ManageEngine
Powering IT ahead

EventLog Analyzer 7

Admin Server - User Guide

www.eventloganalyzer.com

eventlog-support@manageengine.com

Table of Contents

INTRODUCTION 3

About EventLog Analyzer Distributed Edition Admin Server 4

Release Notes - Distributed Edition 5

INSTALLATION AND SETUP 6

System Requirements - EventLog Analyzer Distributed Edition Admin Server 6

Prerequisites - EventLog Analyzer Distributed Edition Admin Server 8

Recommended System Setup 8

Installing and Uninstalling - EventLog Analyzer Distributed Edition Admin Server 9

Uninstalling EventLog Analyzer 11

Starting and Shutting Down - EventLog Analyzer Distributed Edition Admin Server 12

Shutting Down EventLog Analyzer 13

Windows Service: 13

Accessing the Web Client - EventLog Analyzer Distributed Edition Admin Server 14

License Information - EventLog Analyzer Distributed Edition Admin Server 15

USER INTERFACE 16

Using the Dashboard 16

Using The Sub Tab 18

Using The Left Navigation Pane 19

Dashboard View Customization 20

VIEWING EVENT REPORTS 22

Viewing Events for a Host 23

Viewing Top Hosts 24

Viewing Event Trends 26

Viewing Compliance Reports 27

Viewing Application Log Reports 30

Users Report 31

Viewing IBM AS/400 System History Log Reports 36

ALERT NOTIFICATIONS 37
Viewing Alerts 37
CONFIGURING SYSTEM SETTINGS 38
Managed Server Settings 39
Viewing Host Groups 40
Viewing Host Details 41
Viewing Alert Profiles 42
Viewing Database Filters 43
Viewing Report Schedules 44
Archiving Log Files 45
Centralized Archive of Log Files 46
Imported Log Files 48
CONFIGURING ADMIN SETTINGS 50
Active Directory Configuration Settings 50
User Management 52
Adding a New User 52
Changing Account Settings 54
Viewing Server Diagnostics 55
TIPS AND TRICKS 56
Frequently Asked Questions - EventLog Analyzer Distributed Edition 56
Troubleshooting Tips - EventLog Analyzer Distributed Edition 59
OTHER TOOLS AND UTILITIES 61
Working with SSL 61
Converting existing Standalone Edition EventLog Analyzer installation to Distributed Edition Managed Server 63
ASK ME 65
Using Ask ME 65
Contacting Technical Support 66
Log Level Setting 68

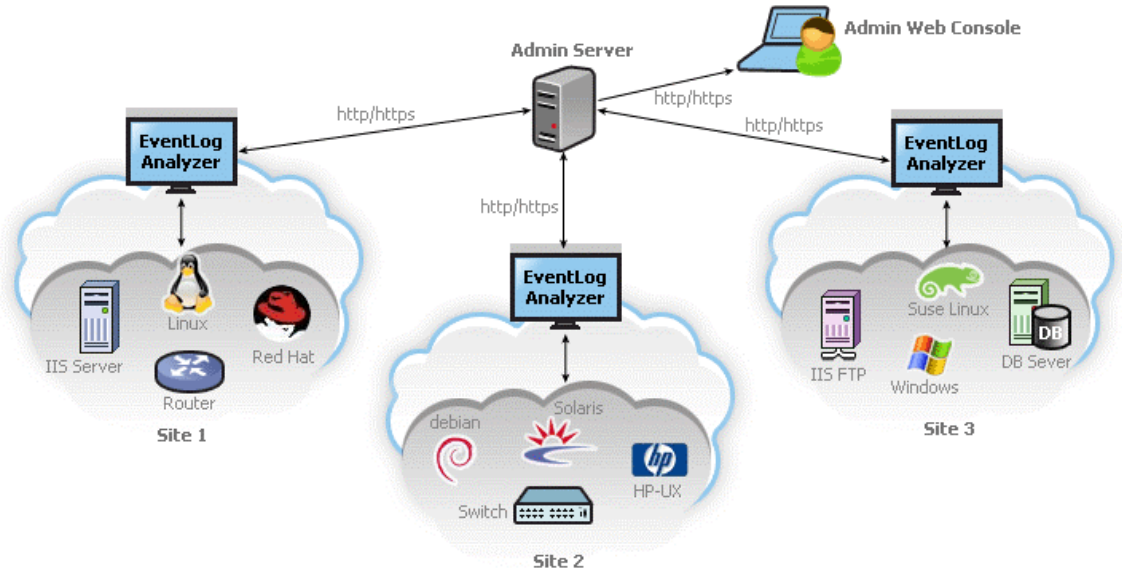
Introduction

Introduction - EventLog Analyzer Distributed Edition Admin 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:

- Aggregated log management of whole enterprise in different physical locations.
- Scalable architecture supporting 1000s of hosts.
- Centralized monitoring using single console view.
- Secured communication using HTTPS.
- Exclusive segmented and secured view for various customers of MSSP.

About EventLog Analyzer Distributed Edition Admin Server

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 the 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 (inbuilt MySQL) database
Compliance reporting	View pre-defined compliance reports which meet the HIPAA, GLBA, SOX, and PCI requirements.
Automatic alerting	View 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.
Pre-defined event reports	view reports on top events, top hosts, etc. across hosts, host groups, users, and even processes.
Multiple report formats	export reports in HTML, PDF, and CSV formats.

Release Notes - Distributed Edition

The new features in the 6.1.0 Enterprise release are mentioned below.

- 6.1.0 - Build 6010 Distributed Edition (GA)

6.1.0 - Build 6010 Distributed Edition

GA release of EventLog Analyzer Distributed Edition.

New Features - Admin Server

The general features available in this release include,

- **Distribution**
  Central Archiving support for imported application logs:

Installation and Setup

System Requirements - EventLog Analyzer Distributed Edition Admin Server

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

- Hardware Requirements
- Operating System Requirements
- Supported Web Browsers

Hardware Requirements

For 32 Bit Installation

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

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

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

Operating System Requirements

EventLog Analyzer Admin Server 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, 2003 Server & 2008 Server
2. Linux - RedHat 8.0/9.0, Mandrake/Mandriva, SuSE, Fedora, CentOS
3. Ability to run in VMware environment

Note: If EventLog Analyzer is installed in SuSE Linux, then ensure that in the **mysql-ds.xml** file, present under *<EventLog Analyzer 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 Web Browsers

EventLog Analyzer Admin Server 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 - EventLog Analyzer Distributed Edition Admin Server

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

Ports to be freed

EventLog Analyzer Admin Server 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.
8763	This is the default HTTPS port. You will connect to the EventLog Analyzer from a web browser in secured mode using this port number.
33335	This is the port used to connect to the MySQL database in EventLog Analyzer.

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.
- If **Centralized Archive** is enabled, EventLog Analyzer transfers all the files from Managed Server to Admin Server using Secure Copy (SCP). SCP is based on SSH. Ensure SSH is available in the server machine.

Changing Default Ports

Changing the default MySQL port:

1. Edit the **mysql-ds.xml** file present in the *<EventLog Analyzer 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 *<EventLog Analyzer 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 Distributed Edition Admin Server

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

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.

- Click **Advanced Install** button.
- Read the *License Agreement* and click **Yes** button.
- Select **Distributed Edition** and click **Next** button.
- Select **Admin Server** and click **Next** button.
- If the Admin Server is behind Proxy Server, configure the **Proxy Server Host**, **Proxy Server Port**, **Proxy User Name**, and **Proxy Password** details. Click **Next** button.
- Select **Destination Folder** using **Browse** button, for installation. Click **Next** button.
- 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.
- Select **Install EventLog Analyzer as service** check box (recommended), if you want to install Collector server as a service. Click **Next** button.
- Configure new Program Folder or retain the default. Click **Next** button.
- The installation details like Installation Directory, Program Folder, and Web Port are displayed. Click **Next** button.
- Now, Distributed Edition - Admin 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 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.

- Click **Advanced Install** button.
- Read the *License Agreement* and click **Yes** button.
- Select **Distributed Edition** and click **Next** button.
- Select **Admin Server** and click **Next** button.
- If the Admin Server is behind Proxy Server, configure the **Proxy Server Host**, **Proxy Server Port**, **Proxy User Name**, and **Proxy Password** details. Click **Next** button.
- Select **Destination Folder** using **Browse** button, for installation. Click **Next** button.
- 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.
- Select **Install EventLog Analyzer as service** check box (recommended), if you want to install Collector server as a service. Click **Next** button.

- Configure new Program Folder or retain the default. Click **Next** button.
- The installation details like Installation Directory, Program Folder, and Web Port are displayed. Click **Next** button.
- Now, Distributed Edition - Admin Server installation is complete.

This will install EventLog Analyzer - Admin Server 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 - EventLog Analyzer Distributed Edition Admin Server

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

Starting EventLog Analyzer

Windows:

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 as 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:

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.

Starting the EventLog Analyzer service in Linux

/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:

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. 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 as 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:

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.

Stopping EventLog Analyzer service in Linux

```
/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 Distributed Edition Admin Server

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 Admin Server.

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 Admin Server is running, and *8400* is the default web server port)

3. Log in to EventLog Analyzer Admin Server using the default username/password combination of **admin/admin**.

Once you log in, you can view event reports, and more.

Secured Mode

Follow the steps below to access EventLog Analyzer Admin Server in secured mode.

1. Open a supported web browser window

2. Type the URL address as ***http://<hostname>:8763*** (where <*hostname*> is the name of the machine on which EventLog Analyzer Admin Server is running, and *8763* is the default HTTPS port)

3. Log in to EventLog Analyzer Admin Server using the default username/password combination of **admin/admin**.

License Information - EventLog Analyzer Distributed Edition Admin Server

After you log in to EventLog Analyzer Admin Server, 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 Admin Server installation.

The License window displays the following information:

- Type of license applied - Trial 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.

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.
Select the EventLog Analyzer Managed Server, of which you want to view the dashboard, in the **Dashboard Views** of the left navigation panel.

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.

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 the selected EventLog Analyzer Managed Server, and the next tab **Applications** lists all application logs imported by the selected EventLog Analyzer Managed Server.

Click the **Hosts** link to view the list of all hosts from which event logs are collected.

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.
Host Name	The host name of the machine from which event logs are collected
Host Group	The host group to which this host belongs
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.

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 **Advanced Search**, **Managed Server Failure Alert** and **Bookmarks** in EventLog Analyzer Admin Server.

Using The Left Navigation Pane

The left navigation pane provides quick links to different tasks and reports in EventLog Analyzer Admin Server. 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. **Customize** link is available by the side to create a new custom dashboard view.
Global Calendar	Allows you to select the time period for all reports from one place. By default, the last day's data is shown.
My Reports	Includes links to view custom reports created in the selected Managed Server.
Top N Reports	Includes links to view event-based reports on top hosts, top processes, and more.
Trend Reports	Includes links to view trend reports based on event logs received from hosts.
Compliance Reports	Includes links to view reports for HIPAA, GLBA, SOX, and PCI compliance requirements.
Applications	Includes links to view application-based reports on top hosts, top users, top file types, top Page URLs, and more.

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.

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 **Default** view.

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

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 navigation pane top of the Home tab.
- Edit any of the listed views created by user, except the **Managed Server** dashboard views.
- Set any one of the views as default dashboard view.
- Delete any of the listed views created by user, except the **Managed Server** dashboard views 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 required managed server from the **Managed Servers** combo box as per your requirement, which lists all the Managed servers registered with this Admin server.
- 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. 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.

Viewing Event Reports

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
My Reports (Custom Reports)	view custom reports created based on specific reporting criteria
Top N Reports	view top hosts and top processes generating events of different severity
Compliance Reports	view instant reports for HIPAA, GLBA, SOX, and PCI requirements
Trend Reports	view event trends based on event severity or event category, and alert trends
Detailed 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
Detailed Host Reports	view host-specific event summary for each host
IBM AS/400 Reports	view pre-defined reports for IBM AS/400 device

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. Selected Host is displayed on top of the General Summary report. 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.

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 his password, and whether he was successful or not.

If a user has been accessing several hosts with his 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 he was unsuccessful, on which hosts did he 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 his password, and whether he was successful or not.

If a user has been accessing several hosts with his 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 he was unsuccessful, on which hosts did he 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 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.

Viewing Compliance Reports

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

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

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 compliances and the selected list of reports, configure new or existing compliances. You can find this link on the **Reports** menu of the sub-tab. Clicking the **Compliance Reports [View All]** link opens the **Compliance Reports** page. On the right side top of the page, **Add New** and **Edit** links are present. With the **Add New** link, you can add a new compliance and select a set of reports for the compliance. With **Edit** link, you can edit the default compliances available in the EventLog Analyzer. The **Compliance Reports** page displays the four default compliance reports. The page displays the Compliance, its description, provides scheduling of the compliance report with **Schedule** link, allows you to intimate 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.

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 to help comply with the HIPAA regulations:

- User Logon/Logoff
- Logon Failure
- Audit Logs Access
- Object Access
- System Events

- 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 to help comply with the SOX regulations:

- User Logon/Logoff
- Logon Failure
- Audit Logs Access
- Object Access
- System Events
- Track Account management changes
- Track User Group changes
- Track Audit policy changes
- Successful User Account Validation
- UnSuccessful User Account Validation
- Track Individual User Action

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 to help comply with the GLBA regulations:

- User Logon/Logoff
- Logon Failure
- Audit Logs Access

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

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 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

- User Logon/Logoff
- Logon Failure
- Audit Logs Access
- Object Access
- Track Audit Policy Changes
- Track Individual User Action

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

Viewing 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
- MS SQL Server 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 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

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:

- Internal Program Load
- File Operations
- Journal Receiver
- Damages Detected
- Job Logs
- System Time Changed
- EtherNet
- Expiry Details
- Hardware Errors
- Internal Protocol
- Deleted Objects
- System Value Changes
- Subsystem Activities
- Incorrect Password
- Active Interface

Alert Notifications

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.

Configuring System Settings

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

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

Setting	Description
Managed Server Settings	Click this link to view the Managed server settings enable, stop, & reset.
Host Groups	Click this link to view 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 for each Managed server selected
Database Filters	Click this link to view the database filters for each Managed server selected
Schedule Listing	Click this link to view the list of report schedules
Archived Files	Click this link to view and load archived files into the database and configure Centralized Archive settings
Imported Log Files	Click this link to view the imported Windows Event Log files (type *.evt* format) from the local machine or by FTP from remote machine for each Managed server selected

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

Setting	Description
Active Directory	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
Server Diagnostics	Click this link to view system-related information

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.

Managed Server Settings

Click the **Managed Server Settings** link under the **Settings** tab. The **Manage Managed Servers** page opens up. The tabular list contains individual and select all Managed servers check boxes.

Delete Managed Servers

Select required Managed server(s) or select all Managed servers to delete. Click the **Delete Managed Server(s)** link on top left side of the page. The selected Managed server(s) will be deleted.

Managed Server Details	Description
Managed Server Name	Name of the Managed server. **Edit user details** icon. Use the icon to update the admin username and password whenever any changes are made in the Managed Server.
Managed Server Status	Status of the Managed server, whether **Up** UP or **Down** Down
Last Collection Time	The time of last log collection by the respective server.
Data Collection Status	If the log collection is on the status icon appears and if the log collection is not happening then the status icon appears with appropriate error message.
No of Host/Applications	Number of Host/Applications being monitored by the corresponding Managed server.
Flow rate (messages/sec)	Number of log messages received per second by the Managed Server
Action	Use the **Enable** option to change Data Collection status. **Stop/Up** - Stops the data collection/Starts the data collection **Reset** - Resets the data collection and starts collecting data from scratch

Edit user details

Click the **Edit user details** icon. The **Edit user details** window pops up. Change the *User Name*, *Password*, *Web Protocol*, and *Web Port* as per requirement. Once you have made the required changes, click **Save** to save the changes. Click **Cancel** to cancel the user detail changes.

Viewing Host Groups

EventLog Analyzer Admin Server lets you to view host groups from which event logs are collected. In the Managed Server, 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.

Managed Server : combo box lists all the Managed servers registered with this Admin server. Select the Managed server as per your requirement.

Click the **Host Groups** link from the **Settings** tab to view host groups of the selected Managed Server.

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**.

Click on the **Number of Hosts** link to list the hosts belonging to the corresponding group.

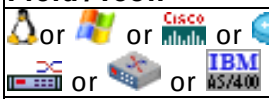
Viewing Host Details

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

The **Host Details** link also lists the ports on which the selected Managed Server is listening for event logs. The **Managed Server** table lists the following details of the selected Managed Server: Name, Host, Status, Host Name/IP Address, and Listening Ports. By default, **Listening Ports** 513 and 514 is added.

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

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.
HostName	The host name of the machine from which event logs are collected
HostGroup	The host group under which the host is grouped
HostIPAddress	The IP Address of 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 in the respective Managed Server, where the field **Monitor Interval in minutes** decides the next schedule of the scan, the default being 10 minutes.
LastMessageOn	Displays the last time at which the host sent an event log to the server.

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

Viewing Alert Profiles

Click the **Alert Profiles** link in the **Settings** tab, to view all the alert profiles set up for the selected Managed Server. Clicking the option will open the **Alert Profile Details** page. The page contains a combo box and list of alert profiles available.

Managed Server : combo box lists all the Managed servers registered with this Admin server. Select the Managed server as per your requirement.

The Alert Profile Details table lists all the alert profiles set up for the selected Managed Server, along with all the details such as Name, Host/Group, LogType, and Notifications. Click on an alert profile to see the corresponding list of alerts triggered.

The  icon indicates that an e-mail notification has been set up for this alert profile. The corresponding e-mail address is also displayed next to this icon.

Viewing Database Filters

Click the **Database Filters** option in the **Settings** tab, to view 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 a particular event, and optimizing the capacity of the database. Clicking the option will open the **Filter Details** page. The page contains a combo box and list of filters available.

Managed Server : combo box lists all the Managed servers registered with this Admin server. Select the Managed server as per your requirement.

Viewing Database Filters

The Database Filters option lists all the filters created so far. The list displays the Filter Name, Filter Type, Host Name and Groups for which the filter has been set up.

Note on 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.

Viewing Report Schedules

Once you have created a custom report profile in the Managed Server, 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 in PDF or CSV formats

Managed Server : combo box lists all the Managed servers registered with this Admin server. Select the Managed server as per your requirement.

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.

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.

Managed Server : combo box lists all the Managed servers registered with this Admin server. Select the Managed server as per your requirement.

Loading Archived Files

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

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, you can search for data in the archives, and view specific information. Click on  **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.

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, enter the criteria for the data, such as the hostname, user name, protocol, etc. You can enter a maximum of three criteria.

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.

Configuring Centralized Archive Settings

Click the  **Archive Settings** link to configure the centralized archiving in the Admin Server. Refer the Configuring Centralized Archive of Log Files page for deatiled procedure.

Centralized Archive of Log Files

EventLog Analyzer Distributed Edition can support centralized archiving of event logs received from each host. In the normal deployment of distributed edition, the archived files are stored in the respective Managed Servers. The **Centralized Archive** feature has to be enabled in the Admin Server and there is no configuration required to be done in the Managed Servers.

Description

The Centralied Archive feature mechanism is explained below:

In centralized archiving of the distributed set up, the logs are zipped at periodic intervals and the archive file is transported to the Admin Server using Secured Shell (SSH). The archive file will be received by the Admin Server and confirmation message for the receipt of the file is sent by the Admin Server to the respective Manage Server. Managed Server upon receiving the confirmation message deletes the archive file.

	SSH Server will be started, if Centralized Archive is enabled.

Configuring Centralized Archive

In the Admin Server, select **Settings** tab > **Archived Files** link. The **Archive Files** screen opens up. Click **Centralized Archive Settings** link to configure the centralized archive settings. The **File Archive Settings** screen pops up.

To enable the Centralized Archive in the distributed set up, select the **Enable Centralized Archive** check box.

If **Centralized Archive** is enabled, EventLog Analyzer transfers all the files from Managed Server to Admin Server using Secure Copy (SCP). SCP is based on SSH.

SSH Server will be started with the below configurations if Centralized Archive is enabled.

Setting	Description
Archive Location	Configure the Admin Server Centralized Archive location in this field. By default the location is set to *<EventLog Analyzer Admin Server Home>/archive/<Individual Managed Server>/*.
Server IP/Name	Configure the IP address of the server in which the SSH is running. In our it will be Admin Server.
User Name	Configure the user name of the SSH service.
Password	Configure the password of the SSH service.
Port	The default SSH port will be **22**. You can configure any other port from **1024** to **65535**. You can click on the **Availability** link, to check whether the port is free or occupied by some other application.

Trouble Shooting Tips:

If the Centralized Archive is enabled, the SSH Server will be started with the configured values. If the SSH Server fails to start, then **Failed** status will be indicated besides the **Centralized Archive Settings** link.

If the SSH Server is not getting started, there could be two reasons:

- The SSH Server is not able to bind with the configured IP Address. (This is more likely to happen with dual NIC machine). Check and configure the IP Address of the appropriate NIC.
- The Archive Location configured may be invalid. Configure valid location to archive the files.

Imported Log Files

The **Imported Log Files** link lets you import a windows event log file (type *.evt* format) from the local machine or remotely, through FTP. You can import both Event Log and Application Log files.

Managed Server : combo box lists all the Managed servers registered with this Admin server. Select the Managed server as per your requirement.

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.

Imported Event Log Files

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 inbuilt MySQL DB.
	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 DropDB link to drop the imported log file table.

Imported Application Log Files

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.

Column Head	Description
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* link to load the event log file into the inbuilt MySQL DB.
	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 DropDB link to drop the imported log file table.

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.

Configuring Admin Settings

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 rescan 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 **Host Group** as *Windows Group*.

Procedure to configure AD settings

Click the **Active Directory** link under the **Settings** tab to configure the AD user details import, periodic import, and to enable user authentication usage. On clicking the link, 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 rescan 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 gray out.

User Management

Click the **User Management** link to create and manage the different users who are allowed to access the EventLog Analyzer Distributed Edition - Admin server.

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

User	Description
Administrator	This user can do all operations meant for Distributed Edition - Admin server including adding additional users and more
Operator	This user can do all Administrator operations **except** configuring the user
Guest	This user can only view device details, and basically has only read-only privileges. The Alerts & Support tabs are not available for guest users

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.

Adding a New User

Click the **Add New User** link to add another user to access EventLog Analyzer. Enter the new user's username, password, access level, default e-mail address, and Managed Server.

Managed Server selection allows the Administrator to assign Managed Servers to users with Guest or Operator privileges, and only the assigned devices in that particular Managed Server can be viewed by the particular user when they login to Distributed Edition - Admin server.

Assign Devices To View section allows the Administrator to assign devices to users with Guest or Operator privileges, and only the assigned devices can be viewed by the particular user when they login to EventLog Analyzer.

By default, users with "Administrator" privileges can view all the devices.

Click **Add User** to add this user to the list of users accessing EventLog Analyzer.

Editing User Details

If you have logged in as a user with administrative privileges, the User Management page lists all the users created so far. Click the user's username to view the respective user details. You can change the password, access level, the default e-mail address for this user and can also reassign the devices that can be viewed by the particular user.

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 **Save User Details** to save the new changes.

Viewing Login Details

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

EventLog Analyzer User Privileges

Types of User Privileges in EventLog Analyzer

- **Administrator** - Can view details of all Hosts/Managed Servers.
- **Operator** - Can view details of the Hosts/Managed Servers assigned to him and cannot perform User Management.
- **Guest** - Has read-only privileges for the Hosts assigned to him.

Comparison of Feature Access to the Users

Sl No	Feature Name	Administrator	Operator	Guest
1	User Management Create/Modify/Delete users	Yes	No	No
2	Dashboard View Customization	For all Hosts	Only for Hosts assigned to him.	Only for Hosts assigned to him
3	Advanced Search	Yes	Yes	The user can perform advanced search except Save as Report Profile.
4	Bookmark	The user can view only his bookmarks.	The user can view only his bookmarks.	The user can view only his bookmarks.
5	User Assistance • Tell a Friend • Upgrade License • Help • Feedback About	Yes	Yes	No

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 **Save User Details** to save the changes. Click **Cancel** to return to the default **Settings** tab.

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

Tips and Tricks

Frequently Asked Questions - EventLog Analyzer Distributed Edition

For the latest list of Frequently Asked Questions on EventLog Analyzer, visit the FAQ on the website or the public user forums.

General

1. **Who should go for EventLog Analyzer - distributed setup (Distributed Edition)?**

   We recommend distributed setup (Distributed Edition):
   - If your's is a **large enterprise**, which have hundreds of security devices (like Windows hosts, Linux hosts, servers), Switches and Routers to manage across different geographical locations.
   - If you are a **Managed Security Service Provide** (MSSP), having a large customer base spread across geographical locations.

2. **How many Managed Servers can a single Admin Server manage?**

   One Admin Server is designed to manage 50 Managed Servers. However, we have carried out simulated testing in our laboratory, which effortlessly managed 20 Managed Servers.

3. **During installation of Admin Server, I am prompted for Proxy Server details? When should I configure it?**

   You need to configure the proxy server details during **Admin Server** installation, if the **Admin Server** needs to pass through **Proxy Server** to contact **Managed Servers**.

4. **Can I convert the existing "*Standalone*" EventLog Analyzer installation to a "*Distributed Setup*"?**

   Yes, you can. Ensure that the existing installation of **EventLog Analyzer build is 6000**. To convert, you need download the EventLog Analyzer 6.0 exe/bin and install as **Admin Server** and then you need to convert the existing installation of EventLog Analyzer 6.0 to **Managed Server**. Refer the procedure in the below help link:

Procedure to convert existing Standalone Edition EventLog Analyzer installation to Distributed Edition Managed Server

5. **I have deleted the Managed Server from Admin Server. How do I re-add?**

Once you have deleted the **Managed Server**, to re-add follow the procedure given below:
- Reinitialize the Managed Server.
- Re-register the Managed Server with Admin Server by executing the *<EventLog Analyzer Home>**troubleshooting***registerWithAdminServer.bat/sh** file.
- Restart the Managed Server.

6. **Where the collected logs are stored, whether in Managed Server database or in both Managed Server and Admin Server databases?**

   All the logs collected by the Managed Server are stored in the Managed Server database only. For archiving, there is a provision to forward the logs to the Admin Server, but not for storing in the Admin Server database

Secured Communication Mode (HTTPS)

1. **What is the mode of communication between Admin Server and Managed Server?**

   By default, the mode of communication is through **HTTP**. There is also an option to convert it to secured mode of communication **HTTPS**. Refer the procedure in the below help link, to setup secure communication mode between Admin and Managed Server.
2. **I have changed the Managed Server communication mode to HTTPS, after installation. How to update this info in Admin server?**

Click on **Settings tab > Managed Server Settings link** in *Admin Server UI* and click on the **Edit** icon of specific Managed and select the appropriate protocol and configure the web server port details.

Licensing

1. **What are the "Licensing Terms" for EventLog Analyzer Distributed Edition?**

EventLog Analyzer Distributed Edition license will be applied in Admin Server. The number of hosts/applications for which the license is purchased, is utilized among the registered Managed Servers. You can keep adding the hosts/applications in various Managed Servers till the total number of licenses purchased get exhausted. View the number of hosts/applications managed by each Managed Server in the Managed Server Settings page.

If the number of hosts/applications being collectively managed by all the registered Managed Servers, exceed the number of License purchased, a warning message appears in the Admin Server. In that scenario, you have various options.

- Purchase license to manage the additional hosts/applications.
- Otherwise, check the number of hosts/applications being managed by each Managed Server in the Managed Server Settings page in the Admin Server.
  - Go to the individual Managed Server and manually manage the licenses. Manually remove the lesser required hosts/applications and make the managed hosts/applications count equal to the number of licenses.
  - You can also remove a registered Managed Server in the Admin Server to make the managed hosts/applications count equal to the number of licenses.

2. **In Managed Server there no is option to apply the license? How the license get applied in the Managed Server?**

   Yes, there is no option to apply the license in **Managed Server**. The license applied in **Admin Server** will be automatically propagated to all **Managed Servers**.

3. **"*License Restricted*" alert is showing in Admin Server, even though I have unmanaged additional devices in Managed Server. Why?**

The managed/unmanaged status of devices in Managed Server are synchronized with Admin Server during the data collection cycle, which happens at an interval of 5 minutes.

Troubleshooting Tips - EventLog Analyzer Distributed Edition

For the latest Troubleshooting Tips on EventLog Analyzer, visit the Troubleshooting Tips on the website or the public user forums.

Trouble Shooting - General

1. **When I login, why "*No Data Available*" is shown?**

Check for the following reasons:

- Click on the current date in the **Calendar**. If data is displayed, then there could be some time difference between **Admin** and **Managed Server**.
- If both **Admin** and **Managed Server**s are in different time zones, then you need to choose the appropriate time using **Calendar**.

2. **Data collection is not happening?**

The possible reasons could be:

The **Admin Server** unable to contact **Managed Server** or the **Managed Server** status is **down**.

a. If the **Admin Server** is unable to contact **Managed Server**,
   i. The **Managed Server** added may not be of **Distributed Server** type.
   ii. The **username** and **password** configured for respective **Managed Server** may not have **Administrative** privilege.

b. If the **Managed Server** status is **down**, check for the following conditions:
   i. Is the **Managed Server** running? Is the **Port** and **Protocol** information configured **correct**?
   ii. Is the **Admin Server** needs to pass through **Proxy Server**? If so, is the same has been configured?
   iii. Are the **Ports** required are opened/allowed in **Host/Server(s)**?

3. **When Alert count is clicked, "Security Statistics" page is shown with "No Data Available" message?**

The possible reasons are listed below:

- Time difference between **Admin** and **Managed Server**.
- All report page are fetched from Managed Server directly, but the generated alerts are fetched from **Admin Server**. The generated alerts from all **Managed Servers** are synchronized periodically (at 5 minutes interval). This could be the case where the generated alerts are yet to be synchronized.
- If you have converted a standalone EventLog Analyzer installation to **Managed Server**, previously generated alerts will not be synchronized. Only new alerts will be synchronized.

Trouble Shooting - Managed Server Synchronization

1. **After installing *Managed Server*, unable to start it. It says "*Distributed Edition: Problem encountered while registering with Admin Server.*"?**
   This happens when **Managed Server** fails to establish contact with **Admin Server**.
   The conditions under which communication could fail are listed below:
   a. **Admin Server** is not running in configured machine at given port.
   b. **Managed Server** needs to pass through **Proxy Server** and it has not been configured. In case configured, check if values are valid.
   c. Appropriate ports (**8500** - default web server port), (**8763** - default HTTPS port) are not opened in Host/Server(s).
   d. **Build** mismatch between **Admin** and **Managed Servers**.

2. **Installed both *Admin* and *Managed Servers*, but when I login into *Admin Server*, I see *Managed Settings* page only. Why?**
   - This could be because the data collection for all the **Managed Servers** added in the **Admin Server** are yet to happen. By default, the data collection for a **Managed Server** is scheduled every 5 minutes.
   - No device/resource exists in **Managed Server**.

3. **In Admin Server, the status of the Managed Server is shown as "*Down*", even though I am able to view reports for devices in it?**
   The status update of the **Managed Server** is performed at the end of every data collection cycle which is scheduled for every 5 minutes.

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 <*EventLog Analyzer 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 8400 -->
 <Connector port="8400" 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*>:8763 where <*hostname*> is the machine where the server is running

Converting existing Standalone Edition EventLog Analyzer installation to Distributed Edition Managed Server

To convert existing Standalone Edition EventLog Analyzer installation to Distributed Edition Managed Server follow the procedure given below:

- Shutdown the EventLog Analyzer Service. Ensure that ports 33335 (default MySQL) and 8400 (default 8400) are free.
- Take a backup of database.
- Open a **Command Prompt/Console** and navigate to *<EventLog Analyzer Home>/troubleshooting* directory.
- Execute the **ConvertToManagedServer.bat/sh** file.

  It will prompt you to take backup of **mysql** data folder and to continue running the script.

```
Please take backup of database before running this script.
 Do you really want to continue this script? [y/n]: y
```

- It will prompt you to shut down the server or service, if it is running.

```
EventLog Analyzer Server is running. Server should not run while running this
tool. Please shutdown the server before running this tool.
```

- Enter the details of the Admin Server.

```
Enter Web Port of this server [8400] :8400
 Enter Web Server Protocol of this server [http] :http
 Enter Admin Server Name/IPAddress :EventLog-test
 Enter Admin Server Web Port [8400] :8400
 Enter Admin Server Web Protocol [http] :http
```

- Enter the details of the Proxy Server, if required.

```
Use Proxy to reach Admin server [n/y] :y
 Enter Proxy Server Name :proxy-server
 Enter Proxy Server Port :80
 Enter Proxy UserName :root
 Enter Proxy Password :public
```

- If this server registers successfully with the intended Admin Server, the following message is displayed.

```
Successfully registered with the AdminServer
 Database not started. Starting .....
 Table successfully updated
 ....
....
....
....
Server noted as Converted Managed
```

```
TablesToSync.xml delete status ::::::: true
stopping DB Server .......
```

Open the Admin Server UI and check the Managed Server Settings and ensure that the converted server is listed.

- If this server cannot register with the intended Admin Server, it will prompt you to check the Admin Server availability.

```
Unable to connect with the Admin Server on given port and protocol. Kindly
ensure the following

 1. Admin Server is accessible on given port and protocol.
 2. Is Admin Server behind Proxy-Server ? If so, has those details been
configured ?
Exit due to error during register
```

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.

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 eventloganalyzer-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 SIP file and then press Upload.
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 granularity 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 eventloganalyzer-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 eventloganalyzer-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 Sec 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 eventloganalyzer-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

Log Level Setting

The Log Level Setting is used for setting the granularity level of EventLog Analyzer server logs. The logs will form part of the Support Information File (SIF) generated for sending to ZOHO Corp. These logs will be used for debugging EventLog Analyzer server issues. The procedure to set the log levels is given below:

In the **Set Logger Level** screen,

1. Select the **Server Log Filter Settings** (values from 2 to 5) from the combo box.
2. Select the **Level of Log data to be stored** from the combo box. The values available are:
   a. ALL
   b. FINEST
   c. FINER
   d. FINE
   e. CONFIG
   f. INFO
   g. WARNING
   h. SEVERE
   i. OFF
3. Select the **Logger Name** from the list. The loggers available are given below. For each available logger or set of loggers, you can set the log filter level and log level independently.
4. Click **Save Settings** button to save the log level settings. Setting completion message with details appears on top of the screen. Click **Cancel** button to cancel the log level setting action

The loggers available are given below:

1. com.adventnet.la
2. com.adventnet.la.RSDatasetModel
3. com.adventnet.la.DepartmentUtil
4. com.adventnet.la.DefaultDataFormatter
5. com.adventnet.la.GLinkGenerator
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