog Analyzer could get corrupted if other processes are accessing these direct

3. How to create SIF (Support Information File) and send the file to ZOHO Corp., 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:\ME\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

4. 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/regsvr32.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, contact eventloganalyzer-support@manageengine.com
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

1. 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 <*EventLog Analyzer Home*>*bin***runSEC.bat / 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:

  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

1. 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.

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.
   Probable cause: The default web server port used by EventLog Analyzer is not free.
   Solution: Kill the other application running on port 8400. If you cannot free this port, then change the web server port used in EventLog Analyzer.

3. 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.
   - The one or more internally used ports 5000, 5001, 5002 may not be free.

   Solution:
   - Check for the process that is occupying the syslog listener port or internally used port, using **netstat -anp udp** . And if possible, try to free up this port. t.
   - 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..

4. 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

1. 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.

2. 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
     ```

3. 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:

   - In Add or Remove Programs, click **Add/Remove Windows Components**.
   - In the Windows Components Wizard, select **Management and Monitoring Tools**, then click **Details**.
   - In the Management and Monitoring Tools dialog box, select **WMI Windows Installer Provider** and then click **OK**.
   - Click **Next**.

4. 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

5. 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

1. I've added a host, but EventLog Analyzer is not collecting event logs from it
   Probable cause: You do not know whether the logs are sent from the host machine (Only for Syslog sources)

   Solution: If you want to find out whether the syslog packets are being sent by the host (source) to the EventLog Analyzer (destination) at the configured port, click the **Syslog Viewer** icon in the **Sub-Tab** and you can mention the Host IP Address (by default it is 'Any') and syslog port of this hosts (by default it '513','514') and click **Apply Filter**. With the filter applied, you can find out whether the raw log packets are sent from the specific host to EventLog Analyzer server in real time.

   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.

2. 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	Cause	Solution

Error Code	Cause	Solution
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: Select **Start > Run** Type `dcomcnfg` in the text box and click **OK** Select the **Default Properties** tab Select the **Enable Distributed COM in this machine** checkbox Click **OK** To enable DCOM on Windows XP hosts: Select **Start > Run** Type `dcomcnfg` in the text box and click **OK** Click on **Component Services > Computers > My Computer** Right-click and select **Properties** Select the **Default Properties** tab Select the **Enable Distributed COM in this machine** checkbox 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	Move the user to the Administrator Group of the workstation or scan the machine using an administrator (preferably

Error Code	Cause	Solution
	scanning operation. Probably, this user does not belong to the Administrator group for this host machine	a Domain Administrator) account.
0x800706ba	A firewall is configured on the remote computer. Such exceptions mostly occur in Windows XP (SP 2), when the default Windows firewall is enabled.	Disable the default Firewall in the Windows XP machine: Select **Start > Run** Type `Firewall.cpl` and click **OK** In the **General** tab, click **Off** Click **OK**

3. 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
   ```
   After scanning, you can disable Remote Administration using the following command:
   ```
   netsh firewall set service RemoteAdmin disable
   ```

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 propelrly.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 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:

17. 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).
18. Connect MS SQL client (using **Microsoft SQL Server Management Studio**) and execute the below query:

    sp_dboption 'eventlog', 'trunc. log on chkpt.', 'true'

    To execute the query, select and highlight the above command and press **F5** key.

19. After executing the above command, select and highlight the below command

and press **F5** key to execute it.

DBCC SHRINKDATABASE (eventlog)

20. **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.

For any other issues, please contact EventLog Analyzer Technical Support.

Other Tools and Utilities

Working with 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.

	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

Stop the server, if it is running, and follow the steps below to enable SSL support:

Generating a valid certificate

1. 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**"
2. If you do not have the keystore file, please follow the steps to create the same.
   - Open <*EventLog Analyzer Home*>*server**default**conf* directory and execute the following command in the command prompt.
     "<EventLog Analyzer Home>\jre\bin\keytool" -genkey -alias tomcat -keyalg RSA -keystore chap8.keystore
   - During the execution of the above command, it will prompt you for keystore password, enter "rmi+ssl" as password. See Note below.
   - It will also prompt for 5 questions on first and last name, organizational unit, organization, city, state, country code.
   - Fill in the fields and for confirmation type '**y**' and press '**Enter**'
   - Again press '**Enter**' for password for tomcat.
     A file named '**chap8.keystore**' will be created in the <*EventLogAnalyzer Home*>*server**default**conf* directory.

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:

```
<!-- A HTTP/1.1 Connector on port 8080 -->
<Connector port="8080" address="${jboss.bind.address}"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" redirectPort="8443" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true"/>
```

Enabling SSL

1. In the same file, enable the HTTPS connection parameters, by removing the <!-- tag before, and the --> tag after the following lines:

```
<!--
<!-- 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" />
-->
```

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**.

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:

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"/>
```

Verifying SSL Setup

1. Restart the EventLog Analyzer server.
2. Verify that the following message appears:
   Server started.
   Please connect your client at http://localhost:8400
3. Connect to the server from a web browser by typing https://<*hostname*>:8443 where <*hostname*> is the machine where the server is running.

Configuring 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 vesion and CPU type of EventLog Analyzer machine.

MSSQL 2005 (32 bit)
http://download.microsoft.com/download/4/4/d/44dbde61-b385-4fc2-a67d-48053b8f9fad/sqlncli.msi

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

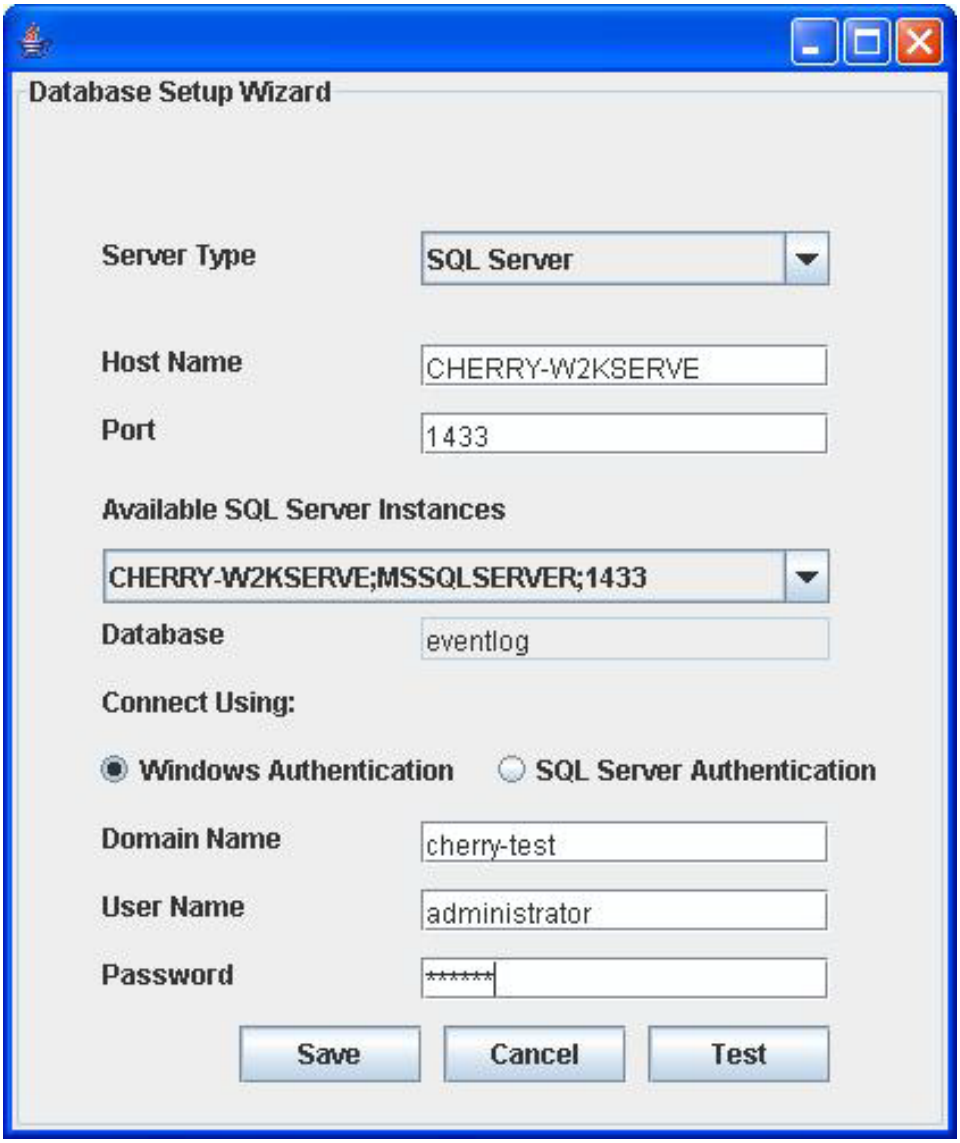
MSSQL 2008 (64 bit)
http://go.microsoft.com/fwlink/?LinkId=123718&clcid=0x409

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:

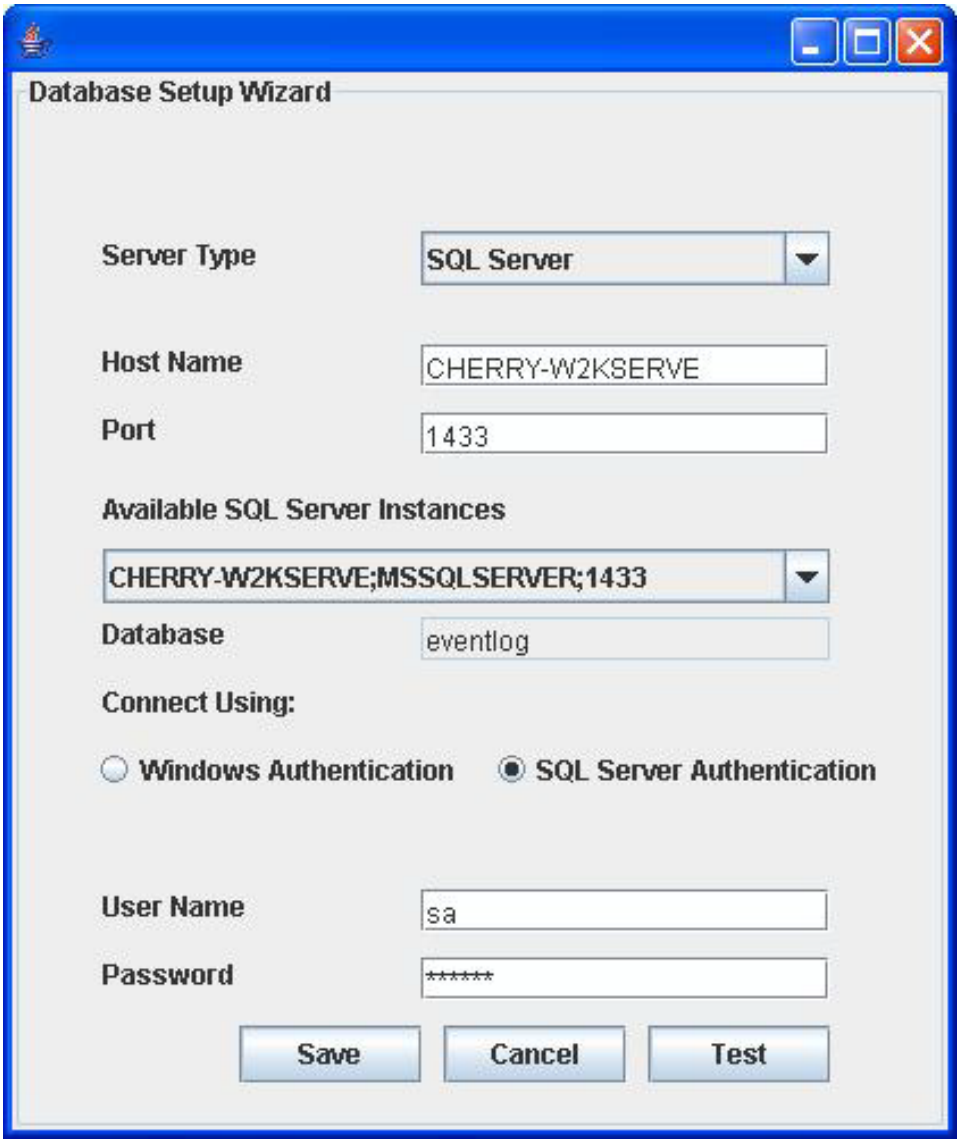
a. Windows Authentication

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**.



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. Clcik **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.

Migrating 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-registerd 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 vesion and CPU type of EventLog Analyzer machine. **MSSQL 2005 (32 bit)** http://download.microsoft.com/download/4/4/d/44dbde61-b385-4fc2-a67d-48053b8f9fad/sqlncli.msi **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

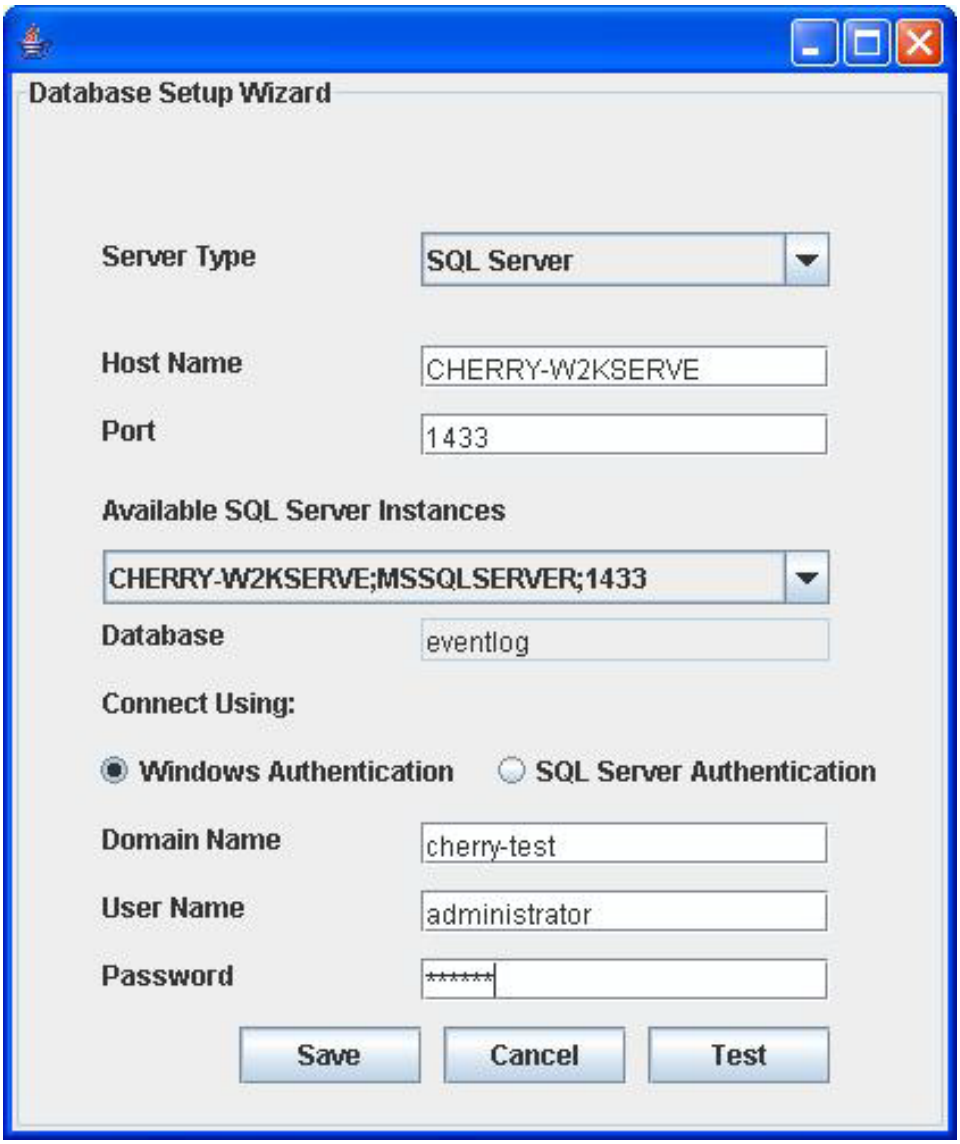
4. Invoke the *<Eventlog Analyzer Home>\tools***changeDBServer.bat** in command

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:

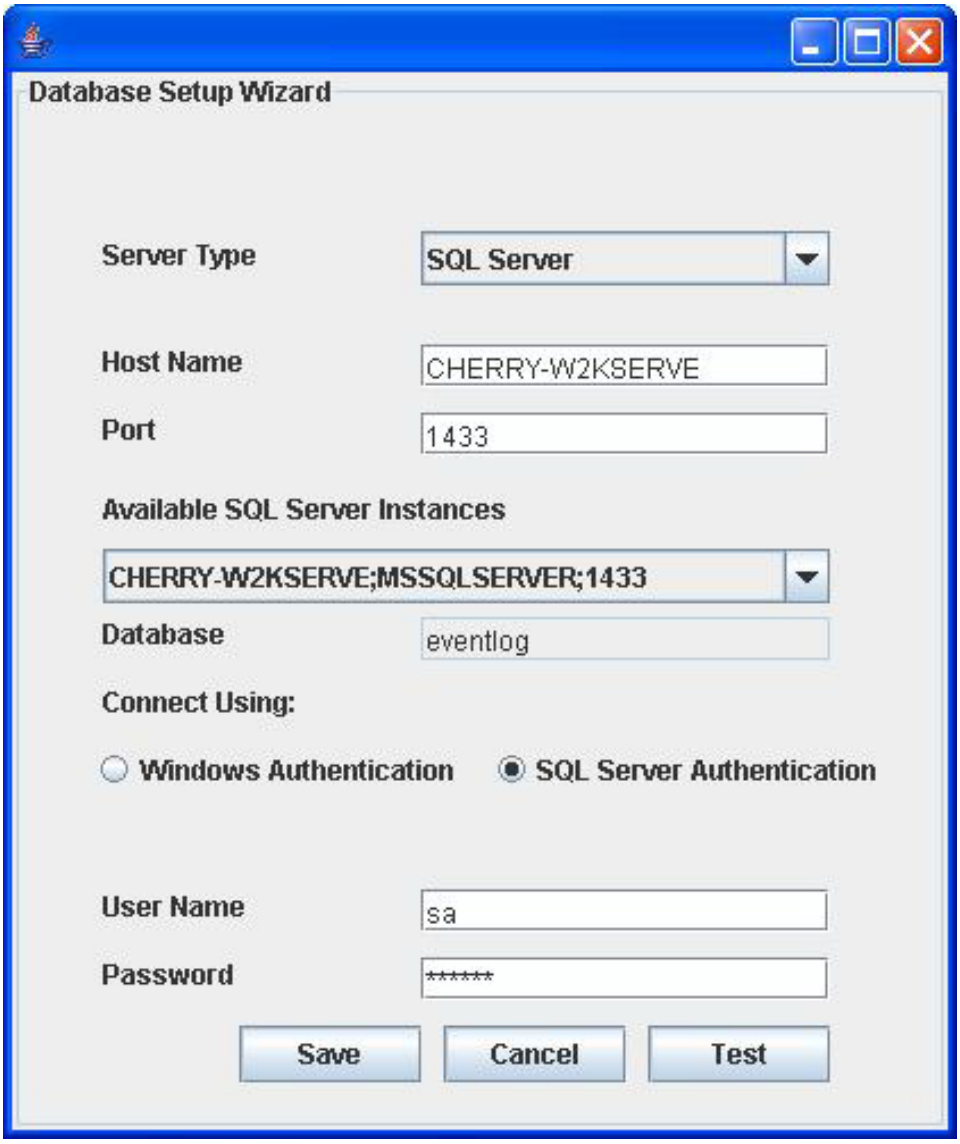
   a. Windows Authentication

   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.

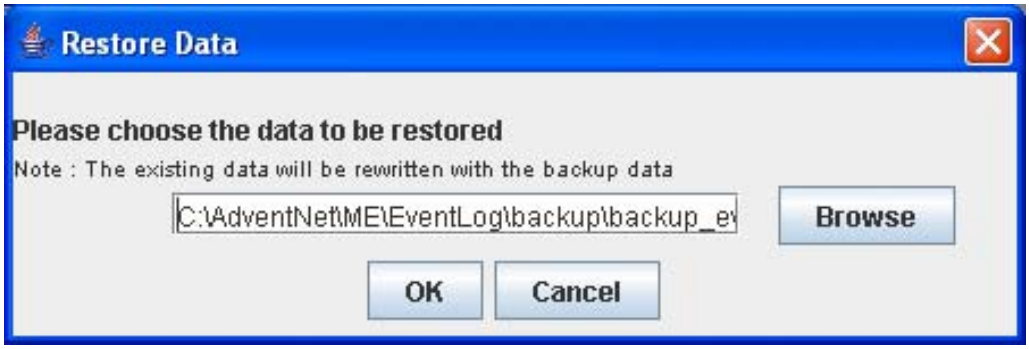


   b. SQL Server Authentication

   For SQL Server Authentication, enter the **User Name** and **Password**.



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.



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.

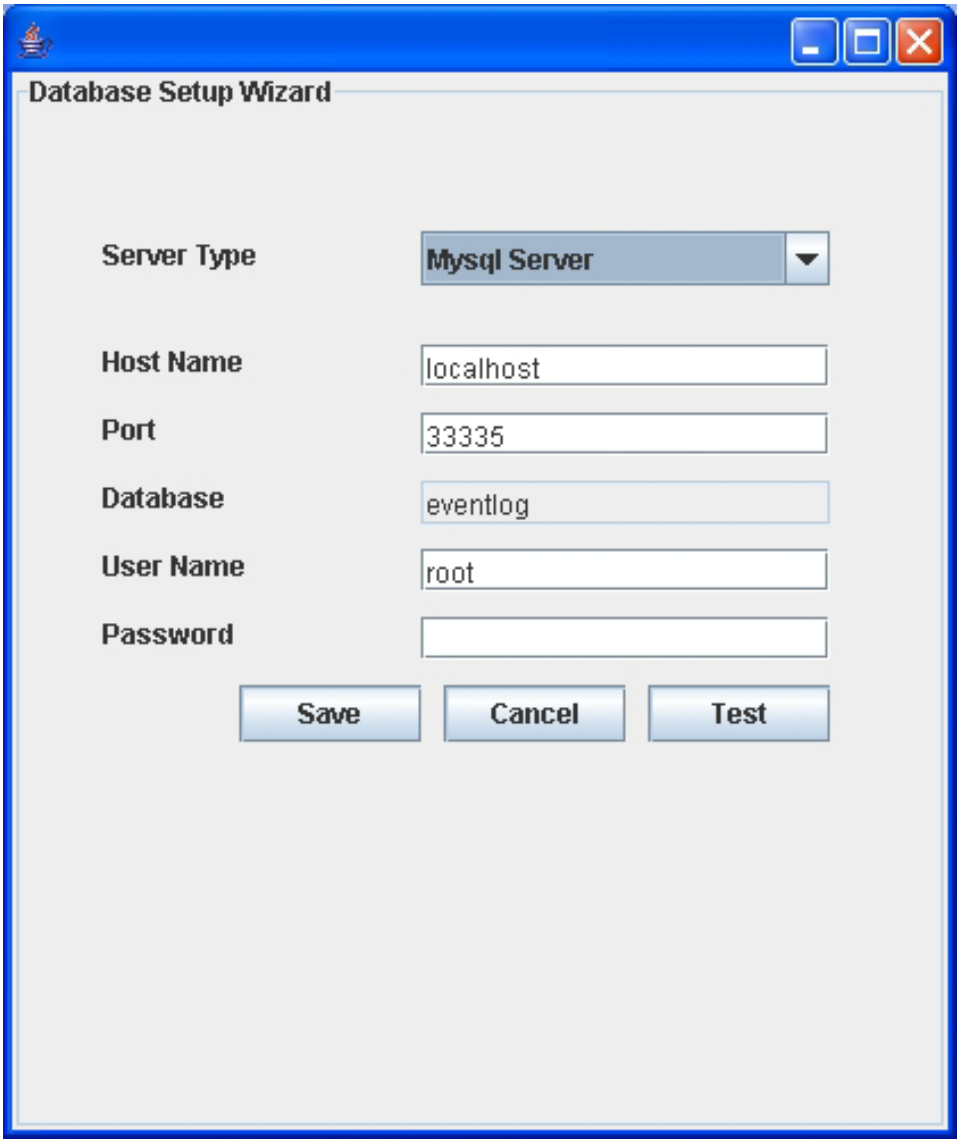
	You can also change the backup directory. Execute the batch file to backup by passing the absolute path of the directory as argument in the command prompt. Example command execution as follows: *<Eventlog Analyzer Home>\tools:\>***backUpDatabase.bat *D:\Mysql***

Migrating EventLog Analyzer Data from MSSQL to MySQL Database

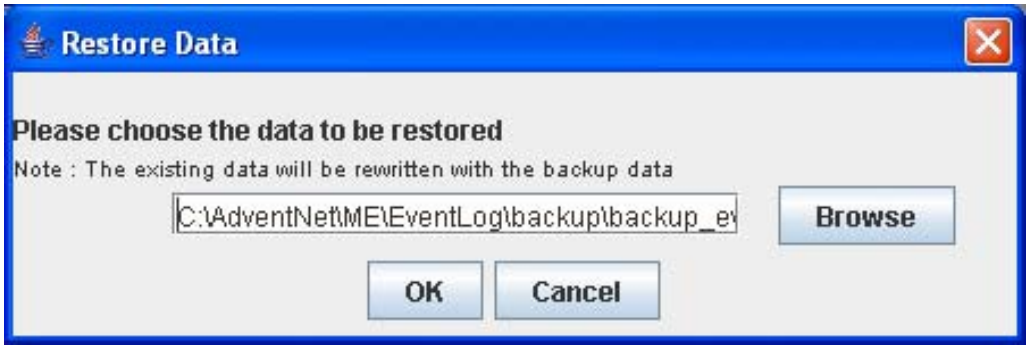
EventLog Analyzer lets users to migrate the existing EventLog Analyzer data available in MSSQL database to MySQL database.

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**.



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 MySQL Server configuration. Note that, it will take few minutes to configure the settings of the MySQL database.
9. Run *<Eventlog Analyzer Home>\bin***stopDB.bat** in command prompt.
10. Invoke the *<Eventlog Analyzer Home>\bin***run.bat** to start the Eventlog Analyzer server in **command prompt**.
11. 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**
12. 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.

12. Start the Eventlog Analyzer Server/Service to work with the MySQL as the database.

	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***

Moving EventLog Analyzer's database to different directory in the same server

To move the Eventlog Analyzer's Indexes to a different drive / directory on the same server

21. Go to **Archive Settings** page.
22. Enable **Change Raw Logs Indexing Location** check box.
23. Modify the Log Indexing Location to the new location and save.

24. Move all the directories from previous location to the new location.

To move the Eventlog Analyzer's 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
```

8. Start the Eventlog Analyzer Server/Service.

Moving EventLog Analyzer Server installation to another server

To move the Eventlog Analyzer's 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.

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.

	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.

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 precautionery 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.

Please make sure that the Eventlog Analyzer installation in the previous is migrated to the latest vesion, 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.

Please make sure 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.

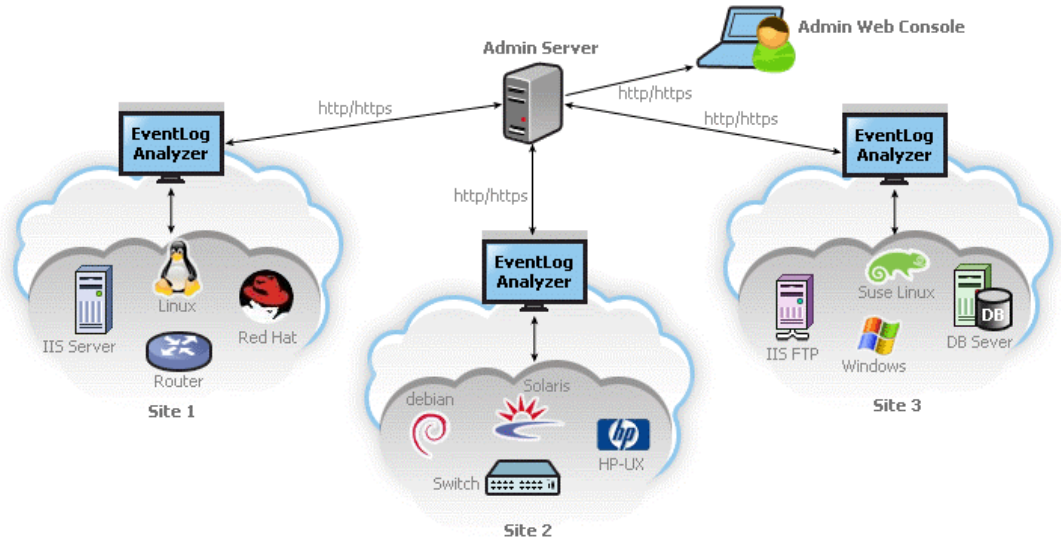
5. Start the Eventlog Analyzer server/service on the new machine and check whether the data and the configurations are intact.

Distributed Edition - Managed Server Introduction - EventLog Analyzer 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 through out 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:

25. Aggregated log management of whole enterprise in different physical locations.
26. Scalable architecture supporting 1000s of hosts.
27. Centralized monitoring using single console view.
28. Secured communication using HTTPS.
29. 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 eventloganalyzer-support@manageengine.com

Installing and Uninstalling - EventLog Analyzer Distributed Edition Managed Server

EventLog Analyzer is available for Windows and Linux platforms. For more information on supported versions and other specifications, look up System Requirements.

This topic covers the following procedures:

- Installing EvntLog Aanalyzer
  - Windows
  - Linux
- Uninstalling EventLog Analyzer
  - Windows
  - Linux

Installing EventLog Analyzer

Windows:

The EventLog Analyzer Windows download is available as an EXE file at http://www.eventloganalyzer.com/download.html

Double-click the downloaded EXE file, and follow the instructions as they appear on screen.

	1. Ensure that the Distributed Edition - Admin Server, you intend to connect this Managed Server, is running. 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.

30. Click **Advanced Install** button.
31. Read the *License Agreement* and click **Yes** button.
32. Select **Distributed Edition** and click **Next** button.
33. Select **Managed Server** and click **Next** button.
34. 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, select **Use a Proxy Server to contact Admin Server** check box. Configure the **Proxy Server Host**, **Proxy Server Port**, **User Name**, and **Password** details. Click **Next** button.
35. Select **Destination Folder** using **Browse** button, for installation. Click **Next** button.
36. Retain or modify the Web Port of Managed Server and select the Language of Installation from the combo box. Three languages are supported for installation and they are Chinese, English, and Japanese. By default English is selected. Click **Next** button.
37. Select **Install EventLog Analyzer as service** check box (recommended), if you want to install Managed server as a service. Click **Next** button.
38. Configure new Program Folder or retain the default. Click **Next** button.
39. The installation details like Installation Directory, Program Folder, and Web Port are displayed. Click **Next** button.
40. Now, Distributed Edition - Managed server installation is complete.

Once the installation is complete you will notice a  tray icon, which provides you with

the following options.

Option	Description
EventLog Server Status	This option provides you details like *Server Name*, *Server IpAddress* , *Server Port*, *Server Status*.
Start WebClient	This option will open up your default browser and connect you to the web login UI of EventLog Analyzer Server, provided the server has already been started.
Shutdown Server	This option will shutdown the EventLog Analyzer Server.

The  tray icon option is only available for Windows !

Linux:

The EventLog Analyzer Linux download is available as a BIN file at http://www.eventloganalyzer.com/download.html

1. Download the BIN file, and assign **execute** permission using the command:
   `chmod a+x <file_name>.bin`
   where <*file_name*> is the name of the downloaded BIN file.
2. Execute the following command: `./<file_name>Bin`

During 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>`

Follow the instructions as they appear on the screen.

1. Ensure that the Distributed Edition - Admin Server, you intend to connect this Managed Server, is running.

Ensure that you configure the Admin Server details correctly during the Managed Server installation procedure. Otherwise, the Managed Server installation will be incomplete.

41. Click **Advanced Install** button.
42. Read the *License Agreement* and click **Yes** button.
43. Select **Distributed Edition** and click **Next** button.
44. Select **Managed Server** and click **Next** button.
45. In Managed Server Configuration, enter **Admin Server Host**, retain or modify **Admin Server Port**, select or unselect **HTTPS** check box as per requirement. If the Managed Server is behind Proxy Server, select **Use a Proxy Server to contact Admin Server** check box. Configure the **Proxy Server Host**, **Proxy Server Port**, **User Name**, and **Password** details. Click **Next** button.
46. Select **Destination Folder** using **Browse** button, for installation. Click **Next** button.
47. Retain or modify the Web Port of Managed Server and select the Language of Installation from the combo box. Three languages are supported for installation and they are Chinese, English, and Japanese. By default English is selected. Click **Next** button.
48. Select **Install EventLog Analyzer as service** check box (recommended), if you want to install Managed server as a service. Click **Next** button.
49. Configure new Program Folder or retain the default. Click **Next** button.
50. The installation details like Installation Directory, Program Folder, and Web Port

are displayed. Click **Next** button.

51. Now, Distributed Edition - Managed Server installation is complete.

This will install EventLog Analyzer on the respective machine.

Uninstalling EventLog Analyzer

Windows:

1. Navigate to the Program folder in which EventLog Analyzer has been installed. By default, this is **Start > Programs > ManageEngine EventLog Analyzer 6** .
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.

	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.

Troubleshooting Tips - EventLog Analyzer Distributed Edition Managed Server

For the latest Troubleshooting Tips on EventLog Analyzer, visit the Troubleshooting Tips on the website or the public user forums.

For any other issues, please contact EventLog Analyzer Technical Support.

Ask ME

Using Ask ME

The **Ask ME** 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.

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 tab shows a series of questions. In Step 1, select the area of interest - login/logoff, users, alerts, etc. If you are not sure, leave it to the default **All Questions** option.

In Step 2, select the appropriate question for which you need an answer. Then click on **Get the Answer**.
The report corresponding to the question selected is now generated and displayed.

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.

With the enhancement of this feature, you can add the custom questions dynamically under this tab. Select the custom question you have added and click **Get the Answer**.
The report corresponding to the custom question will be generated and displayed.

Adding Custom Questions in Ask ME

The **Ask ME** 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.

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

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.
   a. 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.
   b. To get the URL of the custom report:
      i. Select the custom report in the Web Client UI.
      ii. Copy the URL shown in the Address Bar of the browser.
      iii. 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 '**&**' in the copied "link" tag.

   Example entry for "Question" and "link" tags are given below:

   <Question>How many times objects and folders are accessed in the hosts added?</Question>

   <link>index2.do?url=topreport_details&RBBNAME=Compliance_ObjectAccess&tab=askCherry&rtype=toprep&TC=10</link>

   c. Save the file

Refresh the Web Client Ask ME tab. You will see the new question added is lised 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.

	Ensure that you add the new questions after the existing questions. Do not disturb the existing 17 questions.

Contacting Technical Support

The **Support** tab gives you a wide range of options to contact the Technical Support team in case you run into any problems.

Link	Description
Request Technical Support	Click this link to submit a form from the EventLog Analyzer website, with a detailed description of the problem that you encountered
Create Support Information File [SIF]	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 eventlog-support@manageengine.com or upload the ZIP file to our ftp server by clicking on Upload to **FTP Server**, in the pop-up window provide your E-Mail id and browse for the zipped SIF file and then press Upload.
Reset LogCollector	Is used for running EventLog Analyzer in the debug mode. Please contact eventlog-support@manageengine.com before invoking Reset LogCollector.
Troubleshooting Tips	Click this link to see the common problems typically encountered by users, and ways to solve them
Need a Feature	Click this link to submit a feature request from the EventLog Analyzer website
Log Level Setting	Click this link to set the granualarity level of server logs to be stored in the log files
Toll-free Number	Call the toll-free number +1 888 720 9500 to talk to the EventLog Analyzer Technical Support team directly
User Forums	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
Join Meeting	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
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.

The Support tab also displays the latest announcements and discussions in the EventLog Analyzer user forum

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

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 **Support** tab.
- Click the **Create Support Information File** link show in that page.
- Wait for 30-40 Secs and again click the **Support** tab.
- 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 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 eventloganalyzer-support@manageengine.com before invoking Reset LogCollector.

Log Level Setting

The Log Level Setting is used for setting the granualarity 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 loogeres, 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
6. com.adventnet.la.HtmlTimePack
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
12. com.adventnet.la.ReportDS
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
24. com.adventnet.la.util.ResourceCheckerUtil
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.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
48. com.adventnet.la.ReportUtil
49. com.adventnet.sa.webclient.AddScheduleActionSa
50. com.adventnet.sa.webclient.ViewReport
51. com.adventnet.sa.webclient.util.SaUtil
52. com.adventnet.sa.webclient.EditFilterAction
53. com.adventnet.sa.util.dm.LuceneIndexProcessor
54. com.adventnet.sa.SyslogReportTask
55. com.adventnet.sa.server.DomainDiscovery
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
65. com.adventnet.sa.server.ELSInitializer
66. com.adventnet.sa.server.EAService
67. com.adventnet.logsearch.search.BatchSearch
68. com.adventnet.logsearch.index.api.ArchiveIndex
69. com.adventnet.logsearch.index.api.LogIndexingAPI
70. com.adventnet.logsearch.index.util.DBUtil