ManageEngine
Powering IT ahead

EventLog Analyzer 8

Admin Server

USER GUIDE

www.eventloganalyzer.com

Table of Contents

What is in this guide?

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

Are you new to EventLog Analyzer?

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

- *How to manage Managed Servers of EventLog Analyzer, hosts, and applications?*
- *What are the reports available?*
- *View custom and canned reports*
- *How to search the logs?*
- *How to extract additional fields from the logs?*
- *View alerts generated*

Introduction

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 or more 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.

Overview

- *Get log data from systems, devices, and applications*
- *Search any log data and extract new fields to extend search*
- *Get IT audit reports generated to assess the network security and comply with regulatory acts*
- *Get notified in real-time for event alerts and provide quick remediation*

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

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

Get log data from machines and applications

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

Search any log data and extract new fields to extend search

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

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

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

Get notified in real-time for event alerts and provide earliest remediation

EventLog Analyzer comes with another versatile feature, real-time alerts. You can configure alerts to notify in real-time for any specific network events or anomalies. You can get instant notification via email and SMS. You can also execute a program or script on alert generation and take remedial or other actions for the particular alert.

Release Notes

The new features, bug fixes, and limitations in each of the release are mentioned below.
8.0 - Build 8000 (GA)

8.0 - Build 8000 - Distributed Edition - Admin Server

The general features available in this release include all the features of EventLog Analyzer Version 7.4 Build 7400 and

New Features:

- Sleek and stylish user interface with improved functionality and flexibility
- Customizable dashboard widgets provide better visibility into network events, security events, event trend and event alerts

Setup the product

Setup EventLog Analyzer - Distributed Edition Admin Server

- Assess your network for Security Information and Event Management (SIEM)
- Download the product
- Check the installation requirements
- Install the product
- Ensure the prerequisites are met
- Run the product
- Check whether your requirements are met
- Check the EventLog Analyzer editions available
- Buy the product

System Requirements - 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

To install in 32 bit machine

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

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

To install in 64 bit machine

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

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

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

Operating System Requirements

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

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

Supported Web Browsers

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

- Internet Explorer 8 and later
- Firefox 4 and later
- Chrome 8 and later

Recommended System Setup

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

- Run EventLog Analyzer Admin Server on a separate, dedicated PC or server. The software is resource-intensive, and a busy processor may cause problems in connecting Managed servers.
- 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.

How to Install and Uninstall - Distributed Edition Admin Server

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

How to install?

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

There will be two options to install:

- One Click Install
- Advanced Install

One Click Install option cannot be used to install the product as Admin Server. Choose **Advanced Install** option to custom install the product. The wizard screens will guide you through the installation.

Quick view of Advanced Installation

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

  Standalone Edition for Small and Medium Businesses (SMBs) - If you are small or medium business in a single location and monitor less than 600 devices and/or applications, Standalone edition is suitable for you.
  Distributed Edition for Large businesses and MSSPs - If you are a large business or MSSP with geographically distributed environment and monitor less than 12000 devices and/or applications, Distributed edition is suitable for you.
  Free Edition - If you are micro business or SOHO and want to monitor less than five hosts, you can download the ManageEngine_EventLogAnalyzer exe or bin file of Standalone edition and install it as a **Free** edition.

- Select **Distributed Edition** and **Admin Server** and if the Admin Server is behind Proxy Server, configure the **Proxy Server Host**, **Proxy Server Port**, **Proxy User Name**, and **Proxy Password** details

- Select the folder to install the product. Use the **Browse** option. The default installation location will be *C:\ManageEngine\EventLog* folder. If the new folder or the default folder does not exist, it will be created and the product will be installed.

- Enter the web server port. The default port number will be 8400. Ensure the default or the port you have selected is not occupied by some other application.
  Choose the language (Simplified Chinese, Traditional Chinese, English, Japanese, Others). Ensure that the browser supports the selected language.
  Choose the web protocol (HTTP/HTTPS). Use HTTP for unsecured and HTTPS for secured communication.

- Select **Install EventLog Analyzer as service** option to install the product as Windows or Linux service. By default this option is selected. Unselect this option to install as application. You can install as application and later convert the same as service. ManageEngine recommends you to install it as service.

- Enter the folder name in which the product will be shown in the Program Folder. By default it will be **ManageEngine EventLog Analyzer x** folder.

- Enter your personal details to get assistance.

At the end of the procedure, the wizard displays the options to dispaly ReadMe file and start the EventLog Analyzer Admin server.

With this the EventLog Analyzer product installation is complete.

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

How to uninstall?

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

Windows:

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

Linux:

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

Note: At the end of uninstallation you will be taken to the Uninstallation Feedback Form where you can provide reasons for your product uninstallation. This would help us improve this product.

Prerequisites - Distributed Edition Admin Server

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

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

What are the ports required for EventLog Analyzer?

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

Port Numbers	Ports Usage	Description
8400	Web server port	This is the default web server port used by EventLog Analyzer. This port is used to connect EventLog Analyzer using a web browser. Change the port as required.
513, 514	Syslog port	These are the default Syslog listener ports. Ensure that the hosts are configured to send Syslogs to any one of these ports.
33335	MySQL database port	This is the port used to connect to the MySQL database in EventLog Analyzer.

How to change the default ports used by EventLog Analyzer?

Procedure to change the default web server port:

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

Procedure to change the default MySQL port:

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

How to Start and Shutdown - Distributed Edition Admin Server

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

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

How to start?

Windows Application:

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

Windows Service:

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

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

Linux Application:

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

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

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

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

Linux Service:

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

/etc/init.d/eventloganalyzer status
ManageEngine EventLog Analyzer X.0 is running (15935).

How to shutdown?

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

Windows Application:

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

Windows Service:

Ensure that the EventLog Analyzer software is installed and running as Windows Service. To stop Windows Service, follow the steps given below.

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

Linux Application:

- Navigate to the *<EventLog Analyzer Home>/bin* directory. Execute the **shutdown.sh** file.

You will be asked to confirm your choice, after which the EventLog Analyzer server is shut down.

Linux Service:

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

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

```
Stopping ManageEngine EventLog Analyzer X.0...
Stopped ManageEngine EventLog Analyzer X.0
```

Check the status of the service again

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

```
ManageEngine EventLog Analyzer X.0 is not running.
```

Access EventLog Analyzer - Distributed Edition Admin Server

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

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

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

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

Once you log in, check EventLog Analyzer Managed Server event reports, and more.

License Details - Distributed Edition Admin Server

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

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

Sub-editions of Standalone Edition

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

Distributed Edition:

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

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

- **Perpetual model**

  In this model, the licensing is perpetual and a nominal amount is charged as Annual Maintenance and Support (AMS) fee to provide the maintenance, support, and updates.

- **Subscription model**

  In this model, the license is valid for one year and after that the license gets expired. To continue the license should be renewed every year. Annual Maintenance and Support (AMS) fee is included in the subscription price and not charged separately.

Advantages of ManageEngine Licensing

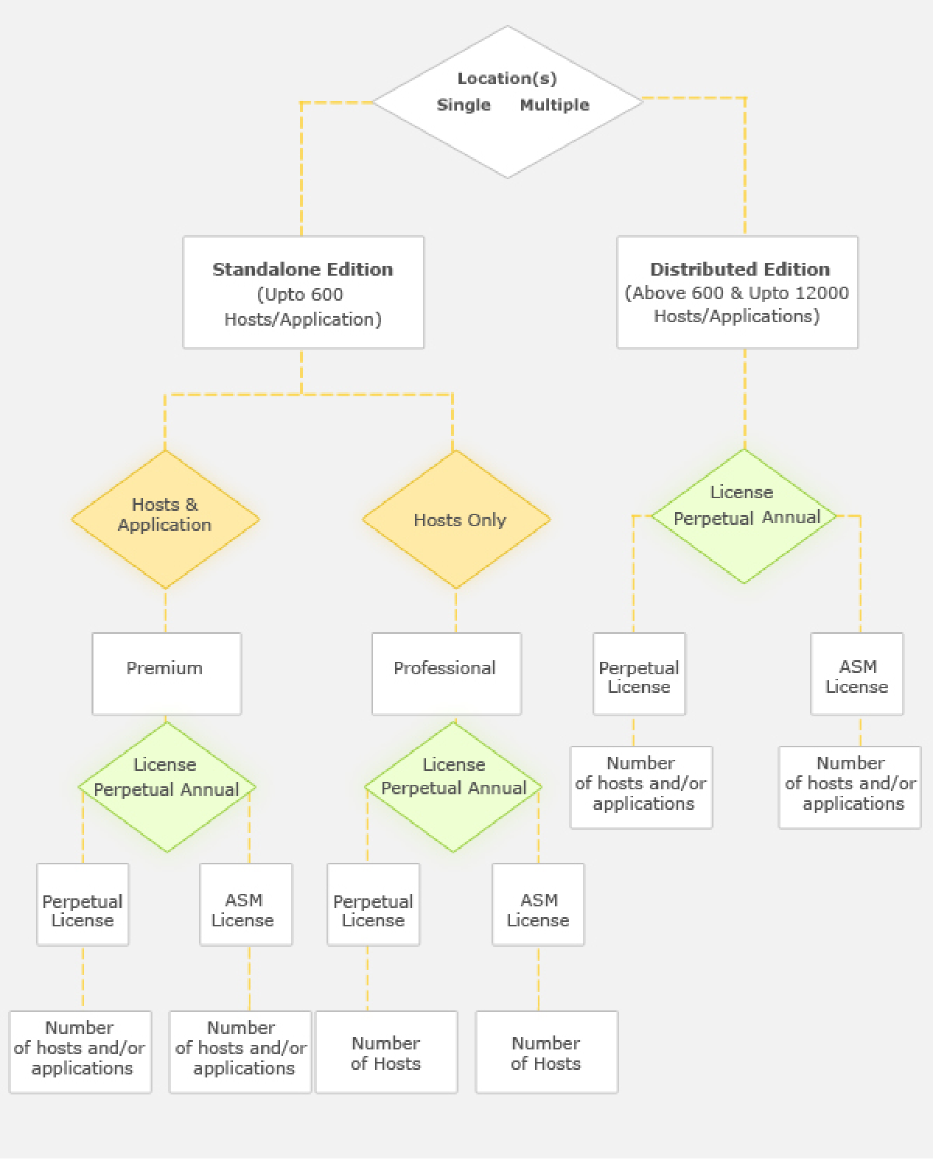
- Simple host/application based, cost conscious, need based licensing

- The 64 bit installation is also of the same price as 32 bit installation
- The Distributed license is applied on the Admin server and there will be no restriction on the number of Managed servers' deployment

How to choose the license

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

Decision Chart to decide EventLog Analyzer Edition



How to upgrade the evaluator license to purchased license

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

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

Display license details

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

- Type of license applied - Free or Professional or Premium
- Number of days remaining for the license to expire

Maximum number of hosts that you are allowed to manage

User Interface

User Interface - Distributed Edition Admin Server

EventLog Analyzer Admin Server client is a web browser based user interface. The advantage is anytime, anywhere access to the client. It is easy to use and navigate. In the client screen, there are tabs for the different functionality. The tabs available are **Home**, **Reports**, **Compliance**, **Search**, **Alerts**, and **Settings**.

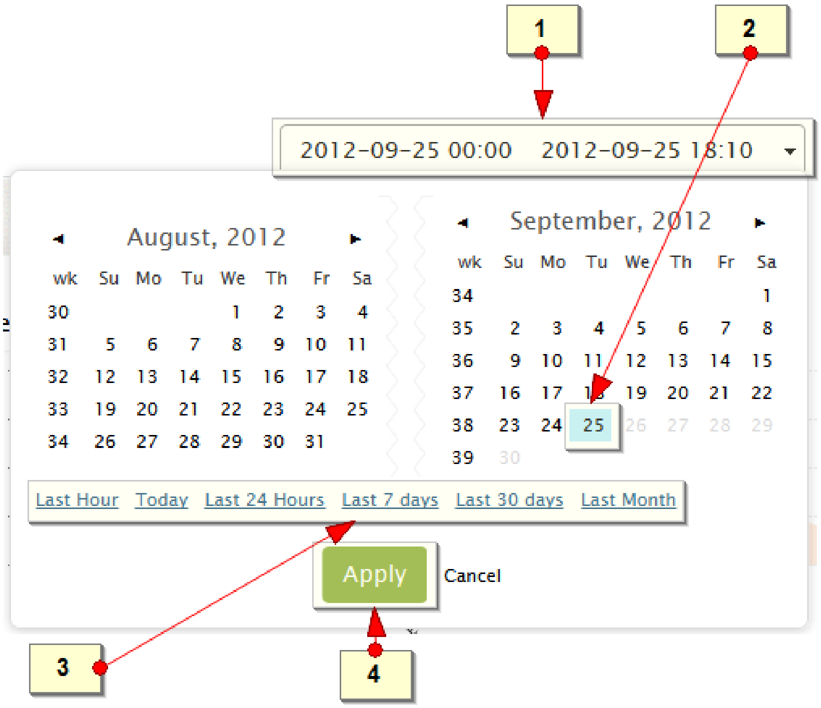
- There is a drop down menu to add a new host, alert, report, filter, and import logs.
- There is a search box available to search the logs.
- During evaluation, there are quick links to get price quote and online purchase the product. For annual subscription licenses, there will be reminder alert before ten days to renew the license.
- There are menu icons to troubleshooting tools to get the details of the EventLog Analyzer listening ports and a Syslog viewer to view the raw packets.
- There is a drop down menu to upgrade the license, contact product support, About the product, user guide, and feedback form.
- There is a calendar element to display the data for the selected time period.

Calendar

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

How to use calendar?

Select a single date



2012-09-25 00:00   2012-09-25 18:10

August, 2012

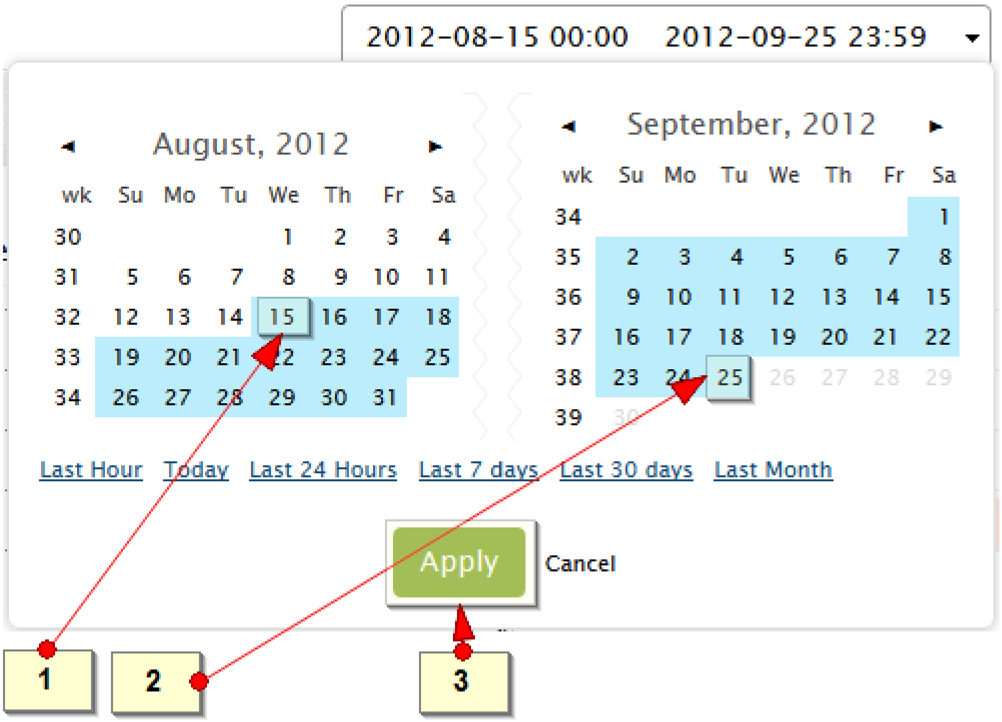
wk	Su	Mo	Tu	We	Th	Fr	Sa
30				1	2	3	4
31	5	6	7	8	9	10	11
32	12	13	14	15	16	17	18
33	19	20	21	22	23	24	25
34	26	27	28	29	30	31	

September, 2012

wk	Su	Mo	Tu	We	Th	Fr	Sa
34							1
35	2	3	4	5	6	7	8
36	9	10	11	12	13	14	15
37	16	17	18	19	20	21	22
38	23	24	25	26	27	28	29
39	30						

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

Select range of days



2012-08-15 00:00 2012-09-25 23:59

August, 2012

wk	Su	Mo	Tu	We	Th	Fr	Sa
30				1	2	3	4
31	5	6	7	8	9	10	11
32	12	13	14	15	16	17	18
33	19	20	21	22	23	24	25
34	26	27	28	29	30	31	

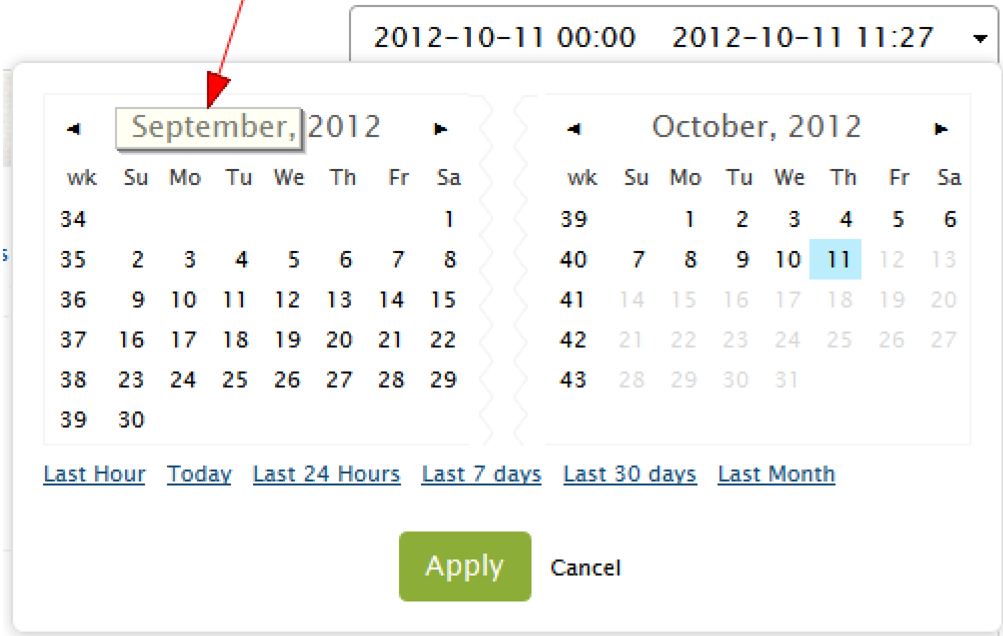
September, 2012

wk	Su	Mo	Tu	We	Th	Fr	Sa
34							1
35	2	3	4	5	6	7	8
36	9	10	11	12	13	14	15
37	16	17	18	19	20	21	22
38	23	24	25	26	27	28	29
39	30						

1. Click on the particular date to be selected as start date. The selection will appear on the top and edit the time if required
2. Click on the particular date to be selected as end date. The selection will appear on the top and edit the time if required. The selected range of days will be highligted in color
3. Click the **Apply** button to complete the date and time range selection

Select across months

Click on month to get the months of the year 2012 listed



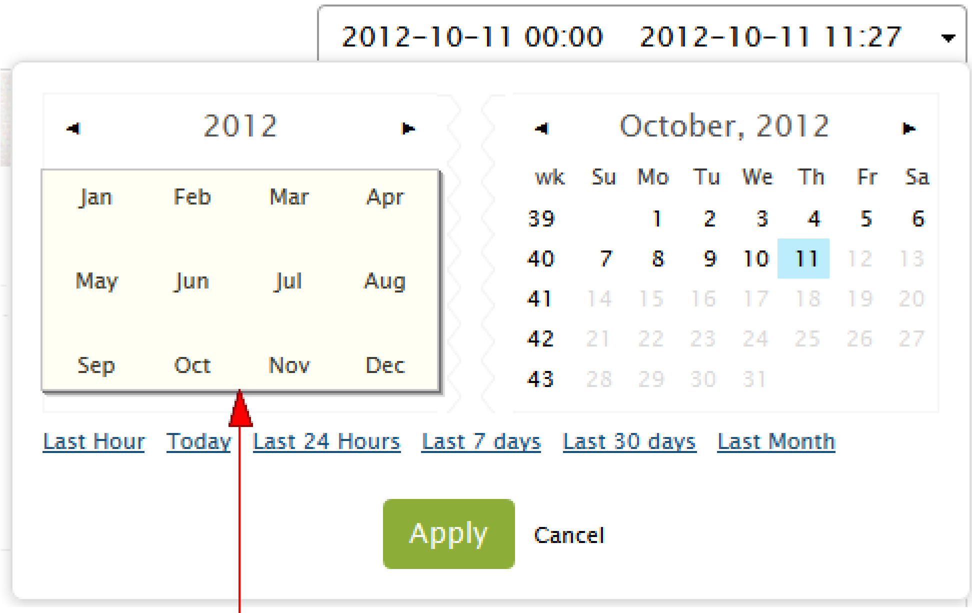
2012-10-11 00:00 2012-10-11 11:27

September, 2012

wk	Su	Mo	Tu	We	Th	Fr	Sa
34							1
35	2	3	4	5	6	7	8
36	9	10	11	12	13	14	15
37	16	17	18	19	20	21	22
38	23	24	25	26	27	28	29
39	30						

October, 2012

wk	Su	Mo	Tu	We	Th	Fr	Sa
39		1	2	3	4	5	6
40	7	8	9	10	11	12	13
41	14	15	16	17	18	19	20
42	21	22	23	24	25	26	27
43	28	29	30	31			



2012-10-11 00:00 2012-10-11 11:27

2012

Jan	Feb	Mar	Apr
May	Jun	Jul	Aug
Sep	Oct	Nov	Dec

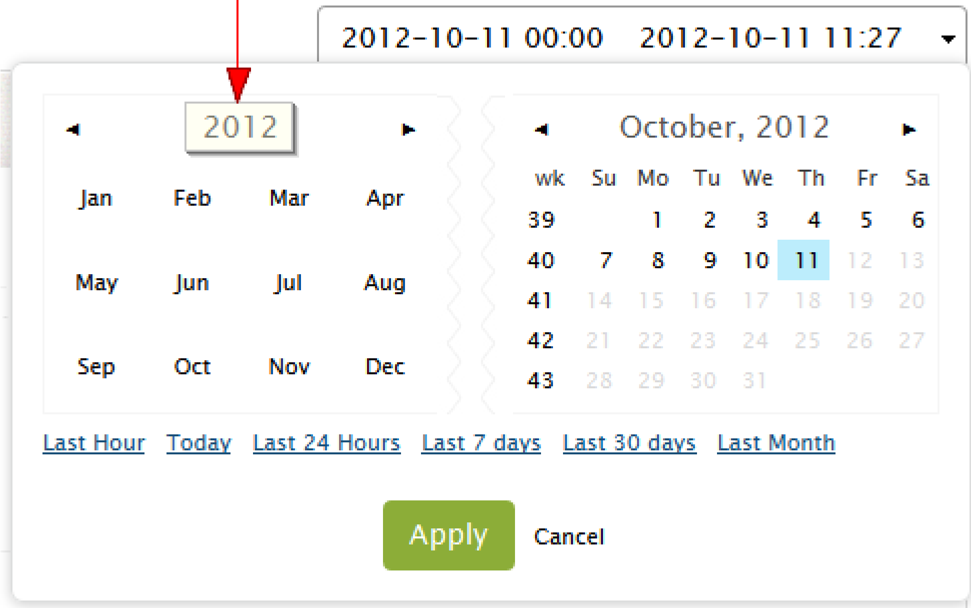
October, 2012

wk	Su	Mo	Tu	We	Th	Fr	Sa
39		1	2	3	4	5	6
40	7	8	9	10	11	12	13
41	14	15	16	17	18	19	20
42	21	22	23	24	25	26	27
43	28	29	30	31			

Months of the year listed

Select across years

Click on the year to get prior 6 & later 5 years listed

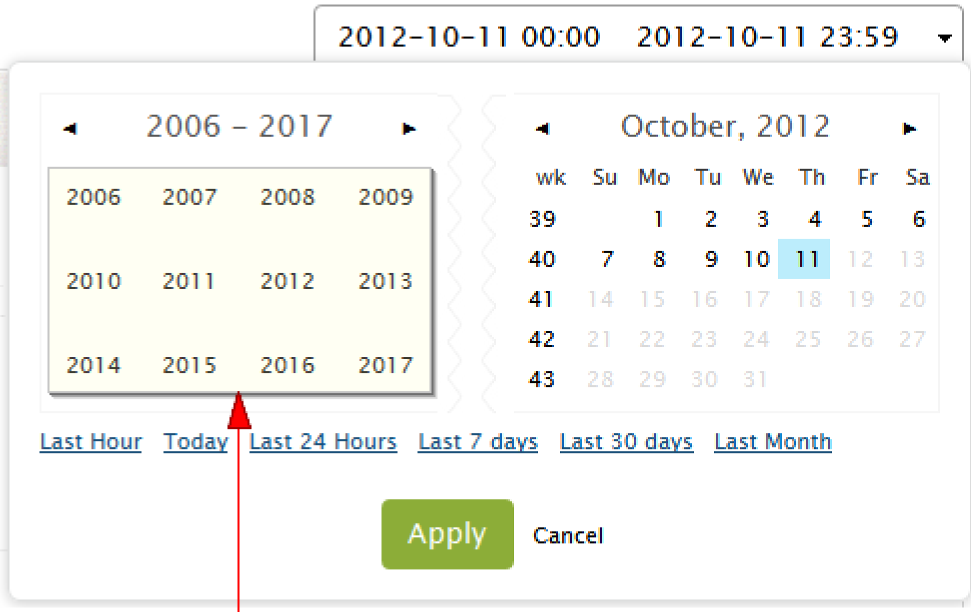


2012-10-11 00:00 2012-10-11 11:27

◂	2012		▸
Jan	Feb	Mar	Apr
May	Jun	Jul	Aug
Sep	Oct	Nov	Dec

◂ October, 2012 ▸

wk	Su	Mo	Tu	We	Th	Fr	Sa
39		1	2	3	4	5	6
40	7	8	9	10	11	12	13
41	14	15	16	17	18	19	20
42	21	22	23	24	25	26	27
43	28	29	30	31			



2012-10-11 00:00 2012-10-11 23:59

◂ 2006 – 2017 ▸

2006	2007	2008	2009
2010	2011	2012	2013
2014	2015	2016	2017

◂ October, 2012 ▸

wk	Su	Mo	Tu	We	Th	Fr	Sa
39		1	2	3	4	5	6
40	7	8	9	10	11	12	13
41	14	15	16	17	18	19	20
42	21	22	23	24	25	26	27
43	28	29	30	31			

Prior 6 & later 5 years to the current year gets listed

User Interface Tabs - Distributed Edition Admin Server

In the EventLog Analyzer client screen, there are tabs for the different functionality. The tabs are:

- Home
- Reports
- Compliance
- Search
- Alerts
- Settings

Home tab

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

Dashboard

EventLog Analyzer dashboard is loaded with useful graphs. The graphs are **All Events**, **Alerts**, **Important Events**, **Event Category**, **Security Events**, and **Log Trend**. It is customizable and can present a user specific segmented view. Each user can create dashboard profiles. A profile can have one or more host groups. The default profile is 'All Groups' and this profile cannot be deleted.

Hosts

All the profiles of the dashboard are available for **Hosts** tab also. New hosts can be added. New report can be created/ scheduled. All the hosts added to EventLog Analyzer are listed. Bulk of hosts can be disabled or deleted. Hostname or IP address can be viewed for hosts. The host type, event summary, connection status of the host, last time the log was fetched, and host group to which the host is assigned are displayed in the table. The table columns can be customized. Number of lines per page view can be set. Standard page navigations icons are present.

Applications

The applications are grouped based on the log format and each group of applications can be viewed separately. New Oracle, Print Server applications can be added. New application logs can be imported. There is a link to view the logs imported in to EventLog Analyzer. All the application logs imported to EventLog Analyzer are listed. Bulk of application logs can be deleted. Associated host is displayed for the application logs. Click on the hosts to drill down to the events specific to the application logs of the host. The application type, total events, number of recent records imported, last log imported time, start time, and end time are displayed in the table. Click on the event count to drill down to the raw logs. The table

columns can be customized. Number of lines per page view can be set.
Standard page navigations icons are present.

Reports tab

The custom reports and canned reports are displayed in the Reports tab. Custom report can be created, modified, deleted, scheduled, rescheduled and the report profiles can be imported, exported.

The pre-built reports available are top N reports, user activity reports, trend reports, detailed application reports, and detailed host reports. The top N reports covers the most number of, user accessed hosts, logged in users, interactive logins, hosts based on event severity, and processes based on event severity.

Compliance tab

The Compliance tab displays the compliance reports for various regulatory compliance acts. The acts are PCI-DSS, FISMA, HIPAA, SOX, and GLBA. Various sections of the acts covered by each report are described. Modify the existing compliance reports to suit specific requirements. Add a new compliance report. This is a futuristic feature, which will be useful when a new compliance mandate comes into force.

Search tab

The Search tab allows to search the logs in two modes **Basic** and **Advanced**. The search result is displayed in this pages and the result can be saved as EventLog Analyzer reports. Use 'Basic' search to search a value directly, field value pairs with relational operators. Number of field value pairs can be grouped and associated using boolean operators. Use 'Advanced' search to form the search query with field value pairs with relational operators. The fields can be grouped with boolean operators.
From both the search results, new, additional fields can be extracted to get them indexed and searched.

Alerts tab

The Alerts tab displays all the alert profiles and alerts generated by EventLog Analyzer. New alert profiles can be created and existing alert profiles can be disabled, modified, and deleted. The alert profiles can be exported and imported.

Settings tab

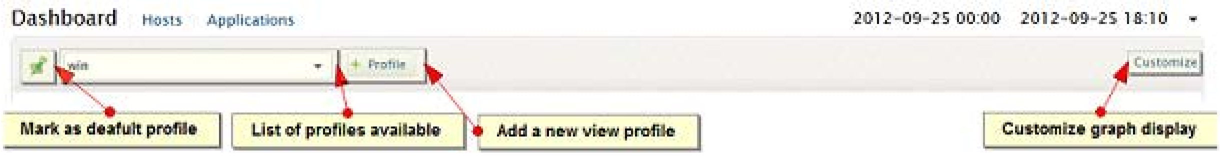
The Settings tab allows various kinds of configuration settings which can be carried out in EventLog Analyzer. It has three sections, Configurations and Settings.

Configuration
In this section, Managed Server Settings, Manage Hosts, Import, Archive, Report Profiles, Alerts, Database Filter, Dashboard Profiles, and Ask ME reports are available.

Settings
In this section, Manage User, DB Storage Settings, External Authentication, Server Diagnostics, and Rebranding are available.

Customize Dashboard Views - Distributed Edition Admin Server

EventLog Analyzer dashboard is customizable and can present a user specific segmented view. Each user can create dashboard profiles. A profile can have one or more host groups. The default profile is '**All Groups**' and this profile cannot be deleted. Even custom profiles created is set as deafult cannot be deleted. If a default profile needs to be deleted, assign a different profile as default one and then delete the required profile.



On the dashboard, all the profiles are listed, any view profile can be selected for display and it can set as default profile. Create a new profile using **+ Profile** button.

Customize dashboard graph display

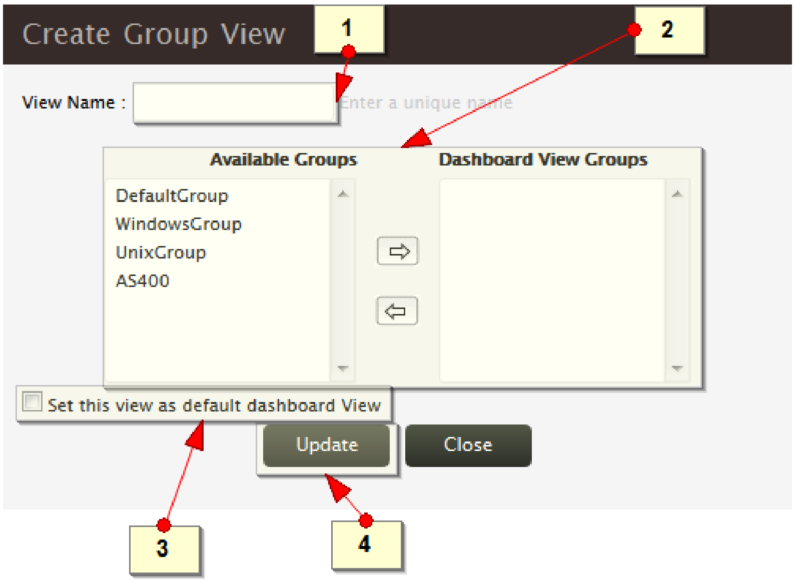
The graphs displayed in the dashboard are, **All Events**, **Alerts**, **Important Events**, **Event Category**, **Security Events**, and **Log Trend**. The graphs can be selectively displayed in the dashboard using the **Customize** link.

How to create dashboard profile

Create dashboard profile in EventLog Analyzer using the following menu:

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

The procedure to create dasboard profile is given below:



1. Enter a unique view name for the new dashboard view profile
2. Select the host group(s) to add to this profile. Use the left to right arrow to add the host group(s) (move the host group(s) from the Available Group(s) list to Dashboard View Group(s) list) and right to left arrow to remove the host group(s) (move the host group(s) from the Dashboard View Group(s) list to Available Group(s) list)
3. Select the '**Set this view as default dashboard view**' check box to set this newly created profile as default profile for the dashboard
4. Use **Update** button to save the new dashboard profile

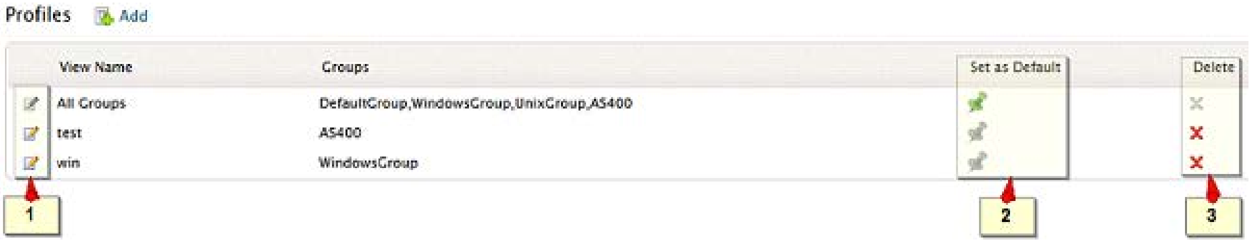
How to edit/ delete dashboard profile

Create dashboard profile in EventLog Analyzer using the following menu:

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

Profiles

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



Profiles Add

	View Name	Groups	Set as Default	Delete
✎	All Groups	DefaultGroup,WindowsGroup,UnixGroup,AS400	📌	✕
✎	test	AS400	📌	✕
✎	win	WindowsGroup	📌	✕

1. **How to edit a profile?**

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

2. **How to set it as default profile?**

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

3. **How to delete a profile?**

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

Event Reports

EventLog Analyzer Reports

EventLog Analyzer offers highly flexible custom reports. It provides a powerful set of canned reports. The reports can be scheduled using a new scheduler or an existing scheduler. The custom report profiles can be exported to XML files and can be imported to the same or different server.

Reports are displayed in the **Reports** tab of the UI. The reports can be scheduled as and when required, the event counts can be drilled down to get the raw logs, and filtered based on event severity

Description of reports

- **My Reports**

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

- **Top N Reports**

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

- **User Activity Reports**

  These reports present the overview of user activities and user wise activity. The overview report of user activities can be filtered for hosts. The user wise activity report can be filtered for hosts, users, and reports

- **Trend Reports**

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

- **Detailed Application Reports**

  The application reports display each application specific number of events. The applications are, **MS IIS W3C Web Server, MS IIS W3C FTP Server, Apache Web Server, DHCP Windows Server, DHCP Linux**

Server, Print Server, MS SQL Database Server, and Oracle Database Server

- **Detailed Hosts Reports**

  The General Summary of host report displays the number of events of each type that have been generated by that host in the selected time period.

  Important Events

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

  All Events

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

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

Host Reports

All the events generated by a host, are collected, aggregated, and grouped under different categories before displaying them in graphs and reports.
From any tab, click on the host name to see a **General Summary** for that host. The General Summary shows you the number of events of each type that have been generated by that host in the selected time period. You can then click on the event count against each event type to see the exact event that was generated.

Important Events tab:

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

All Events tab:

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

Application Log Reports

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

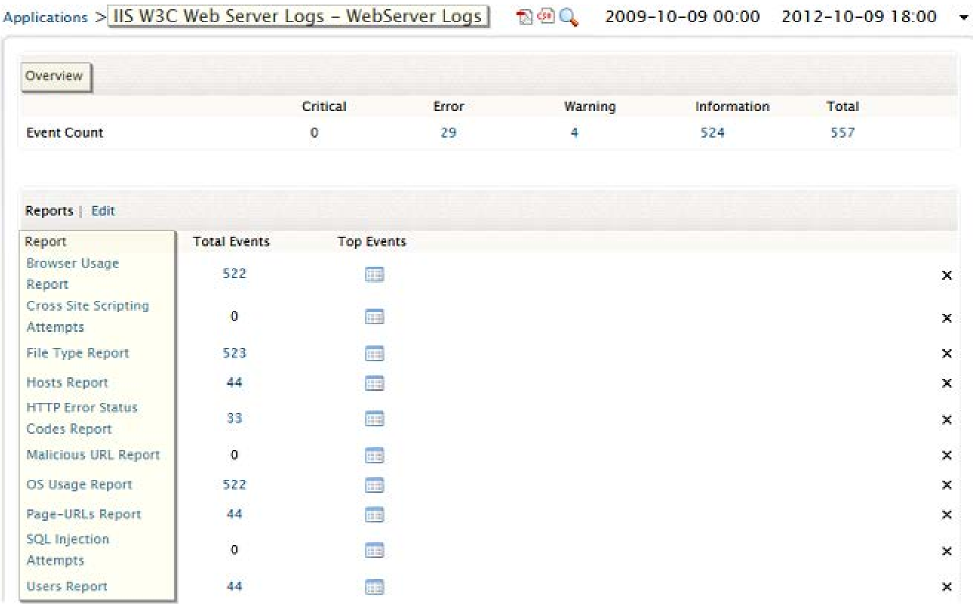
- **Home** tab > **Applications** > Host Name: **<host name of the machine associated with application>**
- **Reports** tab > Detailed Application Reports section > View Report: **<Application Name> Logs**

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

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

Reports for MS IIS W3C Web Server Logs

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



Applications > IIS W3C Web Server Logs – WebServer Logs 2009-10-09 00:00 2012-10-09 18:00

Overview

	Critical	Error	Warning	Information	Total
Event Count	0	29	4	524	557

Reports | Edit

Report	Total Events	Top Events	
Browser Usage Report	522	▦	×
Cross Site Scripting Attempts	0	▦	×
File Type Report	523	▦	×
Hosts Report	44	▦	×
HTTP Error Status Codes Report	33	▦	×
Malicious URL Report	0	▦	×
OS Usage Report	522	▦	×
Page-URLs Report	44	▦	×
SQL Injection Attempts	0	▦	×
Users Report	44	▦	×

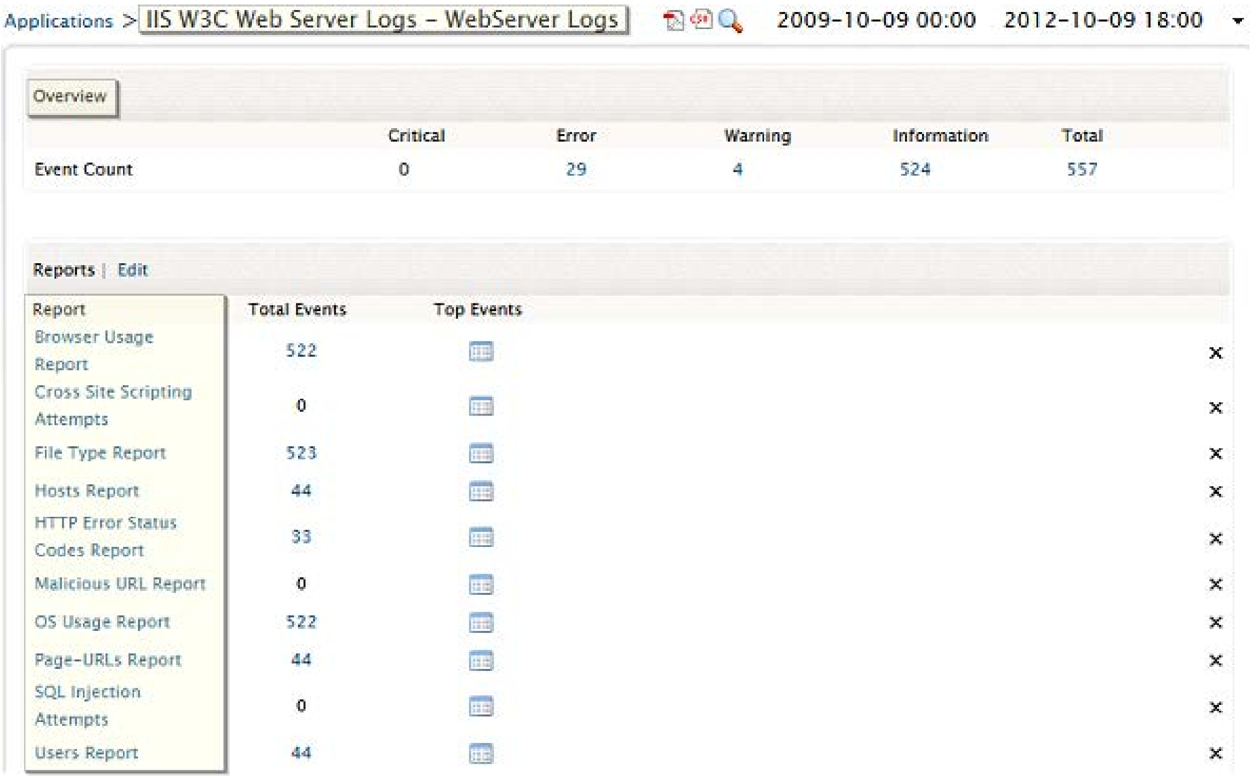
The **Overview** section on top of the page displays the event count in the **Event Count** table. In the table event count is classified based on the severity *Critical, Error, Warning, Information*, and *Total* and displayed in the columns of the table. Below the Event Count table, the page displays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

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

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

Reports for MS IIS W3C FTP Server Logs

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



Applications > IIS W3C Web Server Logs – WebServer Logs 2009-10-09 00:00 2012-10-09 18:00

Overview

	Critical	Error	Warning	Information	Total
Event Count	0	29	4	524	557

Reports | Edit

Report	Total Events	Top Events	
Browser Usage Report	522	▦	×
Cross Site Scripting Attempts	0	▦	×
File Type Report	523	▦	×
Hosts Report	44	▦	×
HTTP Error Status Codes Report	33	▦	×
Malicious URL Report	0	▦	×
OS Usage Report	522	▦	×
Page-URLs Report	44	▦	×
SQL Injection Attempts	0	▦	×
Users Report	44	▦	×

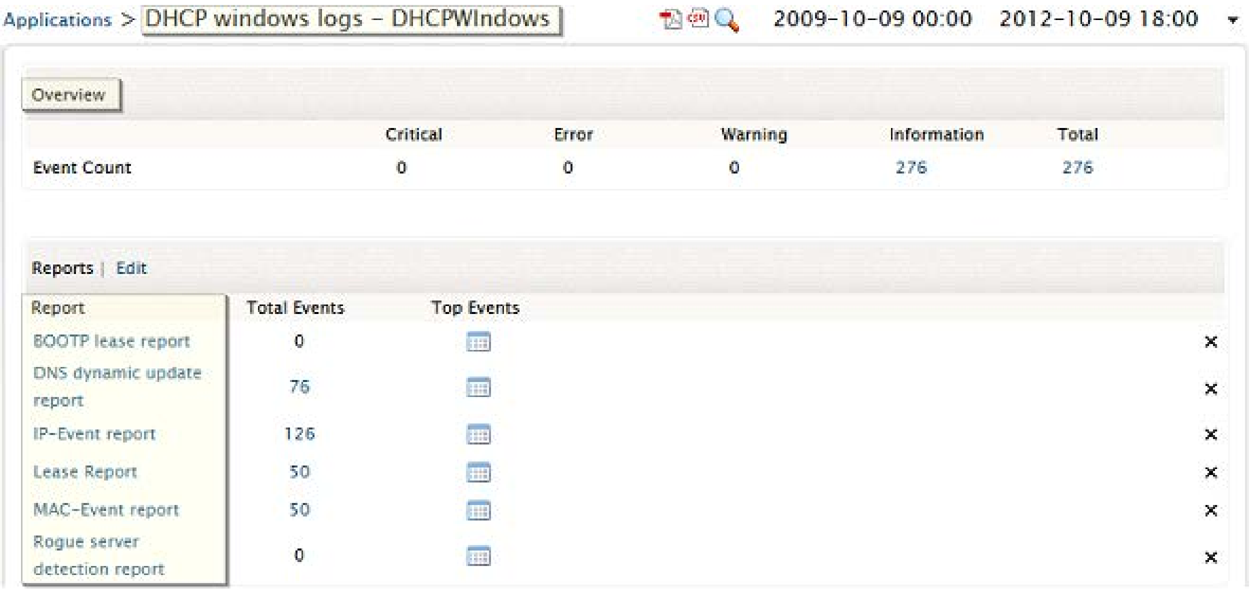
The **Overview** section on top of the page displays the event count in the **Event Count** table. In the table event count is classified based on the severity *Critical, Error, Warning, Information*, and *Total* and displayed in the columns of the table. Below the Event Count table, the page displays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

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

- Server IPs Report - the details covered in this report are: Server IP Address, File Transfers, Bytes Sent, Bytes Received, and Events
- Source Port Report - the details covered in this report are: Server Port, File Transfers, Bytes Sent, Bytes Received, and Events

Reports for DHCP Windows Server Logs

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



Applications > DHCP windows logs – DHCPWIndows

2009-10-09 00:00   2012-10-09 18:00

Overview

	Critical	Error	Warning	Information	Total
Event Count	0	0	0	276	276

Reports | Edit

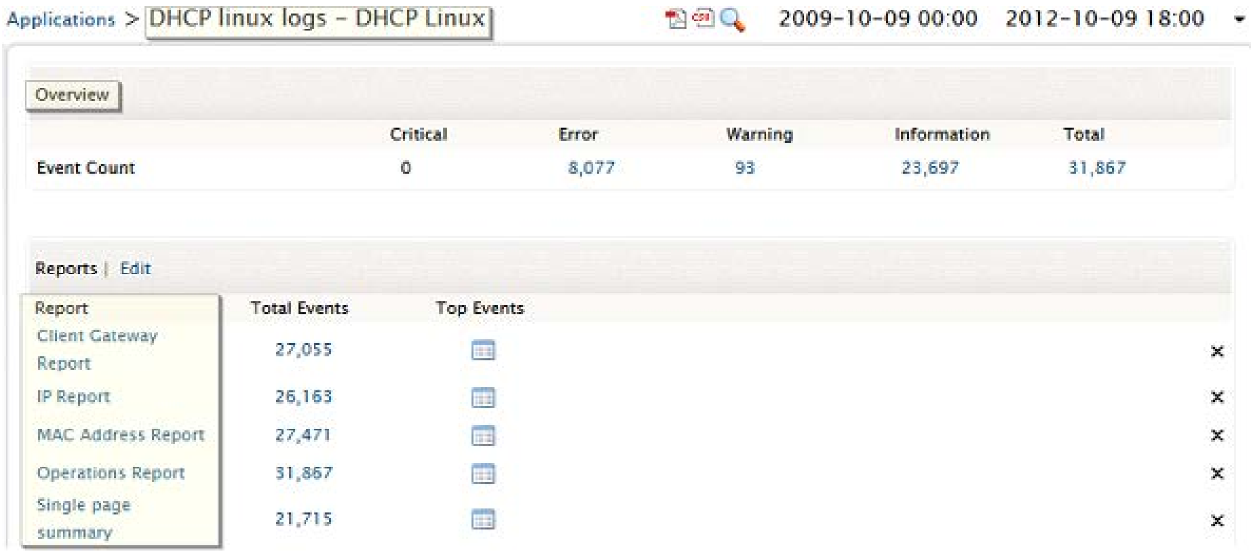
Report	Total Events	Top Events	
BOOTP lease report	0	▦	×
DNS dynamic update report	76	▦	×
IP-Event report	126	▦	×
Lease Report	50	▦	×
MAC-Event report	50	▦	×
Rogue server detection report	0	▦	×

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

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

Reports for DHCP Linux Server Logs

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



Applications > DHCP linux logs - DHCP Linux   2009-10-09 00:00   2012-10-09 18:00

Overview

	Critical	Error	Warning	Information	Total
Event Count	0	8,077	93	23,697	31,867

Reports | Edit

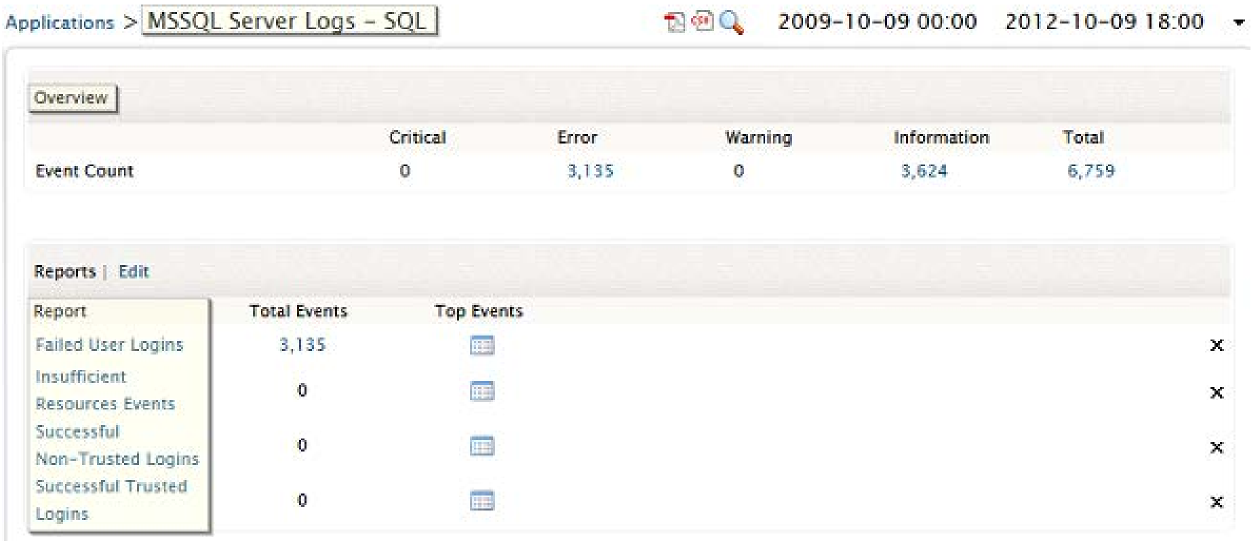
Report	Total Events	Top Events	
Client Gateway Report	27,055	▦	✕
IP Report	26,163	▦	✕
MAC Address Report	27,471	▦	✕
Operations Report	31,867	▦	✕
Single page summary	21,715	▦	✕

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

- Operations Report - the details covered in this report are: Operation and Events. The operations are: DHCPREQUEST, DHCPNAK, DHCPDISCOVER, DHCPOFFER, DHCPACK, DHCPINFORM, if IN, delete, Wrote, DHCPRELEASE, and Abandoning IP
- MAC-Event report - the details covered in this report are: MAC Address and Events
- Client Gateway Report - the details covered in this report are: Gateway and Events
- IP-Event report - the details covered in this report are: IP Address and Events
- Single Page Summary Report - the details covered in this report are: Logging device, Operation, IP Address, MAC Address, Gateway, and Events

Reports for MS SQL Server Logs

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



Applications > MSSQL Server Logs - SQL

2009-10-09 00:00 2012-10-09 18:00

Overview

	Critical	Error	Warning	Information	Total
Event Count	0	3,135	0	3,624	6,759

Reports | Edit

Report	Total Events	Top Events	
Failed User Logins	3,135	▦	×
Insufficient Resources Events	0	▦	×
Successful Non-Trusted Logins	0	▦	×
Successful Trusted Logins	0	▦	×

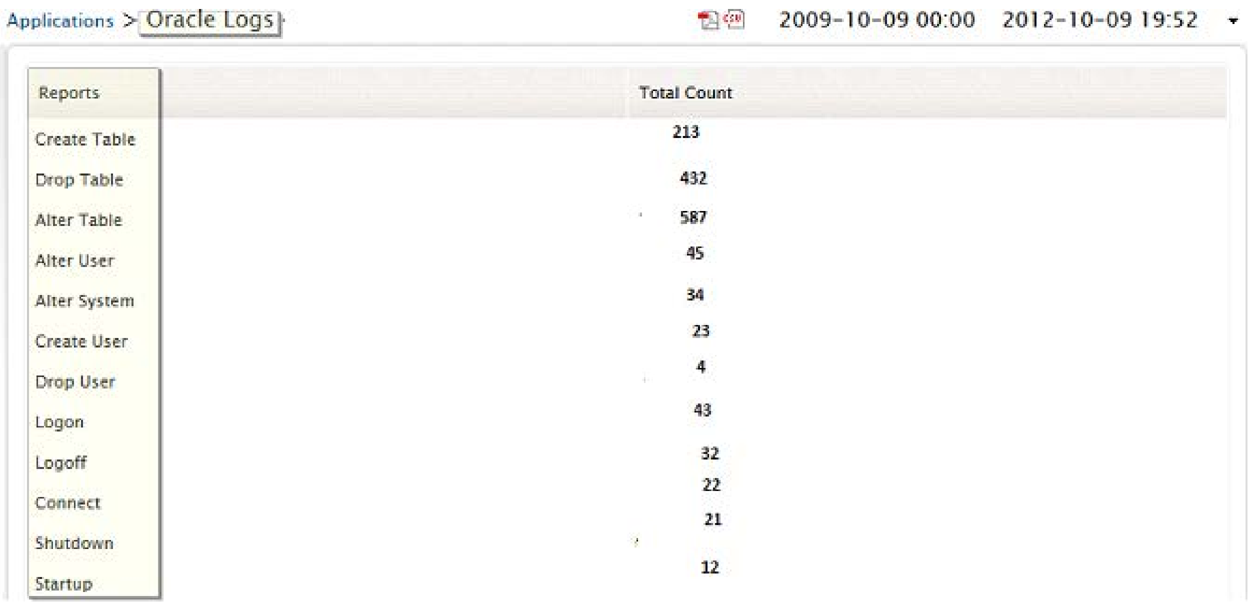
The **Overview** section on top of the page displays the event count in the **Event Count** table. In the table event count is classified based on the severity *Critical, Error, Warning, Information*, and *Total* and displayed in the columns of the table. Below the Event Count table, the page displays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

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

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

Reports for Oracle Audit Logs

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



Applications > Oracle Logs

2009-10-09 00:00 2012-10-09 19:52

Reports	Total Count
Create Table	213
Drop Table	432
Alter Table	587
Alter User	45
Alter System	34
Create User	23
Drop User	4
Logon	43
Logoff	32
Connect	22
Shutdown	21
Startup	12

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

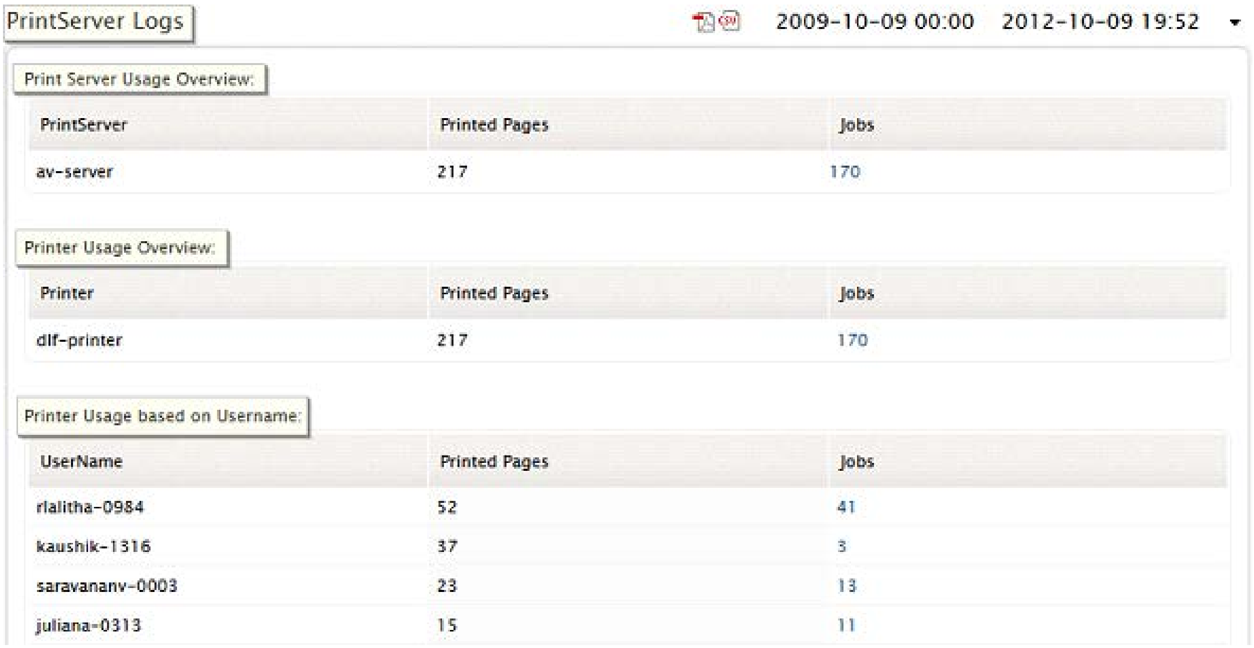
EventLog Analyzer generates the following pre-defined reports for Oracle database server application logs:

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

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

Reports for Print Server Logs

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



Print Server Usage Overview:

PrintServer	Printed Pages	Jobs
av-server	217	170

Printer Usage Overview:

Printer	Printed Pages	Jobs
dlf-printer	217	170

Printer Usage based on Username:

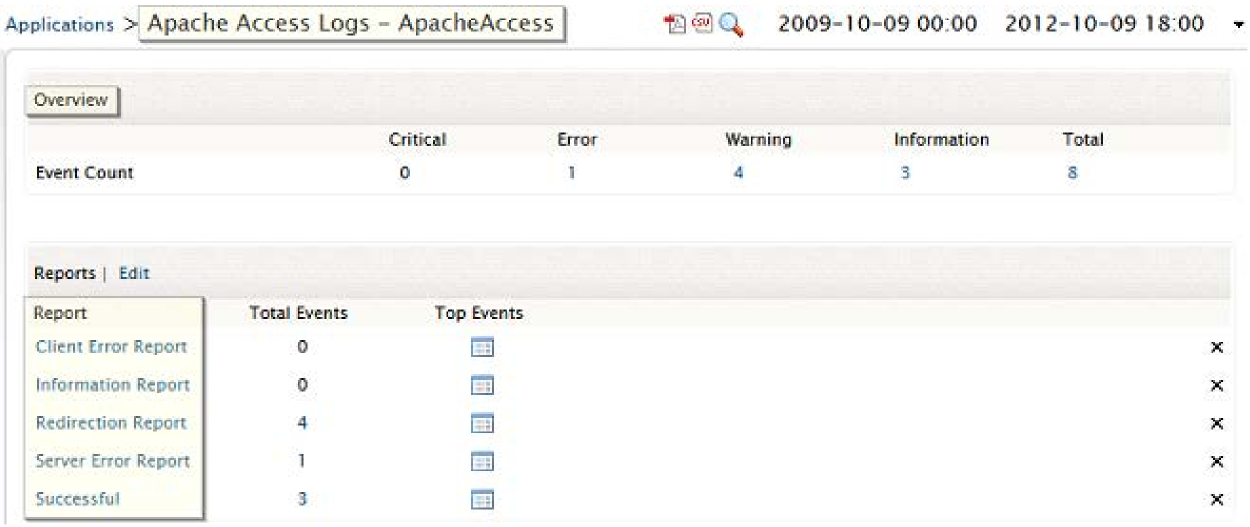
UserName	Printed Pages	Jobs
rlalitha-0984	52	41
kaushik-1316	37	3
saravananv-0003	23	13
juliana-0313	15	11

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

- Print Server Hosts Overview - the details covered in this report are: Print Servers and Job Count
- Print Server Usuage Overview - the details covered in this report are: Print Server, Printed Pages, and Jobs
- Printer Usuage Overview - the details covered in this report are: Printer, Printed Pages, and Jobs
- Printer Usuage based on User Name - the details covered in this report are: User Name, Printed Pages, and Jobs
- Print Job Reports - the details covered in this report are: Reports and Total Counts and the Reports are, Print Usuage, Paused Document, Resumed Document, Deleted Documen, Moved Document, Timed Out Document, Corrupted Document, Priority Changed Document, and Insufficient Privilege Document

Reports for Apache Web Server Logs

Clicking the **View Report** link opens the **Reports for Apache Web Server Logs** page.



	Critical	Error	Warning	Information	Total
Event Count	0	1	4	3	8

Report	Total Events	Top Events	
Client Error Report	0	▦	×
Information Report	0	▦	×
Redirection Report	4	▦	×
Server Error Report	1	▦	×
Successful	3	▦	×

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

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

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

View Top Hosts Reports

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

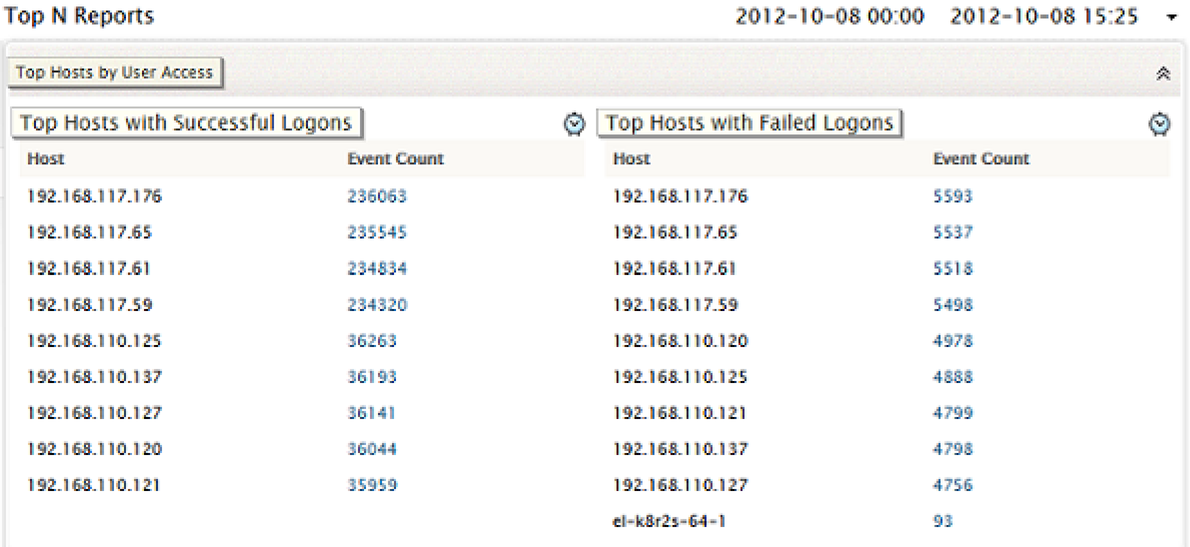
- **Reports** tab > **Top N Reports**

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

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

Top Hosts by User Access

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



Top Hosts with Successful Logons

Host	Event Count
192.168.117.176	236063
192.168.117.65	235545
192.168.117.61	234834
192.168.117.59	234320
192.168.110.125	36263
192.168.110.137	36193
192.168.110.127	36141
192.168.110.120	36044
192.168.110.121	35959

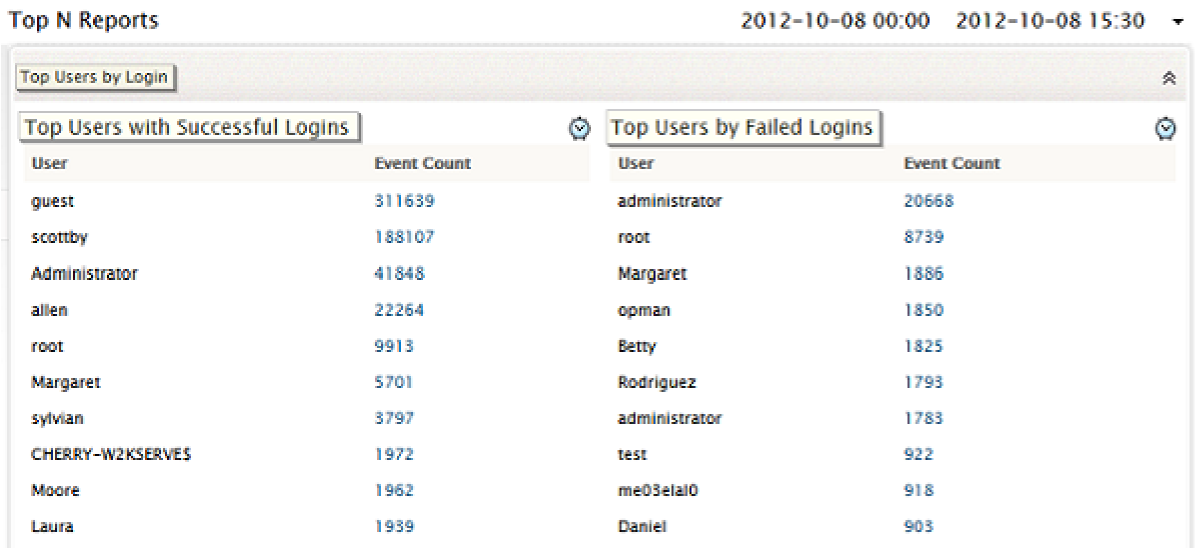
Top Hosts with Failed Logons

Host	Event Count
192.168.117.176	5593
192.168.117.65	5537
192.168.117.61	5518
192.168.117.59	5498
192.168.110.120	4978
192.168.110.125	4888
192.168.110.121	4799
192.168.110.137	4798
192.168.110.127	4756
el-k8r2s-64-1	93

While the former is useful in tracking usage trends of hosts, the latter is important in analyzing which hosts are subject to the most number of security breaches.
You can use this report to decide if security policies need to be changed with respect to certain hosts, or tighten security measures across the network.

Top Users by Login

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



Top N Reports 2012-10-08 00:00 2012-10-08 15:30

Top Users by Login

Top Users with Successful Logins

User	Event Count
guest	311639
scottby	188107
Administrator	41848
allen	22264
root	9913
Margaret	5701
sylvian	3797
CHERRY-W2KSERVE$	1972
Moore	1962
Laura	1939

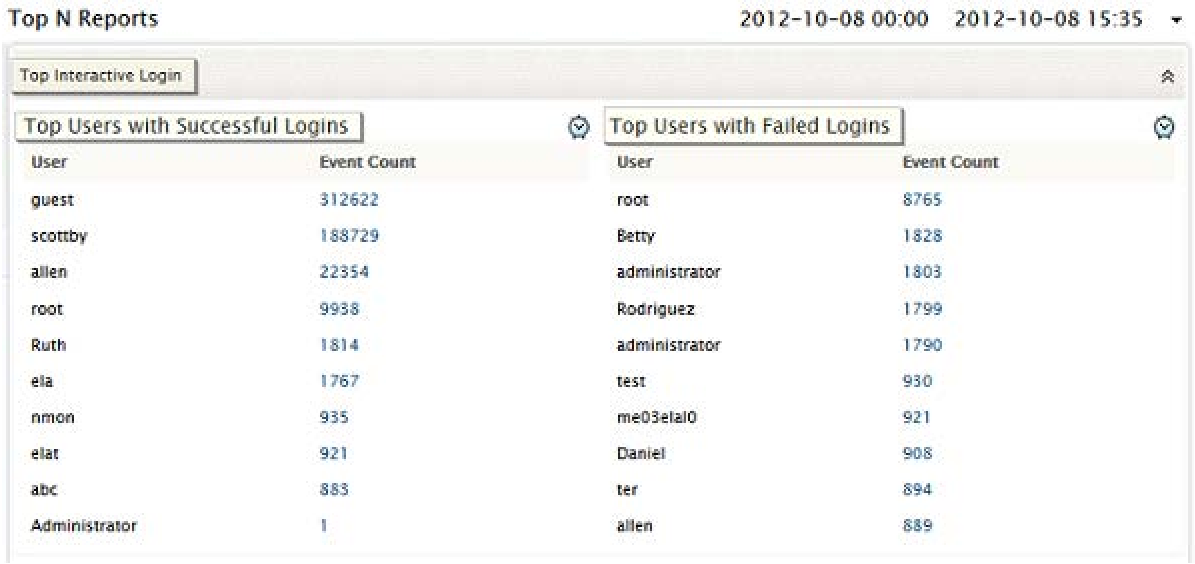
Top Users by Failed Logins

User	Event Count
administrator	20668
root	8739
Margaret	1886
opman	1850
Betty	1825
Rodriguez	1793
administrator	1783
test	922
me03elal0	918
Daniel	903

This report tells you which user logged into which host, using the password, and whether the user was successful or not. If a user has been accessing several hosts with the user name and password, this report will show you which hosts were used, and when. If the user has tried to log on, but was unsuccessful, this report will show you how many times the user was unsuccessful, on which hosts did the user try, and when.
You can use this report to identify errant users on the network, and set up security policies to track such users.

Top Interactive Login

In this report, only the logins done interactively through the UI. This report shows the users with maximum number of successful logins, and the users with maximum number of failed login attempts. This report tells you which user logged into which host, using the password, and whether the user was successful or not.



Top N Reports 2012-10-08 00:00 2012-10-08 15:35

Top Interactive Login

Top Users with Successful Logins

User	Event Count
guest	312622
scottby	188729
allen	22354
root	9938
Ruth	1814
ela	1767
nmon	935
elat	921
abc	883
Administrator	1

Top Users with Failed Logins

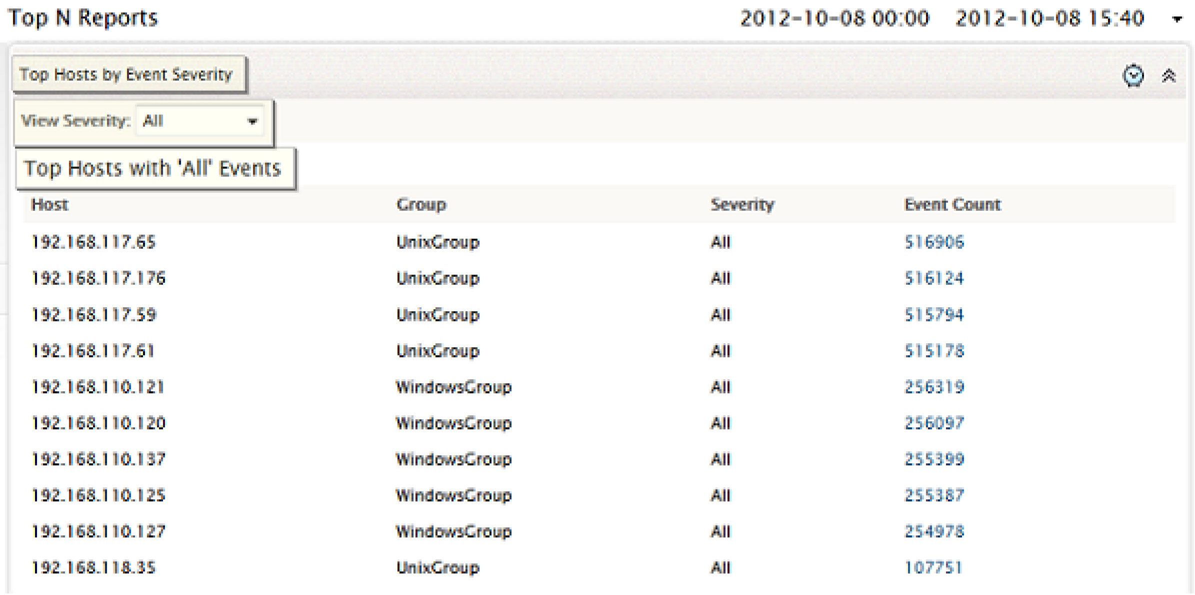
User	Event Count
root	8765
Betty	1828
administrator	1803
Rodriguez	1799
administrator	1790
test	930
me03elal0	921
Daniel	908
ter	894
allen	889

If a user has been accessing several hosts with the user name and password, this report will show you which hosts were used, and when. If the user has tried to log in, but was unsuccessful, this report will show you how many times the user was unsuccessful, on which hosts did the user try, and when.

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

Top Hosts by Event Severity

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



Top N Reports 2012-10-08 00:00 2012-10-08 15:40

Top Hosts by Event Severity

View Severity: All

Top Hosts with 'All' Events

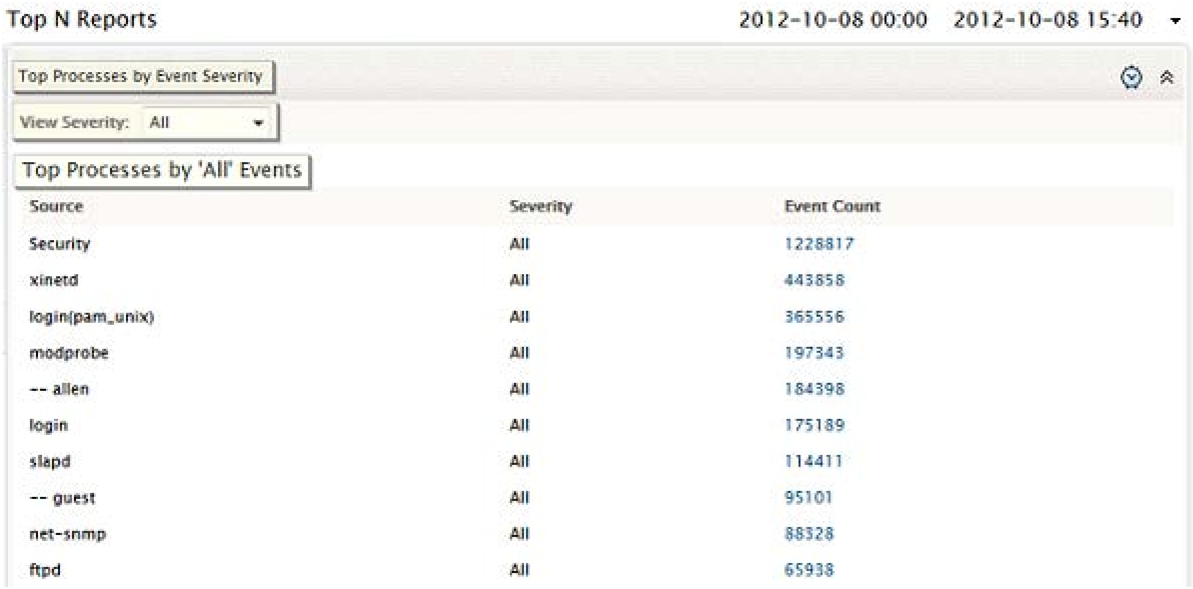
Host	Group	Severity	Event Count
192.168.117.65	UnixGroup	All	516906
192.168.117.176	UnixGroup	All	516124
192.168.117.59	UnixGroup	All	515794
192.168.117.61	UnixGroup	All	515178
192.168.110.121	WindowsGroup	All	256319
192.168.110.120	WindowsGroup	All	256097
192.168.110.137	WindowsGroup	All	255399
192.168.110.125	WindowsGroup	All	255387
192.168.110.127	WindowsGroup	All	254978
192.168.118.35	UnixGroup	All	107751

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

Note: Some event severity are applicable only to Unix hosts

Top Processes by Event Severity

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



Source	Severity	Event Count
Security	All	1228817
xinetd	All	443858
login(pam_unix)	All	365556
modprobe	All	197343
-- allen	All	184398
login	All	175189
slapd	All	114411
-- guest	All	95101
net-snmp	All	88328
ftpd	All	65938

You can use this report to identify the processes with problems, investigate suspicious behavior of critical hosts, determine if there has been a worm or virus attack in the network, and also see which hosts have been affected, thereby reducing network downtime.

User Activity (PUMA) Reports

To view user activity reports use the following menu option:

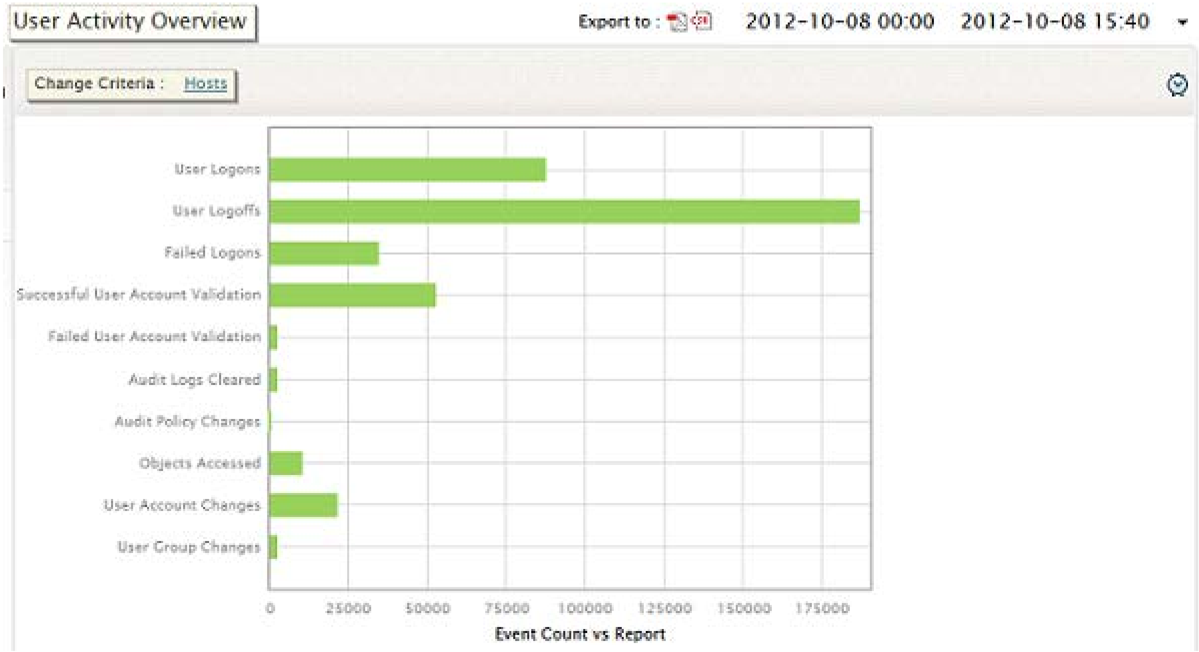
- **Reports** tab > **User Activity Reports**

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

- User Activity - Overview
- User based Activity Reports

User Activity - Overview

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



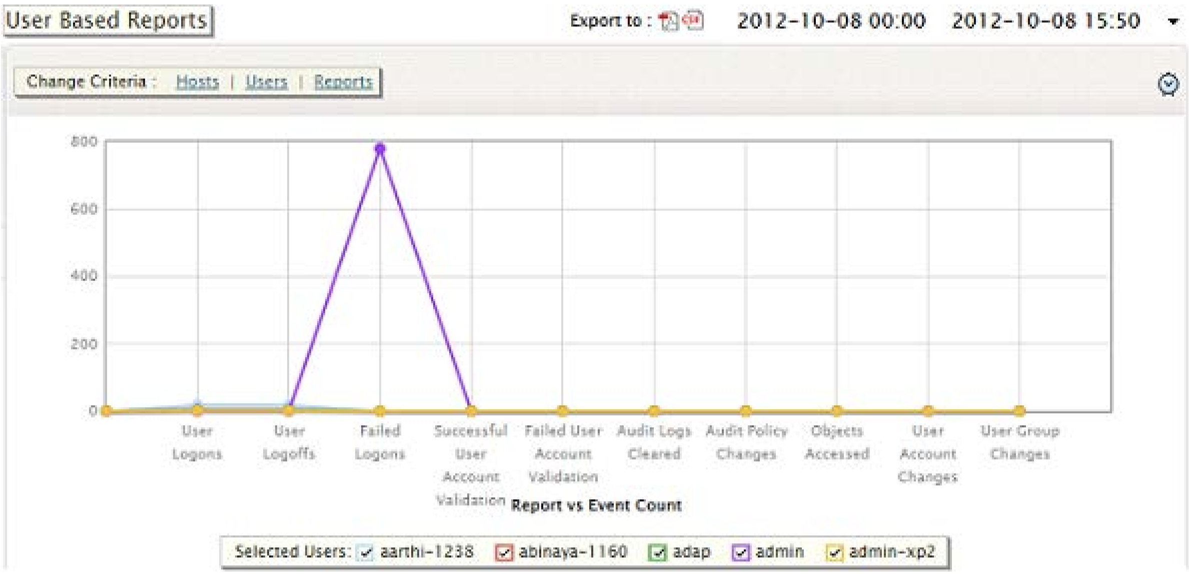
The list of user activity reports are:

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

- Audit Policy Changes
- Objects Accessed
- User Account Changes
- User Group Changes

User based Activity Reports

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



The list of user activity reports are:

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

Trend Reports

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

To view trend reports use the following menu option:

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

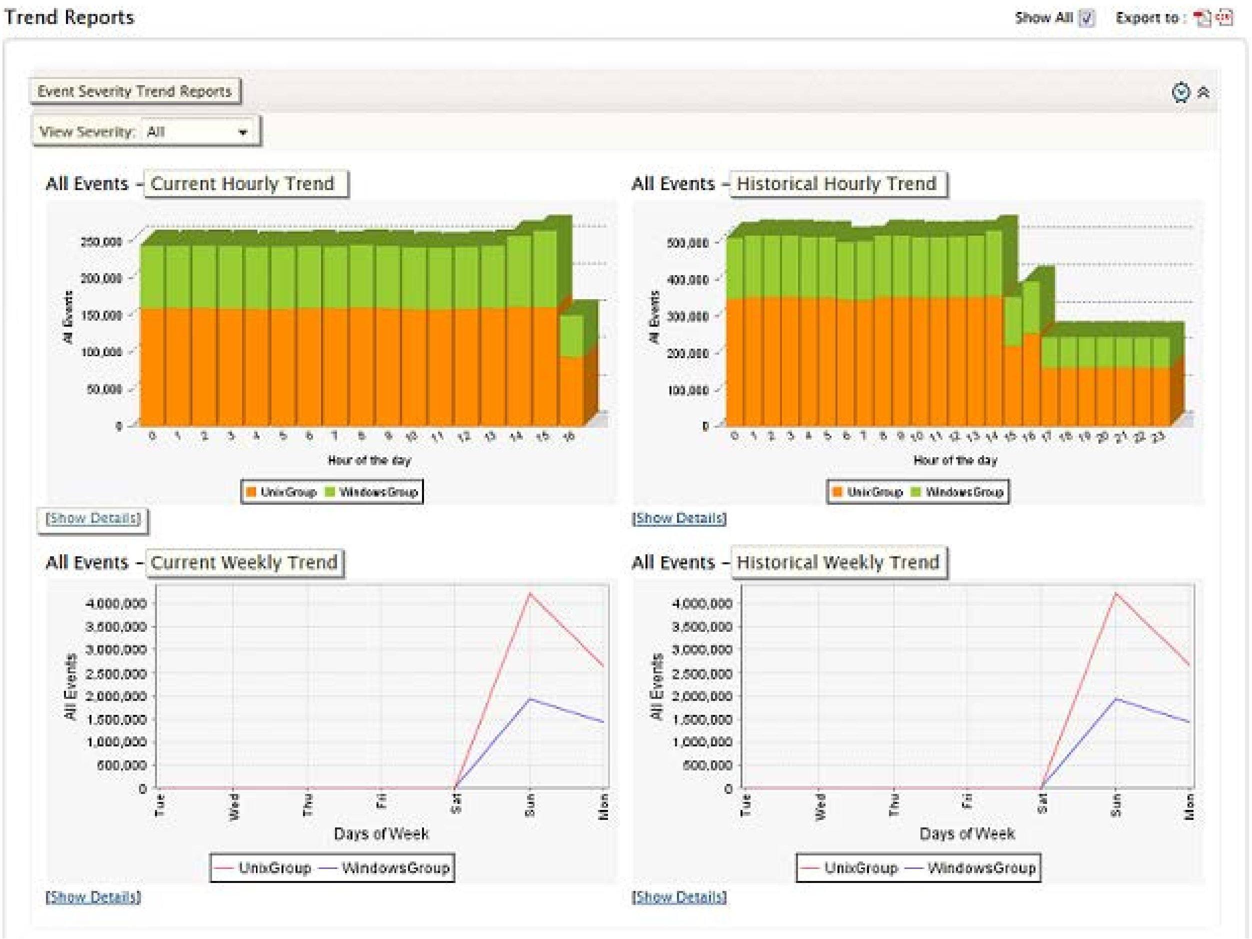
You can monitor trends of events generated across hosts, based on event severity, or event type. You can monitor trends of alerts triggered. All the trend reports in EventLog Analyzer show the current trend, and compare this with the historical trend. The trend reports available are, hourly (with the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

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

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

Event Severity Trend Reports

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



Trend Reports

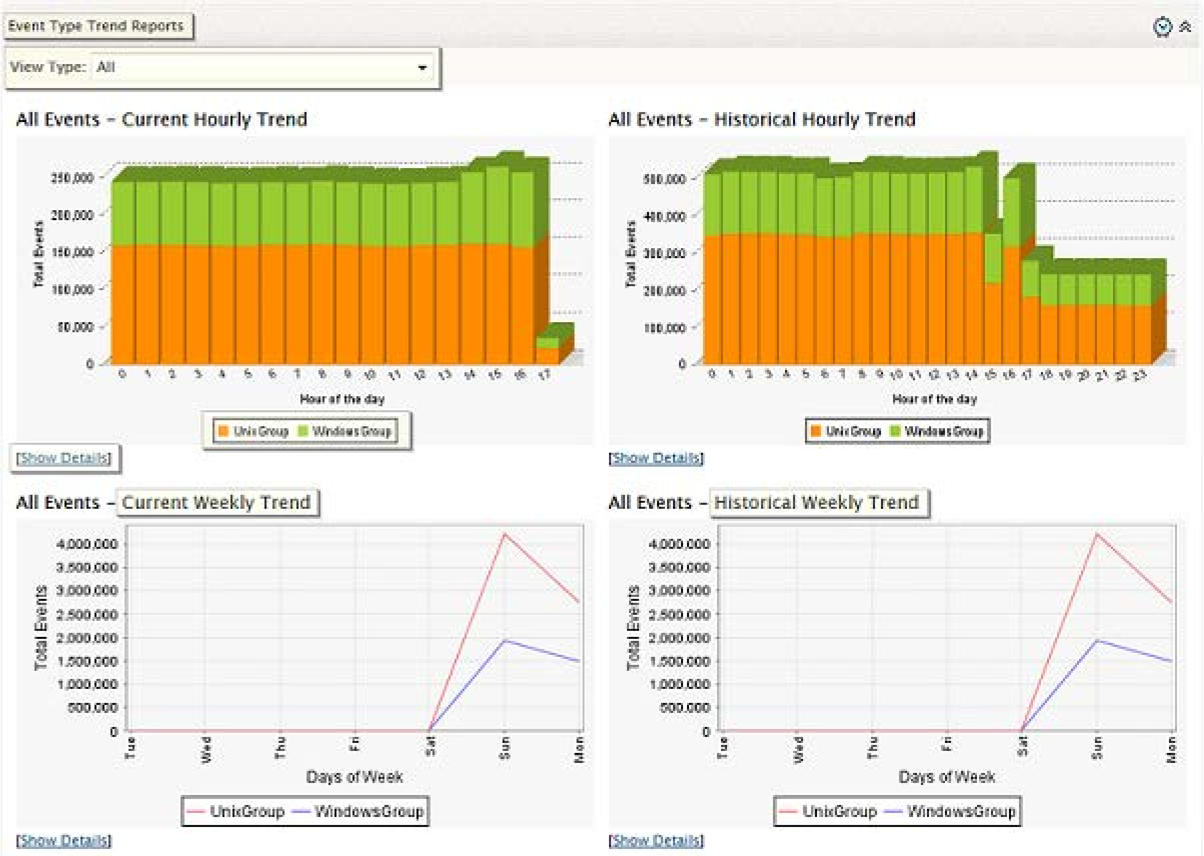
Show All ☑ Export to :

Event Severity Trend Reports

View Severity: All

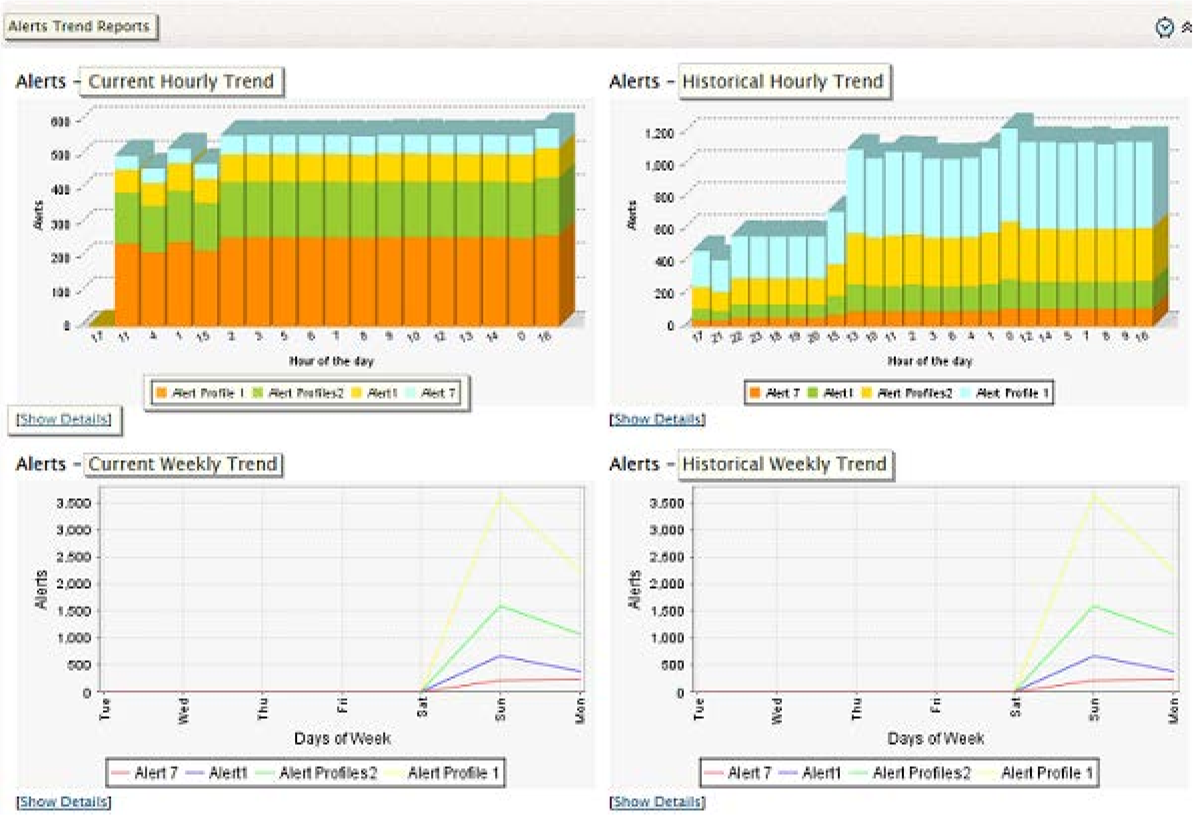
Event Type / Category Trend Reports

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



Alerts Trend Reports

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



Ask ME Reports

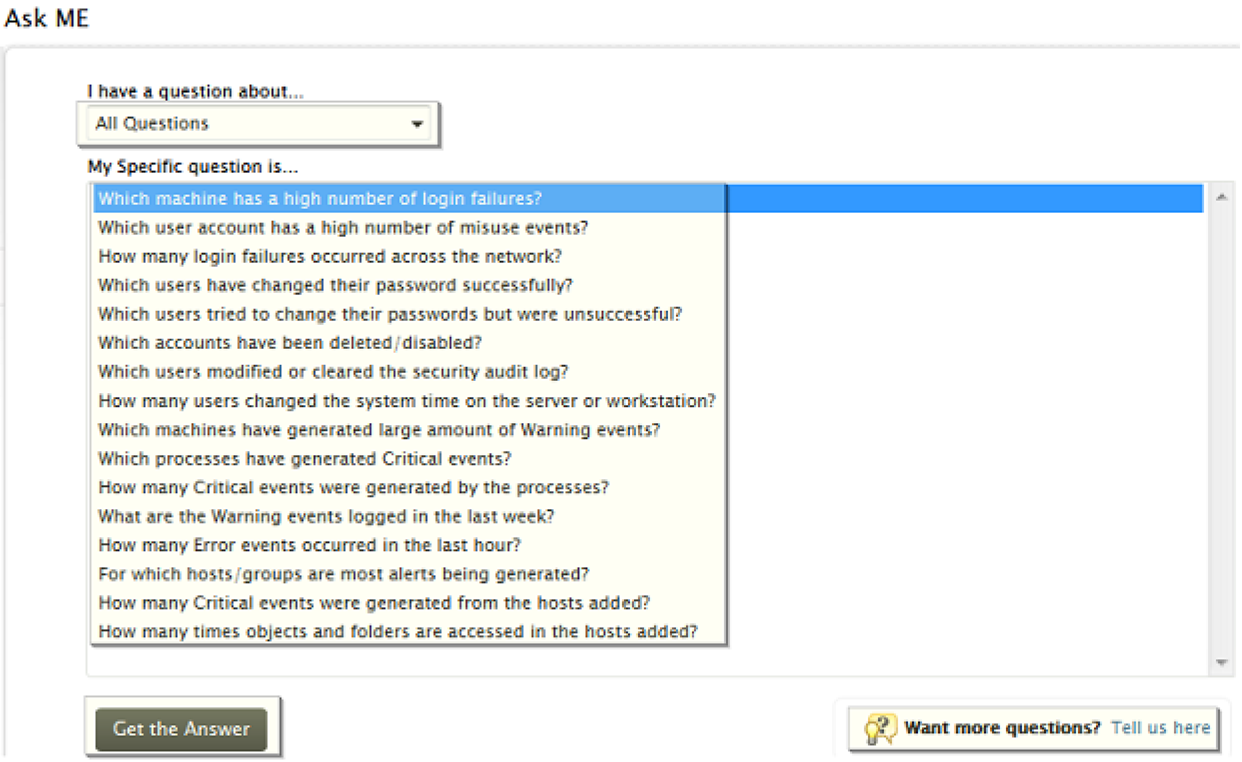
Ask ME enables managers and other non-technical staff to answer simple but critical questions about important network events that are of greater importance. The The **Ask ME** section in the **Reports** tab offers a quick way to see just the reports that you need, without having to create a new report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

To view Ask ME reports use the following menu option:

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

Ask ME section shows a series of questions.

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



Ask ME

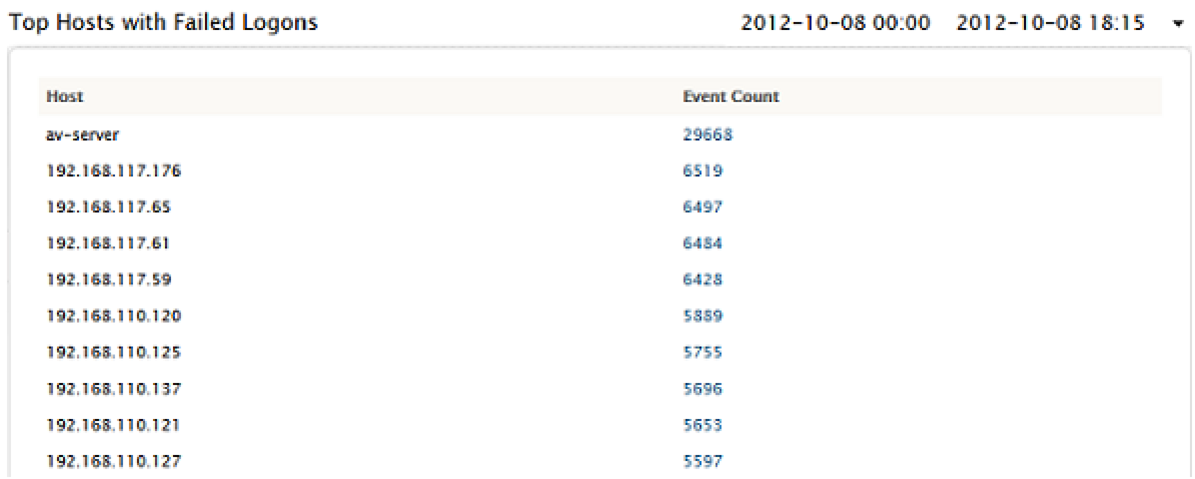
I have a question about...

All Questions

My Specific question is...

Which machine has a high number of login failures?
Which user account has a high number of misuse events?
How many login failures occurred across the network?
Which users have changed their password successfully?
Which users tried to change their passwords but were unsuccessful?
Which accounts have been deleted/disabled?
Which users modified or cleared the security audit log?
How many users changed the system time on the server or workstation?
Which machines have generated large amount of Warning events?
Which processes have generated Critical events?
How many Critical events were generated by the processes?
What are the Warning events logged in the last week?
How many Error events occurred in the last hour?
For which hosts/groups are most alerts being generated?
How many Critical events were generated from the hosts added?
How many times objects and folders are accessed in the hosts added?

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.
The report corresponding to the question selected is now generated and displayed.



Top Hosts with Failed Logons 2012-10-08 00:00 2012-10-08 18:15

Host	Event Count
av-server	29668
192.168.117.176	6519
192.168.117.65	6497
192.168.117.61	6484
192.168.117.59	6428
192.168.110.120	5889
192.168.110.125	5755
192.168.110.137	5696
192.168.110.121	5653
192.168.110.127	5597

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

Adding Custom Questions in Ask ME

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

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

   Example entry for "Question" and "link" tags are given below:
   <Question>How many times objects and folders are accessed in the hosts added?</Question>
   <link>index2.do?url=topreport_details&amp;RBBNAME=Compliance_ObjectAccess&amp;tab=askCherry&amp;rtype=toprep&amp;TC=10</link>

4. Save the file

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

Note: Ensure that you add the new questions after the existing questions. Do not disturb the existing 17 questions.

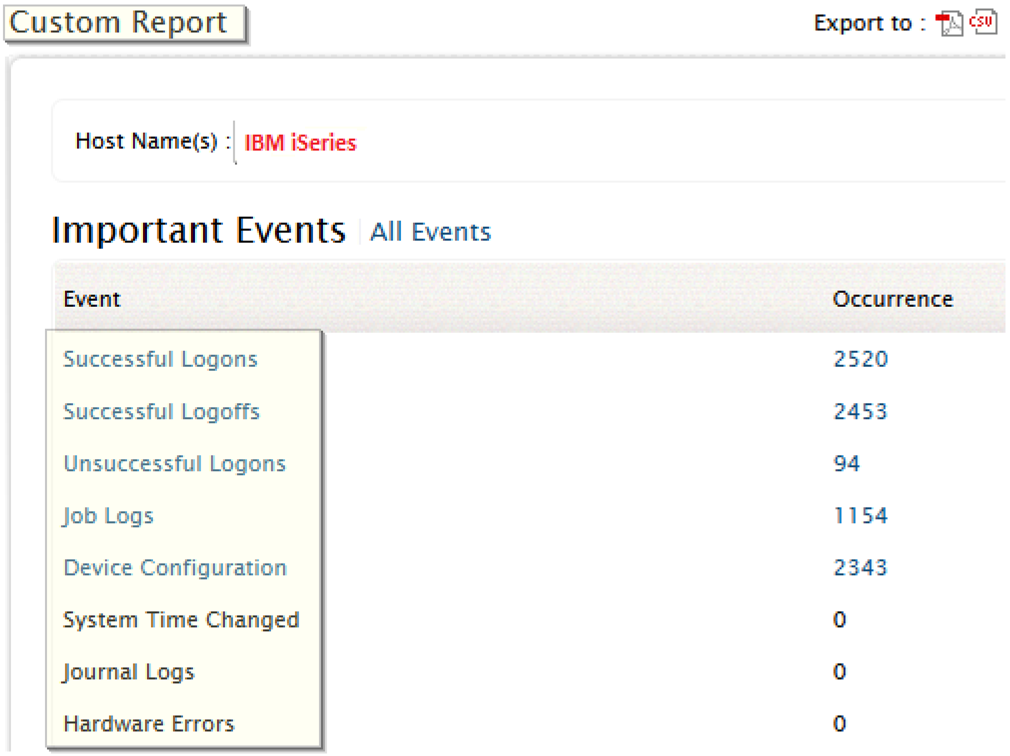
IBM iSeries (AS/400) Reports

The history logs of IBM AS/400 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.
To view IBM iSeries (AS/400) reports use the following menu option:

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

AS/400 System History Log Reports

EventLog Analyzer will generate a variety of special reports using the information extracted from the history logs of AS/400 systems.



Custom Report

Export to :

Host Name(s) : IBM iSeries

Important Events | All Events

Event	Occurrence
Successful Logons	2520
Successful Logoffs	2453
Unsuccessful Logons	94
Job Logs	1154
Device Configuration	2343
System Time Changed	0
Journal Logs	0
Hardware Errors	0

Special Reports generated by the application are:

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

Compliance Reports

The regulatory compliance reports are mandated by industry bodies/ government authorities to assure minimum security to the IT users in various industries. Non-compliance to the regulatory acts attracts penal action. To ensure credible security and address the mandatory requirement compliance reports of IT networks are required. EventLog Analyzer generates the major compliance reports required for the IT industry. The major pre-built reports available in EventLog Analyzer are PCI-DSS, HIPAA, FISMA, SOX, and GLBA. This software keeps the future compliance in mind and offers custom compliance reports. ISO-27001 and NIST-1075 are some of the regulatory compliance acts for which the reports can be generated. Even the existing compliance can be modified to suit the individual internal needs of the company.

Payment Card Industry – Data Security Standards (PCI-DSS) Compliance Reports

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

PCI-DSS requirements 10.1 & 10.2.2 - User Access

- Individual User Action

PCI-DSS requirements 10.2.1 & 10.2.3 - Logon

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

PCI-DSS requirements 10.2.3 - Policy Changes

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

PCI-DSS requirements 10.2.6 - System Events

- System Logs
- Audit Logs Cleared

PCI-DSS requirements 10.2.7 - Object Access

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

Health Insurance Portability and Accountability Act (HIPAA) Compliance Reports

EventLog Analyzer helps you to meet the most challenging HIPAA Security Standards to monitor and audit system activity of a health organization. EventLog Analyzer can easily monitor both perimeter devices, such as IDSs, as well as insider activity. HIPAA regulations mandate analysis of all logs, including OS and application logs.

164.308(a)(1)(ii)(D) - Object Access

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

164.308(a)(3)(ii)(A) & (a)(4)(ii)(B) - Account Logon

- Successful User Account Validation
- Unsuccessful User Account Validation

164.308(a)(5)(ii)(C) & (a)(6)(ii) - Logon

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

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

- System Logs
- Audit Logs Cleared

Federal Information Security Management Act (FISMA) Compliance Reports

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

Audit and Accountability (AU) - Object Access

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

Access Control (AC) - Logon

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

Certification, Accreditation, and Security Assessments (CA) - Security Assessment

- Windows Services

Contingency Planning (CP) - Contingency Planning

- Windows Backup
- Windows Restore

Identification and Authentication (IA) - User Access

- Individual User Action

Configuration Management (CM) - Configuration Management

- Windows Software Updates
- Anti-malwares
- Other Software

Sarbanes-Oxley Act (SOX) Compliance Reports

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

SEC 302 (a)(4)(A) - System Events

- System Logs
- Audit Logs Cleared

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

- Process Access

SEC 302 (a)(4)(B) - Policy Changes

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

SEC 302 (a)(4)(C) - Logon

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

SEC 302 (a)(4)(D) - Account Logon

- Successful User Account Validation
- Unsuccessful User Account Validation

SEC 302 (a)(5)(A) - Object Access

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

SEC 302 (a)(5)(B) - User Access

- Individual User Action

SEC 302 (a)(6) - Account Management

- User Account Changes
- Computer Account Changes
- User Group Changes

Gramm-Leach-Bliley Act (GLBA) Compliance Reports

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

Section 501B (1) - System Events

- System Logs
- Audit Logs Cleared

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

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

Search Logs

In EventLog Analyzer, you can search for any term in the log message.
This section discusses about how to search logs in EventLog Analyzer.

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

Go to Search

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

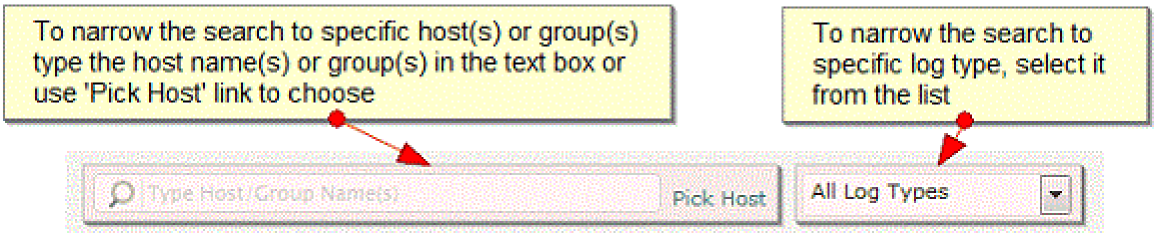
Using the Search Result

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

How to Search

EventLog Analyzer provided a dedicated section for '**Search**' (Click the '**Search**' tab in the GUI), where you can search the raw logs and detect network anomalies like mis-configurations, viruses, unauthorized access, applications errors, etc.

The procedure to search th logs is given below:



To narrow the search to specific host(s) or group(s) type the host name(s) or group(s) in the text box or use 'Pick Host' link to choose

To narrow the search to specific log type, select it from the list

Searching a specific Host(s), Host Group(s) or Log Type(s)

To narrow down the search to a specific host(s) or group of hosts, type in the host name(s) or group(s) name in the text box provided or else use the '**Pick Host**' link to select the host(s) or host group(s). You can also narrow down the search to the type of log (example: Windows Event Log, Syslog, Oracle Logs), by selecting it from the **Log Types** list.

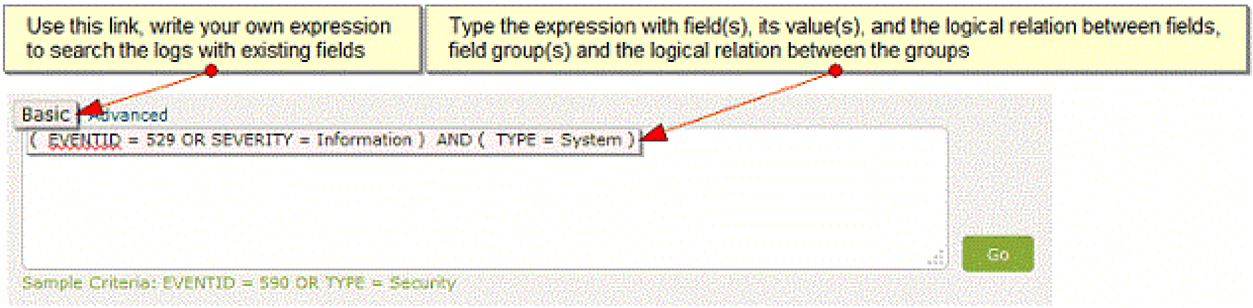
By default (if the host name(s) or group(s) name are not provided, and '**All Log Types**' option remains unchanged), you can search across all hosts and all log types.

Types of Search

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

Basic Search

If you want to write your own expression (search criteria) and search the logs for existing field value(s), use the '**Basic**' search link. In this option, you have to type in the search criteria.



Use this link, write your own expression to search the logs with existing fields

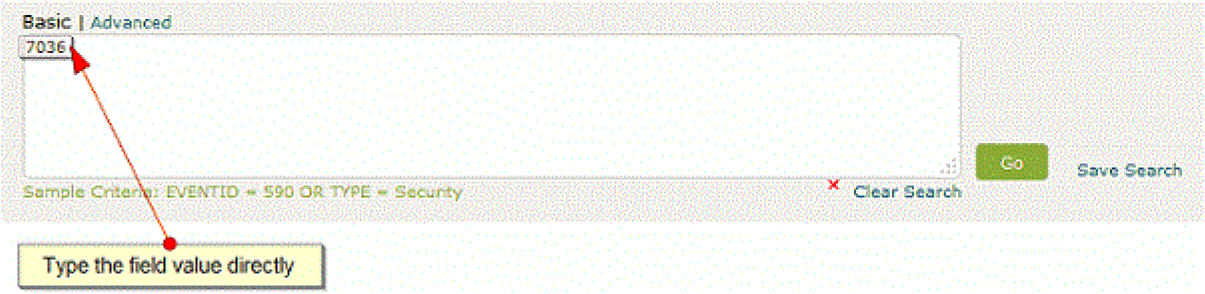
Type the expression with field(s), its value(s), and the logical relation between fields, field group(s) and the logical relation between the groups

(EVENTID = 529 OR SEVERITY = Information) AND (TYPE = System)

Sample Criteria: EVENTID = 590 OR TYPE = Security

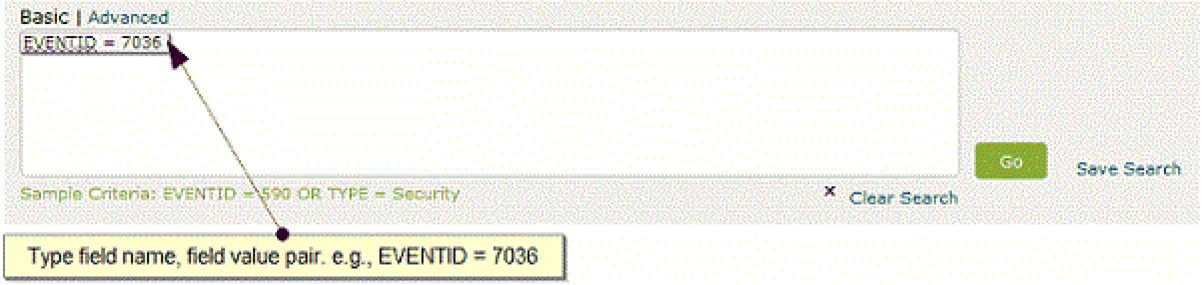
Search for field values

Type the field value directly in to the Search box.


Basic | Advanced
7036
Go
Save Search
Sample Criteria: EVENTID = 590 OR TYPE = Security
Clear Search
Type the field value directly

Search with fields

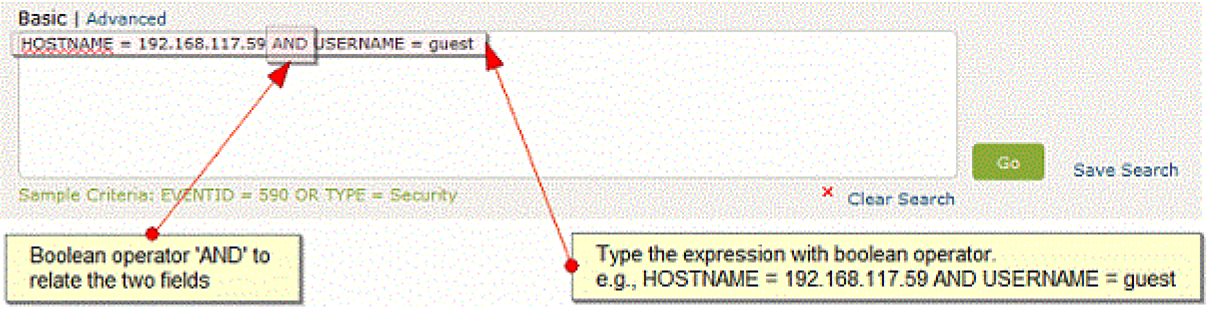
Type the field name and value directly in to the Search box. The expression for field name and value pair is **<field name> = <field value>**
Example: **EVENTID = 7036**


Basic | Advanced
EVENTID = 7036
Go
Save Search
Sample Criteria: EVENTID = 590 OR TYPE = Security
Clear Search
Type field name, field value pair. e.g., EVENTID = 7036

Use boolean operators to search

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

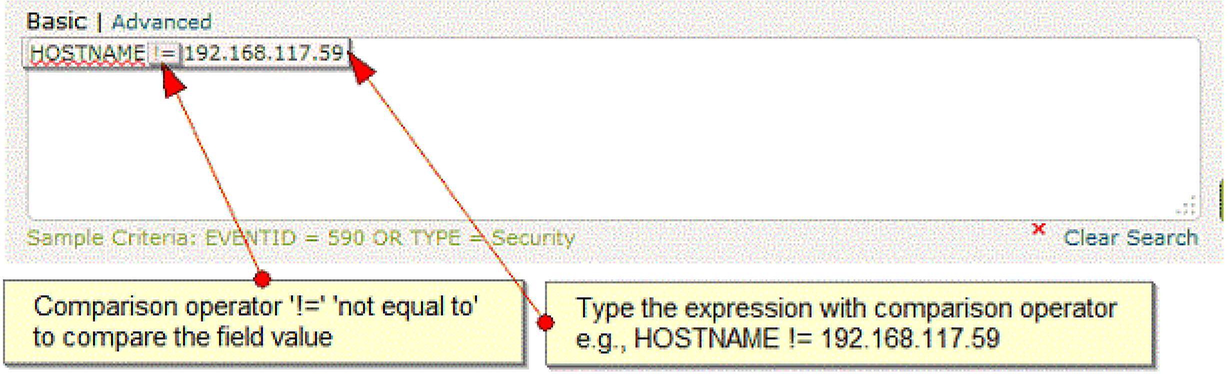
Example: **HOSTNAME = 192.168.117.59 AND USERNAME = guest**


Basic | Advanced
HOSTNAME = 192.168.117.59 AND USERNAME = guest
Go
Save Search
Sample Criteria: EVENTID = 590 OR TYPE = Security
Clear Search
Boolean operator 'AND' to relate the two fields
Type the expression with boolean operator.
e.g., HOSTNAME = 192.168.117.59 AND USERNAME = guest

Use comparison operators to search

The expression with comparison operator is **<field name> <comparison operator> <field value>**. You can use the following comparison operators: **=, !=, >, <, >=, <=**.

Example: **HOSTNAME != 192.168.117.59**



Basic | Advanced
HOSTNAME != 192.168.117.59
Sample Criteria: EVENTID = 590 OR TYPE = Security
Clear Search

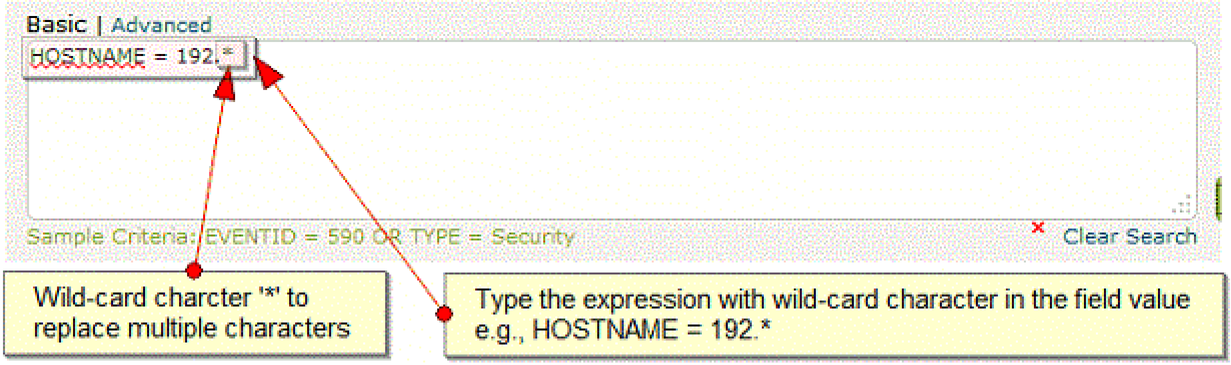
Comparison operator '!=' 'not equal to' to compare the field value

Type the expression with comparison operator e.g., HOSTNAME != 192.168.117.59

Use wild-card characters to search

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

Example: **HOSTNAME = 192.***



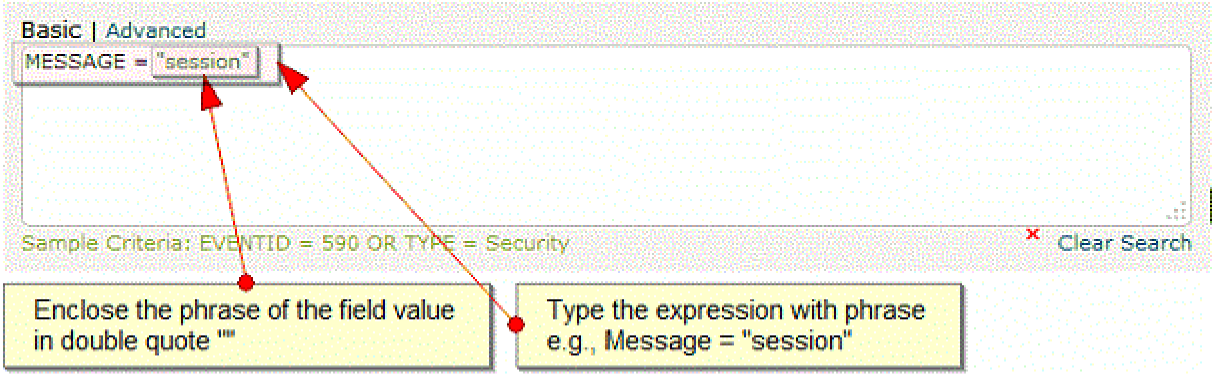
Wild-card charcter '*' to replace multiple characters

Type the expression with wild-card character in the field value e.g., HOSTNAME = 192.*

Use phrase to search

The expression with phrase is **<field name> = <"partial field value">**. Use double quotes (**""**) to define phrase in the field value.

Example: **MESSAGE = "session"**



MESSAGE = "session"

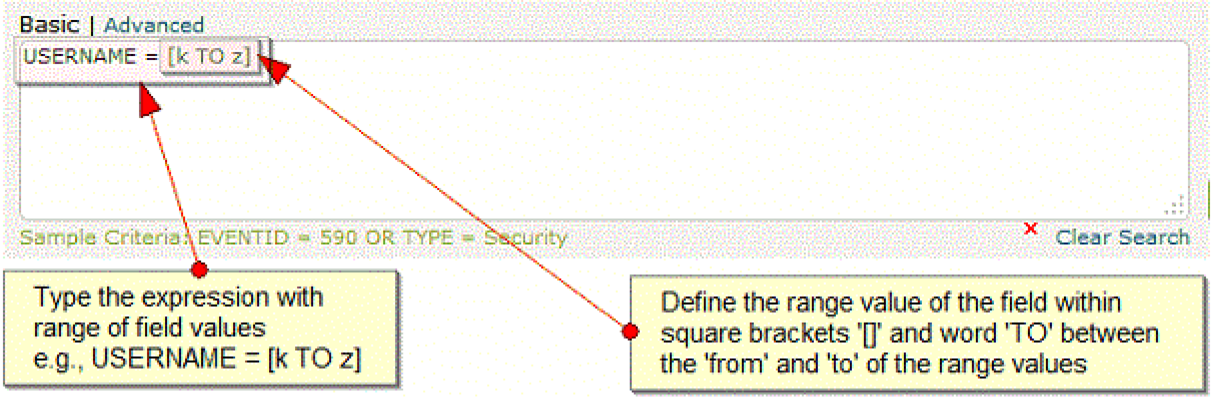
Enclose the phrase of the field value in double quote ""

Type the expression with phrase e.g., Message = "session"

Use range to search

The expression to search for a range of values is **<field name> = field values [<from> TO <to>]**. Use square brackets '**[]**' to define **'from' TO 'to'** range of field values.

Example: **USERNAME = [k To z]**



USERNAME = [k TO z]

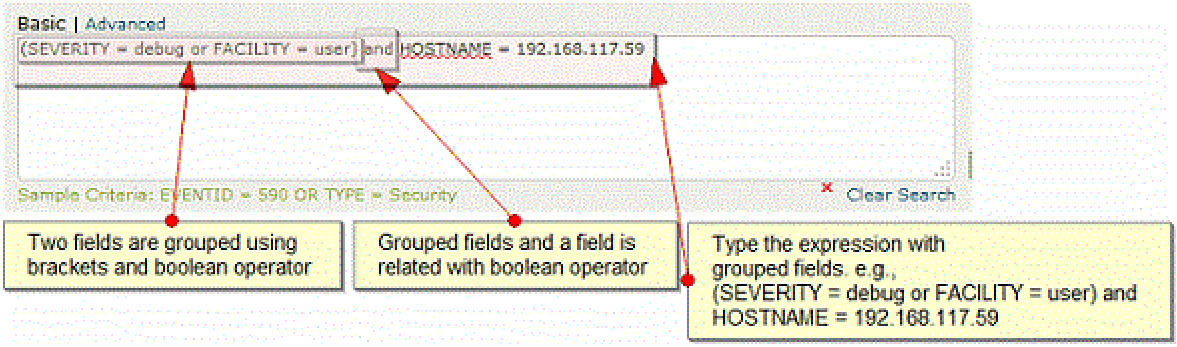
Type the expression with range of field values e.g., USERNAME = [k TO z]

Define the range value of the field within square brackets '[]' and word 'TO' between the 'from' and 'to' of the range values

Use grouped fields to search

The expression to search with grouped fields is **(<field name> = <field value> <logical operator>.<field name> = <field value>) <logical operator>.<field name> = <field value>**. Relate the field value pairs logically and group them using brackets '**()**' and relate the grouped fields logically.

Example: **(SEVERITY = debug or information) and HOSTNAME = 192.168.117.59**



(SEVERITY = debug or FACILITY = user) and HOSTNAME = 192.168.117.59

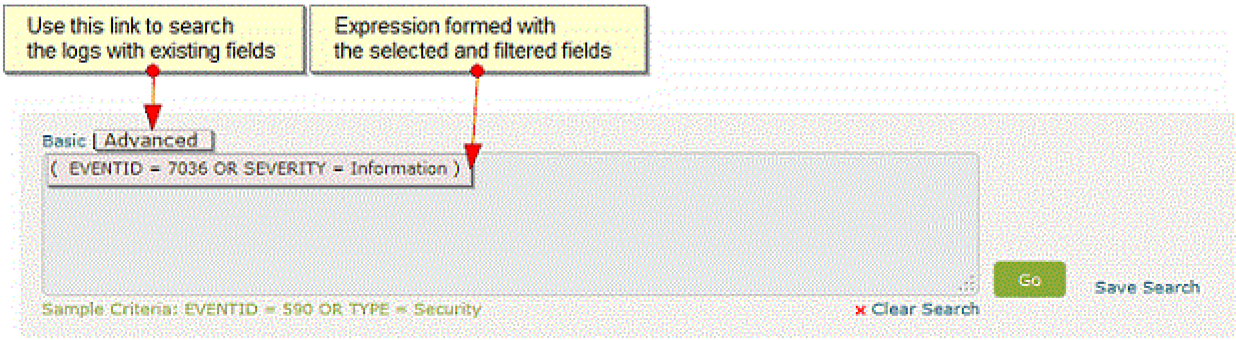
Two fields are grouped using brackets and boolean operator

Grouped fields and a field is related with boolean operator

Type the expression with grouped fields. e.g., (SEVERITY = debug or FACILITY = user) and HOSTNAME = 192.168.117.59

Advanced Search

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



Use this link to search the logs with existing fields

Expression formed with the selected and filtered fields

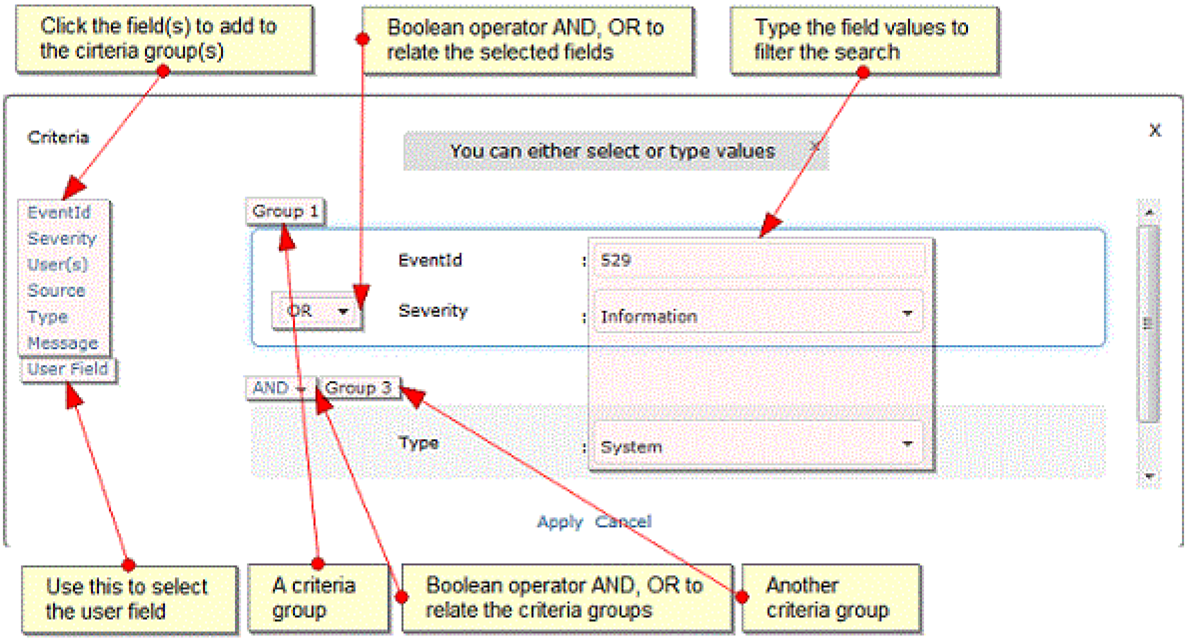
Basic | Advanced

(EVENTID = 7036 OR SEVERITY = Information)

Sample Criteria: EVENTID = 590 OR TYPE = Security

Set criteria to search

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



Click the field(s) to add to the cirteria group(s)

Boolean operator AND, OR to relate the selected fields

Type the field values to filter the search

Criteria

You can either select or type values

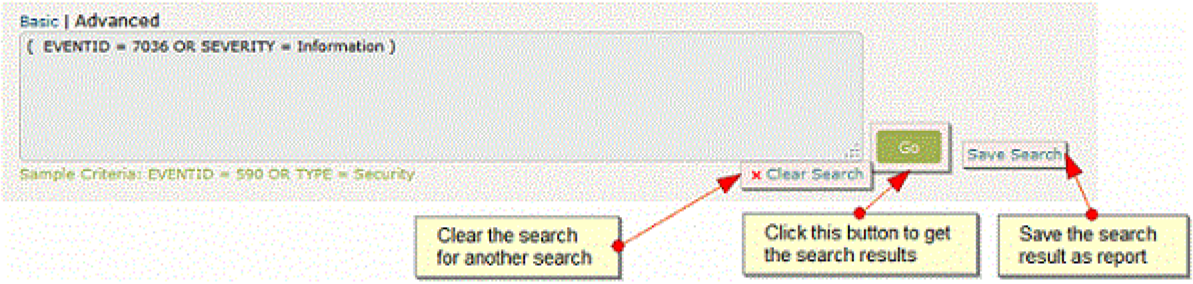
Use this to select the user field

A criteria group

Boolean operator AND, OR to relate the criteria groups

Another criteria group

If you have defined the criteria, click '**Apply**' button. The search criteria expression appears in the text box. Click '**Go**' button to preview the search results. It is displayed in a graph and the entries are listed below.



Basic | Advanced

(EVENTID = 7036 OR SEVERITY = Information)

Sample Criteria: EVENTID = 590 OR TYPE = Security

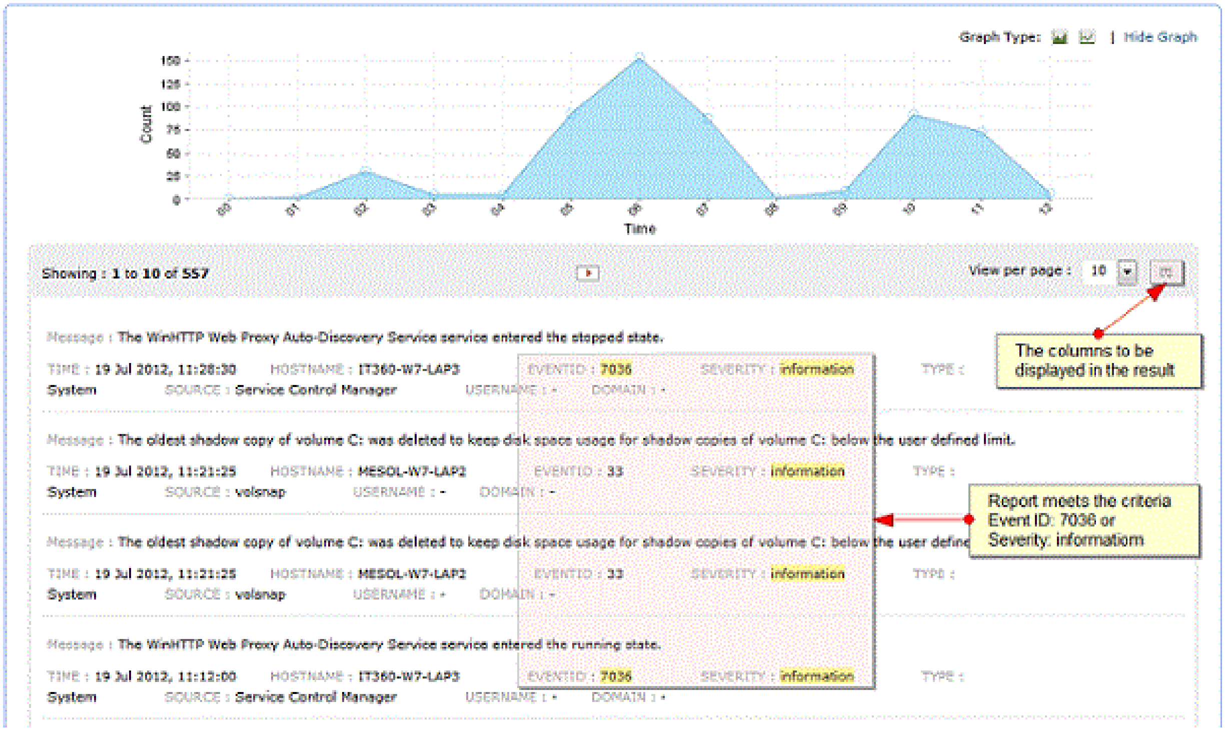
Go
Save Search
× Clear Search
Clear the search for another search
Click this button to get the search results
Save the search result as report

Clear the search

'**Clear Search**' clears the search query.

Save the search

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



Graph Type:
| Hide Graph
Count
150
125
100
75
50
25
0
00
01
02
03
04
05
06
07
08
09
10
11
12
Time
The columns to be displayed in the result
Report meets the criteria Event ID: 7036 or Severity: informatiom

Showing : 1 to 10 of 557

View per page : 10

Message : The WinHTTP Web Proxy Auto-Discovery Service service entered the stopped state.
TIME : 19 Jul 2012, 11:28:30 HOSTNAME : IT360-W7-LAP3 EVENTID : 7036 SEVERITY : information TYPE :
System SOURCE : Service Control Manager USERNAME : - DOMAIN : -

Message : The oldest shadow copy of volume C: was deleted to keep disk space usage for shadow copies of volume C: below the user defined limit.
TIME : 19 Jul 2012, 11:21:25 HOSTNAME : MESOL-W7-LAP2 EVENTID : 33 SEVERITY : information TYPE :
System SOURCE : volsnap USERNAME : - DOMAIN : -

Message : The oldest shadow copy of volume C: was deleted to keep disk space usage for shadow copies of volume C: below the user define
TIME : 19 Jul 2012, 11:21:25 HOSTNAME : MESOL-W7-LAP2 EVENTID : 33 SEVERITY : information TYPE :
System SOURCE : volsnap USERNAME : - DOMAIN : -

Message : The WinHTTP Web Proxy Auto-Discovery Service service entered the running state.
TIME : 19 Jul 2012, 11:12:00 HOSTNAME : IT360-W7-LAP3 EVENTID : 7036 SEVERITY : information TYPE :
System SOURCE : Service Control Manager USERNAME : - DOMAIN : -

Extract New Fields to Parse and Index Logs

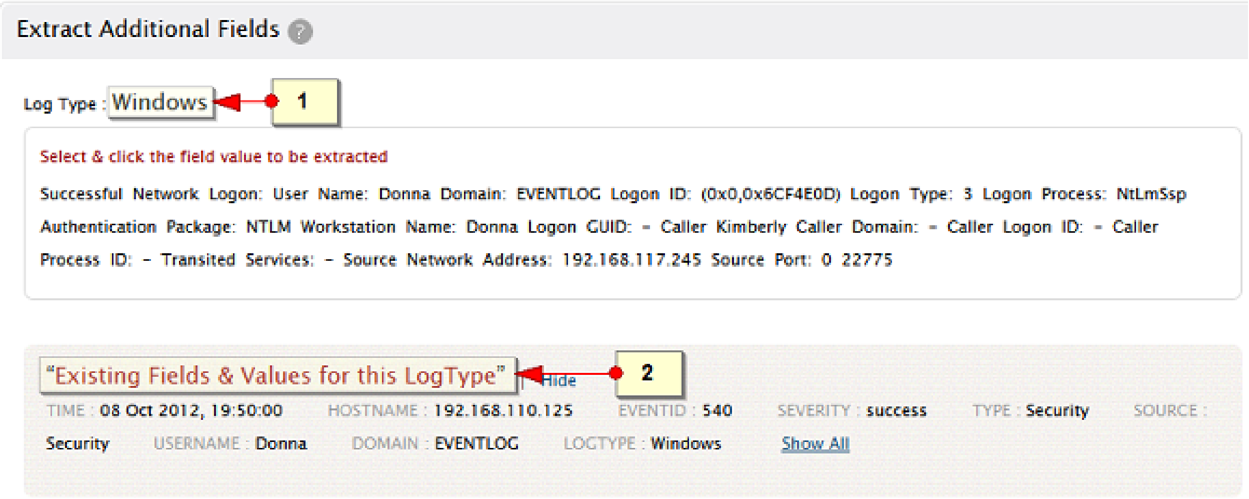
Network Administrators are always in need of more information and insights from their log data. There are times when an IT administrator would identify some log information which is useful and would like to have it indexed automatically as a new field. Having more fields being indexed makes your log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

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

Procedure to extract new fields

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

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



Extract Additional Fields

Log Type : Windows

Select & click the field value to be extracted

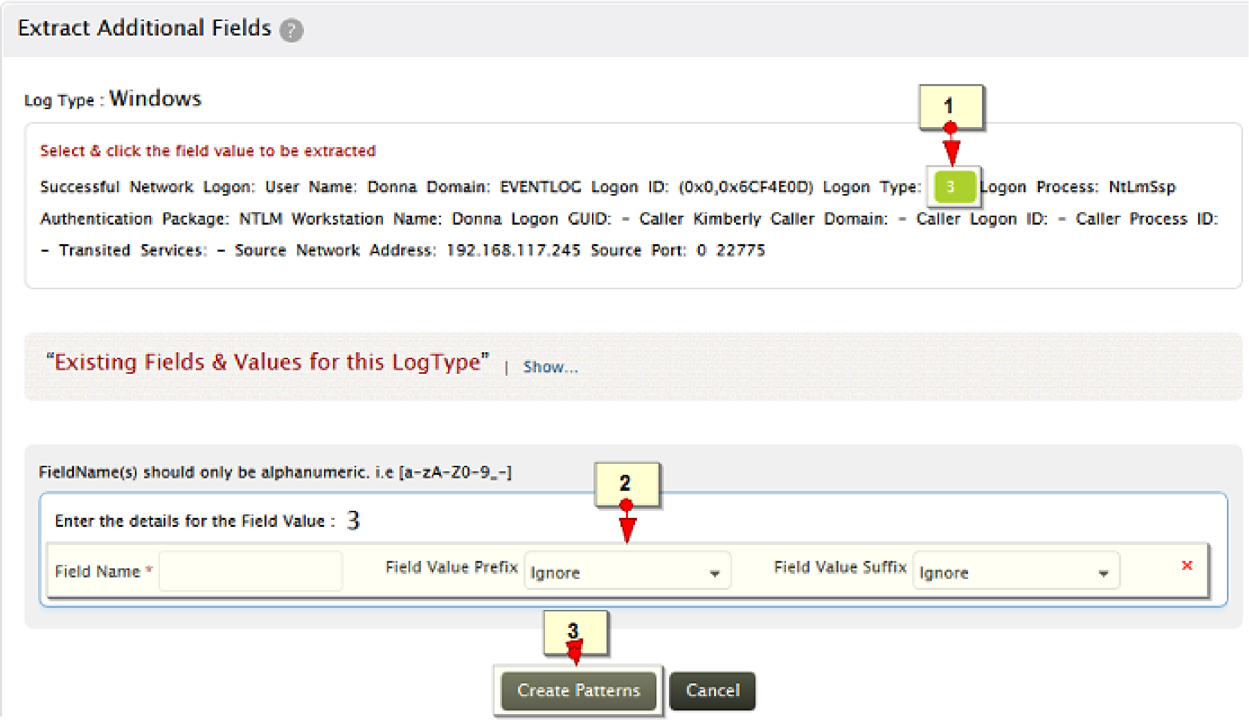
Successful Network Logon: User Name: Donna Domain: EVENTLOG Logon ID: (0x0,0x6CF4E0D) Logon Type: 3 Logon Process: NtLmSsp Authentication Package: NTLM Workstation Name: Donna Logon GUID: - Caller Kimberly Caller Domain: - Caller Logon ID: - Caller Process ID: - Transited Services: - Source Network Address: 192.168.117.245 Source Port: 0 22775

"Existing Fields & Values for this LogType"

TIME : 08 Oct 2012, 19:50:00 HOSTNAME : 192.168.110.125 EVENTID : 540 SEVERITY : success TYPE : Security SOURCE : Security USERNAME : Donna DOMAIN : EVENTLOG LOGTYPE : Windows

1. Edit the **Log Type** display name, if it is not default log type. For non-default log types, the display name will be name of the imported log file or hostname/port
2. View the details of the '**Existing Fields**' with the help of **Show** and **Show All** links.

Step 2: Select the required custom field value(s) and specify the details



Extract Additional Fields

Log Type : Windows

Select & click the field value to be extracted

Successful Network Logon: User Name: Donna Domain: EVENTLOG Logon ID: (0x0,0x6CF4E0D) Logon Type: 3 Logon Process: NtLmSsp Authentication Package: NTLM Workstation Name: Donna Logon GUID: - Caller Kimberly Caller Domain: - Caller Logon ID: - Caller Process ID: - Transited Services: - Source Network Address: 192.168.117.245 Source Port: 0 22775

"Existing Fields & Values for this LogType" | Show...

FieldName(s) should only be alphanumeric. i.e [a-zA-Z0-9_-]

Enter the details for the Field Value : 3

Field Name * | Field Value Prefix: Ignore | Field Value Suffix: Ignore

1. Select and click the word(s) in the message, to be extracted as field
2. Provide a name for this field. Optinally, specify the prefix and suffix to the field value
3. Click on **Create Pattern** to generate a parser rule pattern

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

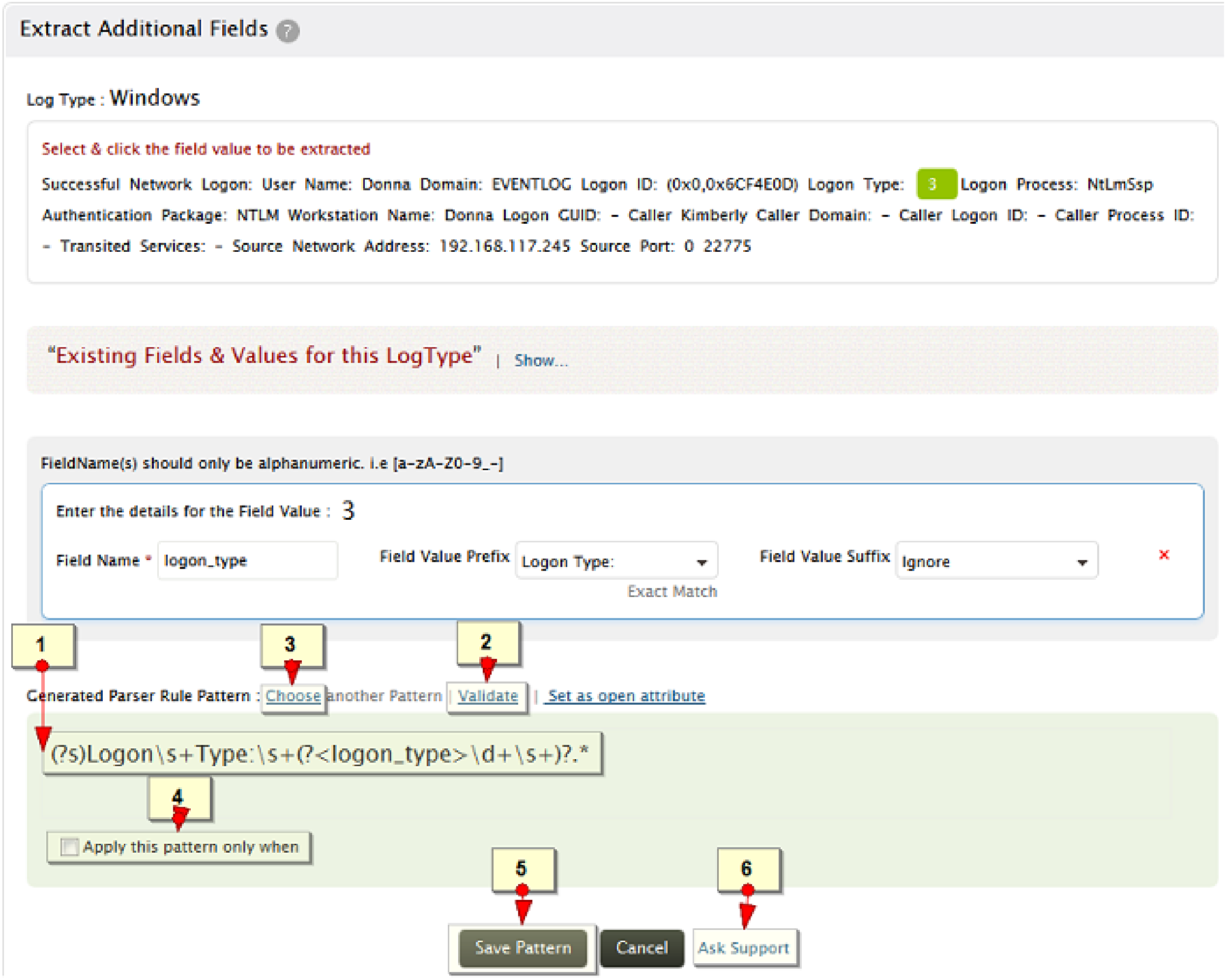
Example for Static and Dynamic value for Prefix and Suffix

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

The prefix **Logon Type** can be a **static** value as most of the logs will have the exact word as '**Logon Type**' where as '**Source Network Address**' can be **dynamic** as the logs may have different word(s) like, Source IP Address, Source Address, but with same pattern.

If the prefix and suffix are defined with exact match, the field extraction will be precise.

Step 3: Validate the pattern and save it to extract the new field



Extract Additional Fields

Log Type : Windows

Select & click the field value to be extracted

Successful Network Logon: User Name: Donna Domain: EVENTLOG Logon ID: (0x0,0x6CF4E0D) Logon Type: 3 Logon Process: NtLmSsp Authentication Package: NTLM Workstation Name: Donna Logon GUID: - Caller Kimberly Caller Domain: - Caller Logon ID: - Caller Process ID: - Transited Services: - Source Network Address: 192.168.117.245 Source Port: 0 22775

"Existing Fields & Values for this LogType" | Show...

FieldName(s) should only be alphanumeric. i.e [a-zA-Z0-9_-]

Enter the details for the Field Value : 3

Field Name * logon_type Field Value Prefix Logon Type: Exact Match Field Value Suffix Ignore

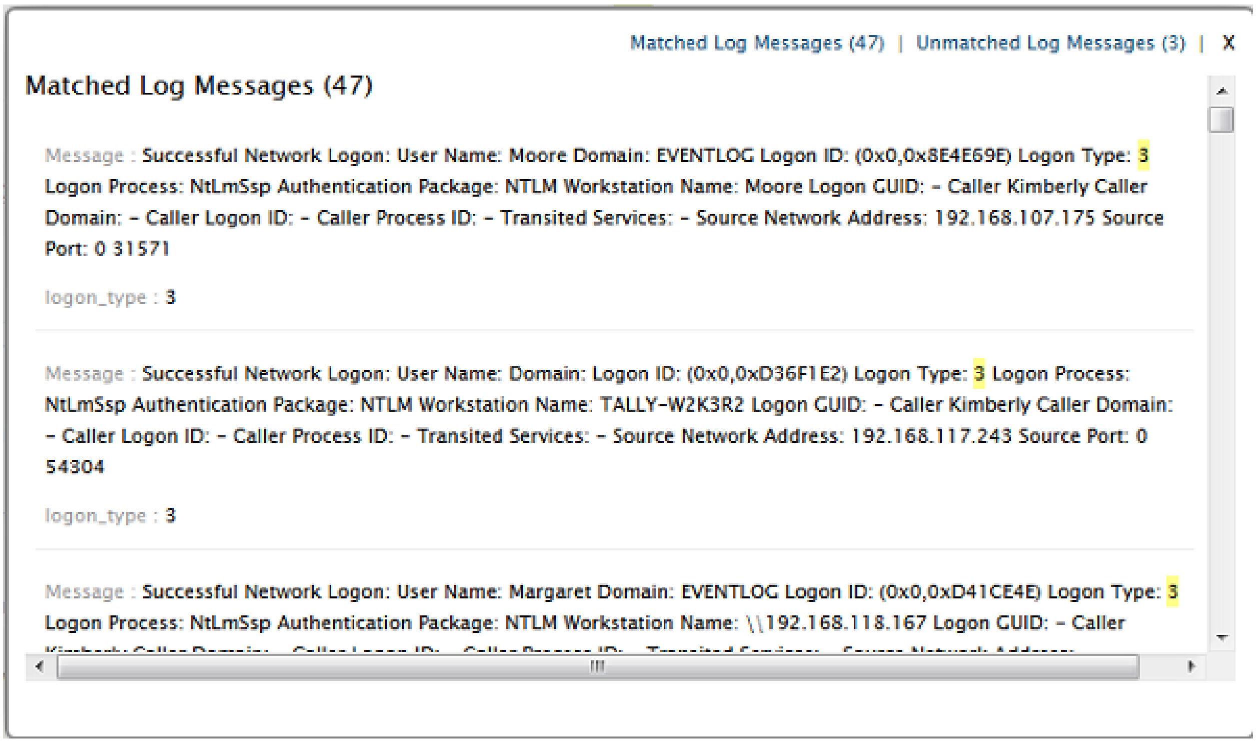
Generated Parser Rule Pattern : Choose another Pattern | Validate | Set as open attribute

```
(?s)Logon\s+Type:\s+(?<logon_type>\d+\s+)?.*
```

□ Apply this pattern only when

1. A parser rule pattern is created using the field definition. You can edit the generated pattern manually, if you are familiar with regular expression
2. **Validate** link is used to test the generated pattern against the previous search results. You can manually check the suitability of the pattern by analyzing the 'Matched Log Messages' and 'Unmatched Log Messages' displayed.
3. Optionally, click on **Choose another Pattern** to choose a pattern from a list of patterns generated by the application
4. Optionally, you can define any existing field matching criteria to apply the pattern for this specific log type
5. Save the pattern to extract the field(s) from the upcoming logs. The saved pattern will be listed in the **Settings** tab under **Custom Pattern Settings** section
6. Use the **Ask Support** button, if you face any problem and get assistance from the EventLog Analyzer team

Screenshot of Validate check



Matched Log Messages (47)

Message : Successful Network Logon: User Name: Moore Domain: EVENTLOG Logon ID: (0x0,0x8E4E69E) Logon Type: 3 Logon Process: NtLmSsp Authentication Package: NTLM Workstation Name: Moore Logon GUID: - Caller Kimberly Caller Domain: - Caller Logon ID: - Caller Process ID: - Transited Services: - Source Network Address: 192.168.107.175 Source Port: 0 31571

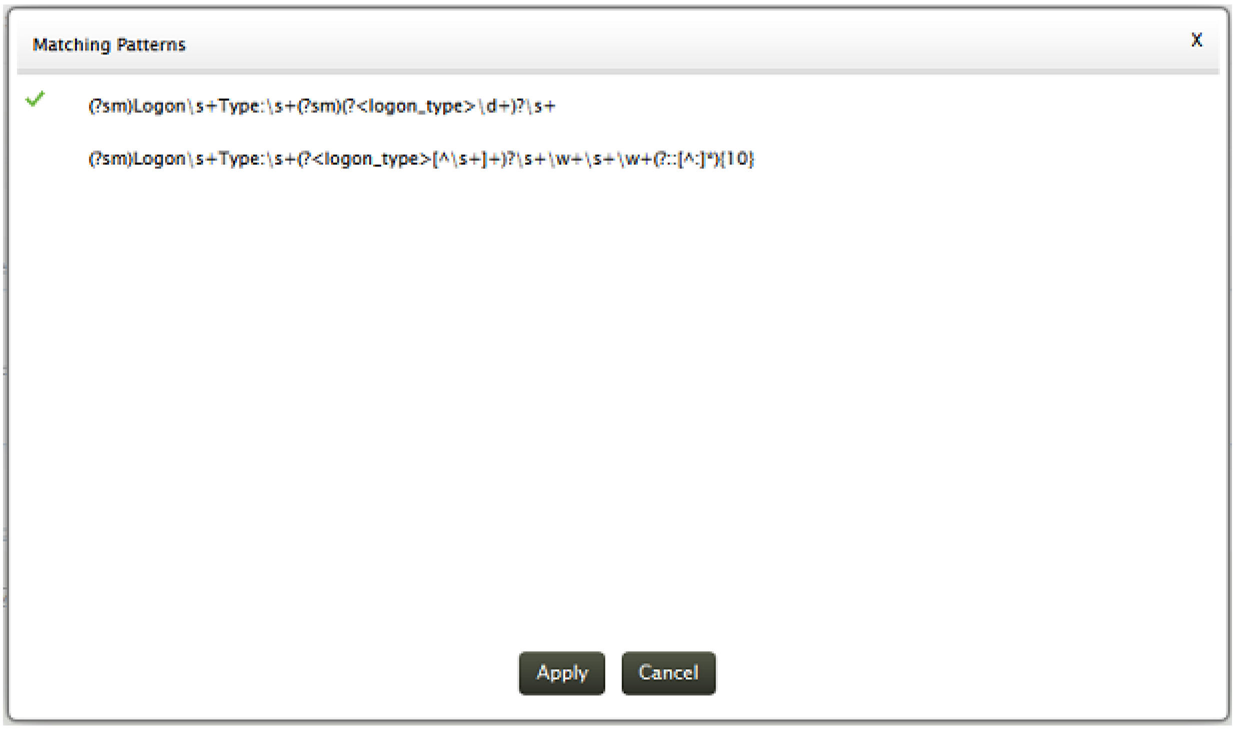
logon_type : 3

Message : Successful Network Logon: User Name: Domain: Logon ID: (0x0,0xD36F1E2) Logon Type: 3 Logon Process: NtLmSsp Authentication Package: NTLM Workstation Name: TALLY-W2K3R2 Logon GUID: - Caller Kimberly Caller Domain: - Caller Logon ID: - Caller Process ID: - Transited Services: - Source Network Address: 192.168.117.243 Source Port: 0 54304

logon_type : 3

Message : Successful Network Logon: User Name: Margaret Domain: EVENTLOG Logon ID: (0x0,0xD41CE4E) Logon Type: 3 Logon Process: NtLmSsp Authentication Package: NTLM Workstation Name: \\192.168.118.167 Logon GUID: - Caller Kimberly Caller Domain: - Caller Logon ID: - Caller Process ID: - Transited Services: - Source Network Address:

Screenshot of patterns generated by the application



```
✓ (?sm)Logon\s+Type:\s+(?sm)(?<logon_type>\d+)?\s+

(?sm)Logon\s+Type:\s+(?<logon_type>[^\s+]+)?\s+\w+\s+\w+(?::[^:]*){10}
```

Event Alerts

Log Alerts

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

View Log Alerts

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

Viewing Alerts for an Alert Profile

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

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

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

Configuration

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

- Managed Server Settings
- Manage Hosts - Manage Host Groups
- Import
- Archive - Centralized Archive
- Report Profiles - Schedule Reports
- Alerts
- Database Filter
- Dashboard Profiles - Add | Edit / Del | All Profiles
- Ask ME - Quick Answers

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** or **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

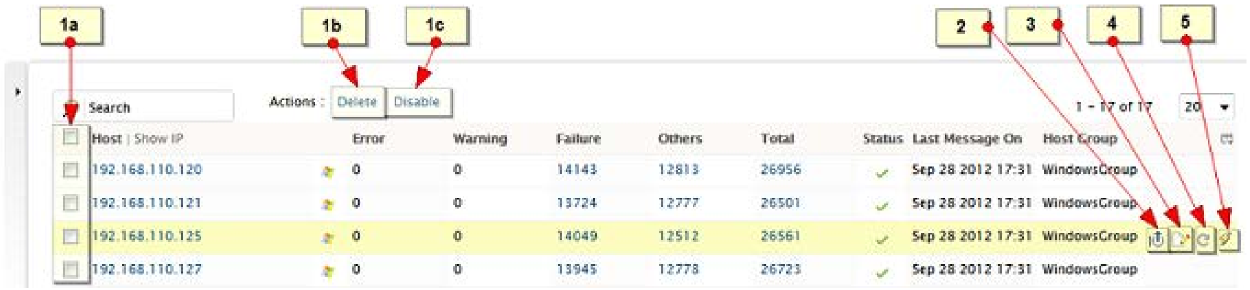
Click the **Edit user details** icon. The **Edit user details** window pops up.
Change the *User Name*, *Password*, *Web Protocol*, and *Web Port* as per requirement.
Once you have made the required changes, click **Save** to save the changes. Click **Cancel** to cancel the user detail changes.

Manage Hosts

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

- Manage Hosts
- Manage Host Groups

Hosts



□	Host | Show IP	Error	Warning	Failure	Others	Total	Status	Last Message On	Host Group
□	192.168.110.120	0	0	14143	12813	26956	✓	Sep 28 2012 17:31	WindowsGroup
□	192.168.110.121	0	0	13724	12777	26501	✓	Sep 28 2012 17:31	WindowsGroup
□	192.168.110.125	0	0	14049	12512	26561	✓	Sep 28 2012 17:31	WindowsGroup
□	192.168.110.127	0	0	13945	12778	26723	✓	Sep 28 2012 17:31	WindowsGroup

How to edit a host?

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

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

How to delete a host?

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

How to disable, enable a host?

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

Other operations on host(s)

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

2. To view the last 10 events from the specific host, use the 'Show Last 10 Events' icon.

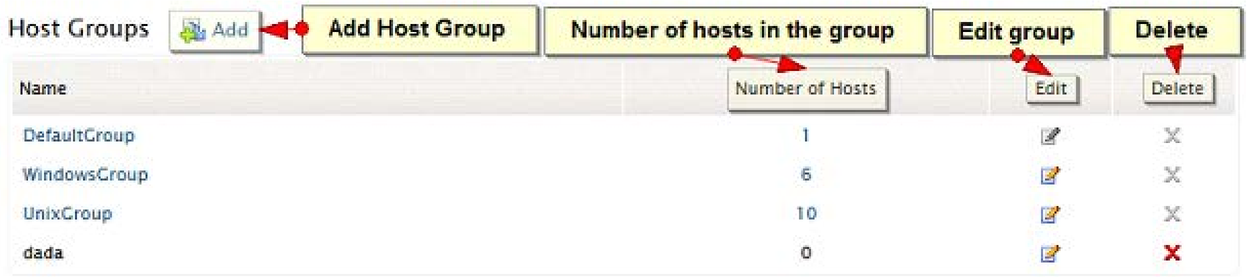
3. Use the Edit icon to edit the selected host.
4. To troubleshoot the host for connectivity, use the ‘Ping Now’ icon.
5. If the host is disabled, use the ‘Enable’ icon to enable it and if it enabled, use the 'Disable' icon to diasable it.

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

All Hosts

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

Host Groups



Name	Number of Hosts	Edit	Delete
DefaultGroup	1	✎	✗
WindowsGroup	6	✎	✗
UnixGroup	10	✎	✗
dada	0	✎	✗

How to edit a host group?

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

How to delete a host group?

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

Host Groups

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

Import

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

How to import log files?

Refer the 'Import log file' topic to import the logs.

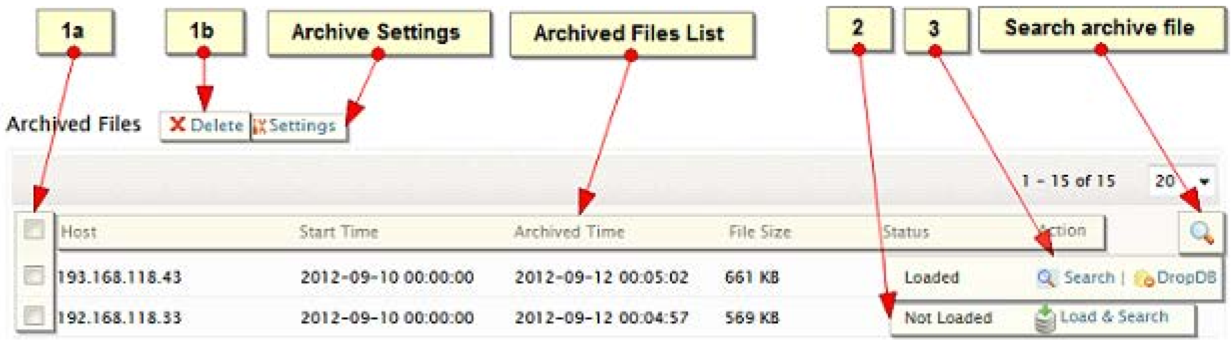
Imported Log Files

In the Imported Log Files page all the logs imported to EventLog Analyzer for monitoring are displayed. There are two tabs, Event log imports and Application log imports.
The **Event log imports** table displays the event log files imported along with the name of the imported file, the name of the host from which it was imported, the type of log, the method of import (HTTP/FTP), the time it was imported, the start time and end time of the log record, and the type of report generated.

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

Archive

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



□	Host	Start Time	Archived Time	File Size	Status	Action
□	193.168.118.43	2012-09-10 00:00:00	2012-09-12 00:05:02	661 KB	Loaded	Search | DropDB
□	192.168.118.33	2012-09-10 00:00:00	2012-09-12 00:04:57	569 KB	Not Loaded	Load & Search

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

How to delete archived files?

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

How to generate report from the archived files?

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

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.

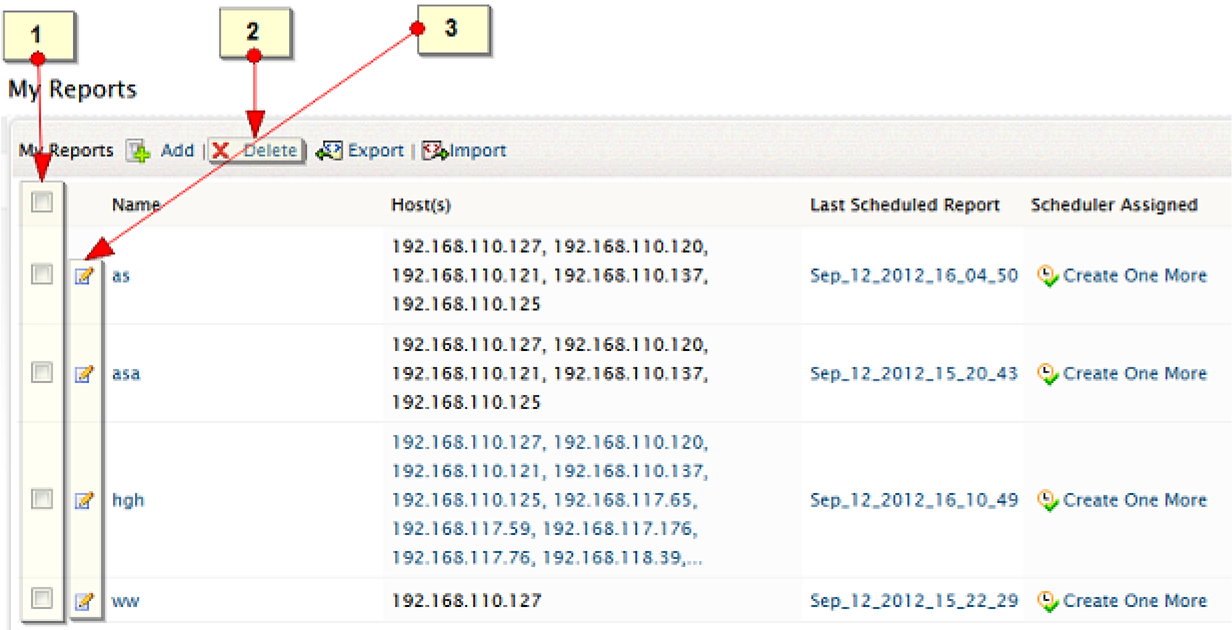
Report Profiles

To edit report in EventLog Analyzer, use the following menu option:

- **Settings** tab > **Report Profiles** > **Edit/ Del**

How to edit report profile?

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



□		Name	Host(s)	Last Scheduled Report	Scheduler Assigned
□	✎	as	192.168.110.127, 192.168.110.120, 192.168.110.121, 192.168.110.137, 192.168.110.125	Sep_12_2012_16_04_50	Create One More
□	✎	asa	192.168.110.127, 192.168.110.120, 192.168.110.121, 192.168.110.137, 192.168.110.125	Sep_12_2012_15_20_43	Create One More
□	✎	hgh	192.168.110.127, 192.168.110.120, 192.168.110.121, 192.168.110.137, 192.168.110.125, 192.168.117.65, 192.168.117.59, 192.168.117.176, 192.168.117.76, 192.168.118.39,...	Sep_12_2012_16_10_49	Create One More
□	✎	ww	192.168.110.127	Sep_12_2012_15_22_29	Create One More

3. Use the Edit icon to edit the selected report profile.

How to delete report profile?

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

My Reports

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

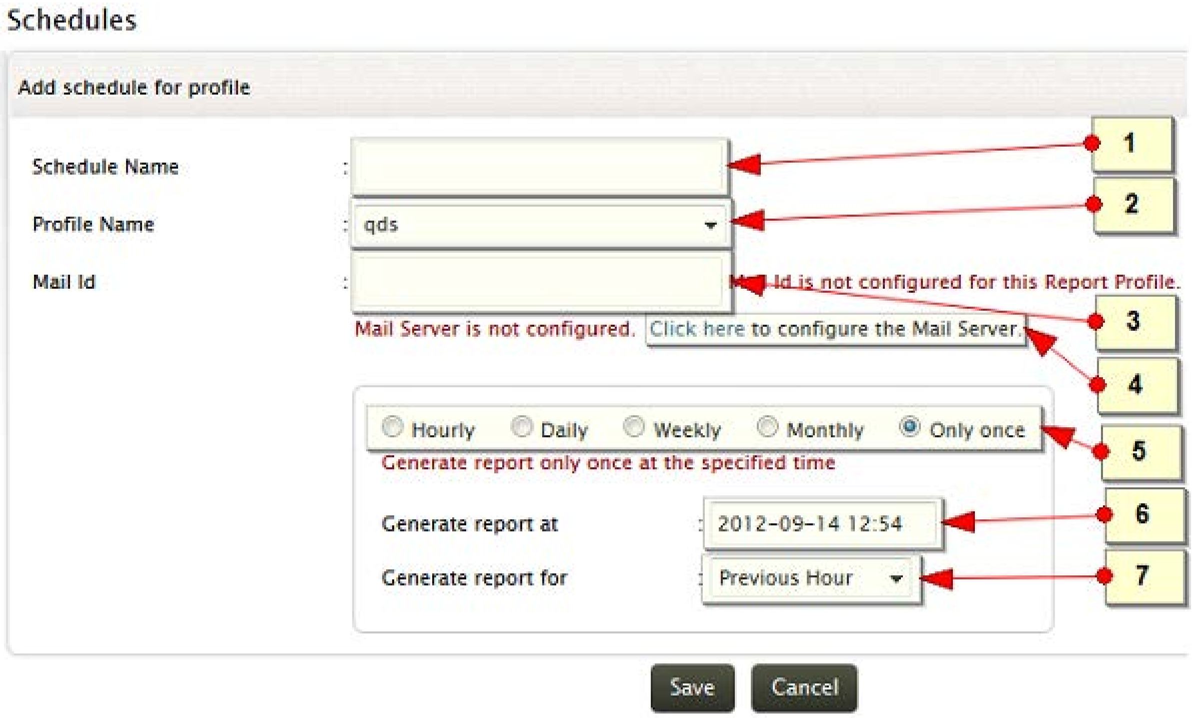
Schedule

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

To create a scheduler for a report profile, use the following menu option:

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

To create a schedule, follow the steps given below:



Schedules

Add schedule for profile

Schedule Name :

Profile Name : qds

Mail Id :

Mail Id is not configured for this Report Profile.

Mail Server is not configured. Click here to configure the Mail Server.

○ Hourly ○ Daily ○ Weekly ○ Monthly ● Only once

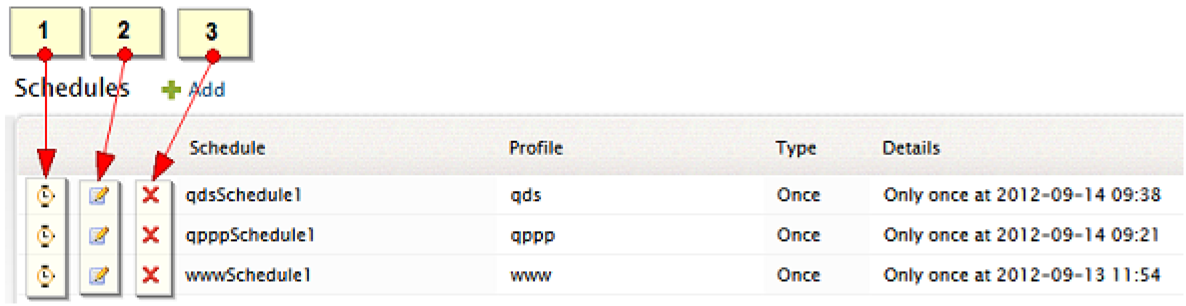
Generate report only once at the specified time

Generate report at : 2012-09-14 12:54

Generate report for : Previous Hour

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

How to edit schedule?



			Schedule	Profile	Type	Details
⏲	✎	✕	qdsSchedule1	qds	Once	Only once at 2012-09-14 09:38
⏲	✎	✕	qpppSchedule1	qppp	Once	Only once at 2012-09-14 09:21
⏲	✎	✕	wwwSchedule1	www	Once	Only once at 2012-09-13 11:54

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

How to disable/enable schedule?

- Use the Enable/Disable icon to enable or disable the schedule

How to edit schedule?

On the table row of a specific schedule Edit icon is available.

- Use the Edit icon to edit the selected schedule.

How to delete schedule?

- Use the Delete icon to delete the respective schedule.

Schedules

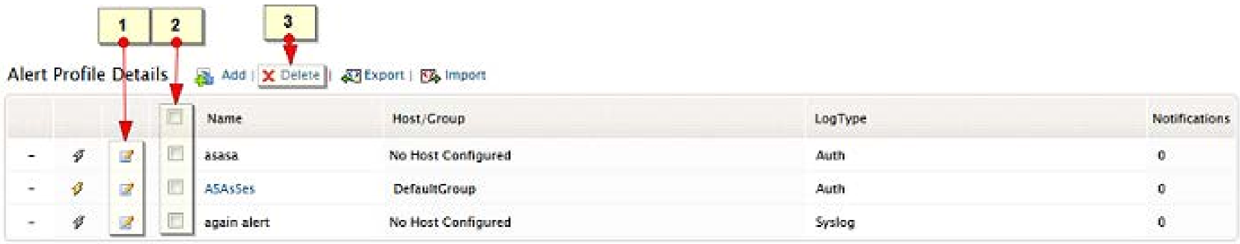
In the Schedules table, all the schedules created are displayed with enable/disable option, edit option, delete option, the name of the schedule, the report profile associated to the schedule, type of schedule, and the details of the reports generated as per schedule.

Alerts

To edit alert profile in EventLog Analyzer, use the following menu option:

- **Settings** tab > **Alerts** > **Edit/ Del**

How to edit alert profile?



Alert Profile Details

			□	Name	Host/Group	LogType	Notifications
-			□	asasa	No Host Configured	Auth	0
-			□	ASAsSes	DefaultGroup	Auth	0
-			□	again alert	No Host Configured	Syslog	0

Edit/ Del menu will take you to the **Alert Profile Details** table, where all the alert profiles are listed. On the table row of a specific profile Edit menu icon is available.

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

How to delete report profile?

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

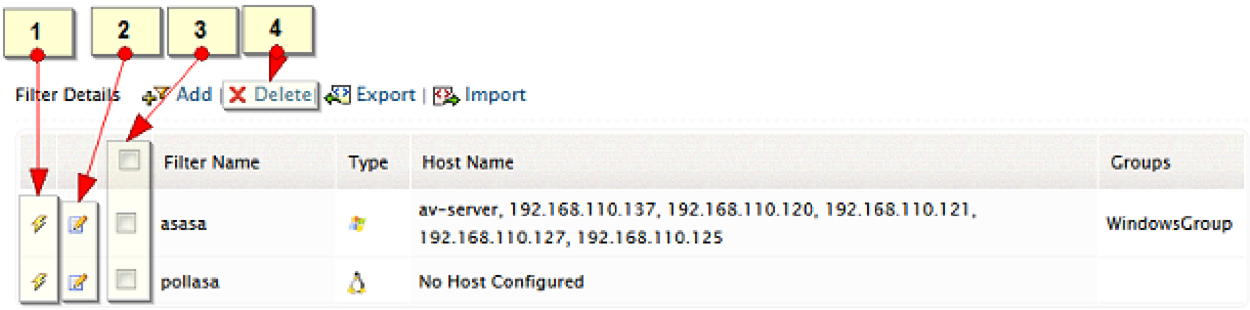
All Alerts

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

Database Filter

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

How to edit/delete database filter?



		□	Filter Name	Type	Host Name	Groups
		□	asasa		av-server, 192.168.110.137, 192.168.110.120, 192.168.110.121, 192.168.110.127, 192.168.110.125	WindowsGroup
		□	pollasa		No Host Configured	

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

How to disable/enable database filter?

1. Use the Enable/Disable icon to enable or disable the filter

How to edit filter?

On the table row of a specific filter Edit icon is available.

2. Use the Edit icon to edit the selected filter.

How to delete filter?

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

Filter Details

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

Settings

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

- Manage User
- DB Storage Settings
- External Authentication
- Server Diagnostics
- Rebranding

Manage User

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

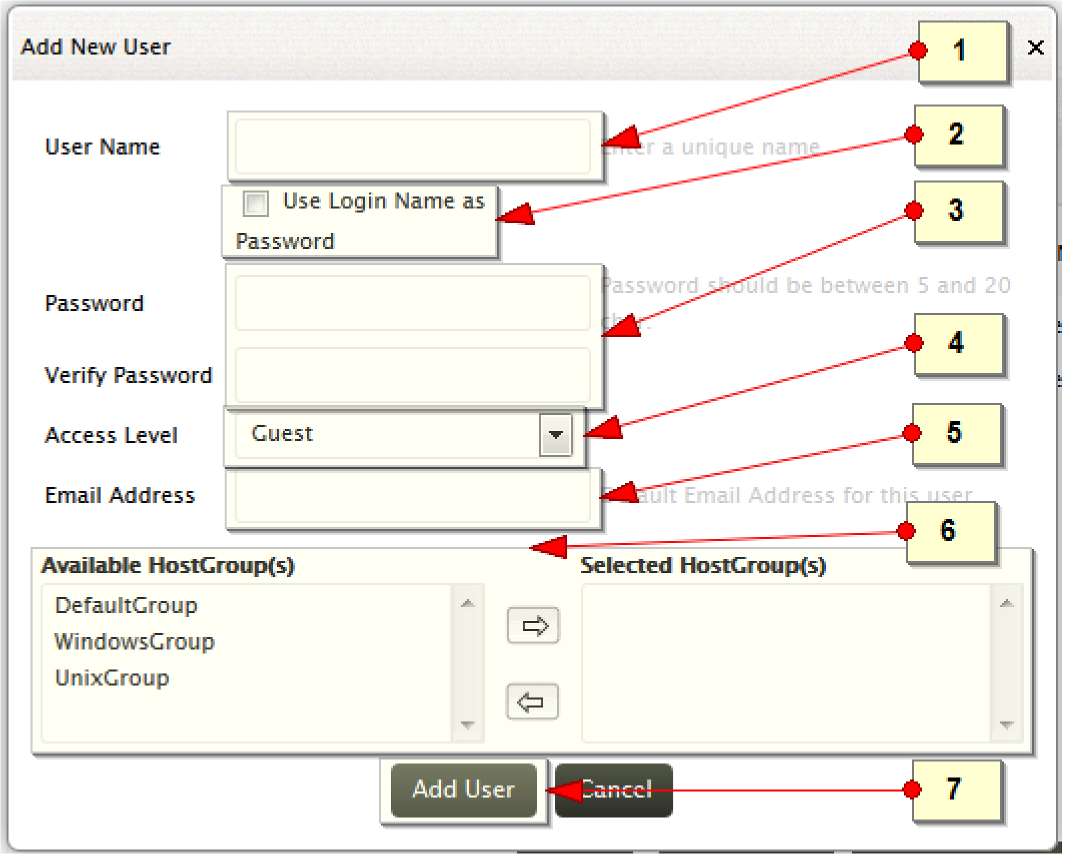
- Add users
- Manage Users
- Import users from Active Directory

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

How to add a new EventLog Analyzer user?

To add new users, use the following menu options:

Settings tab > Admin Settings: Manage User: **Add** > **Add New User**
Add New User window pops-up

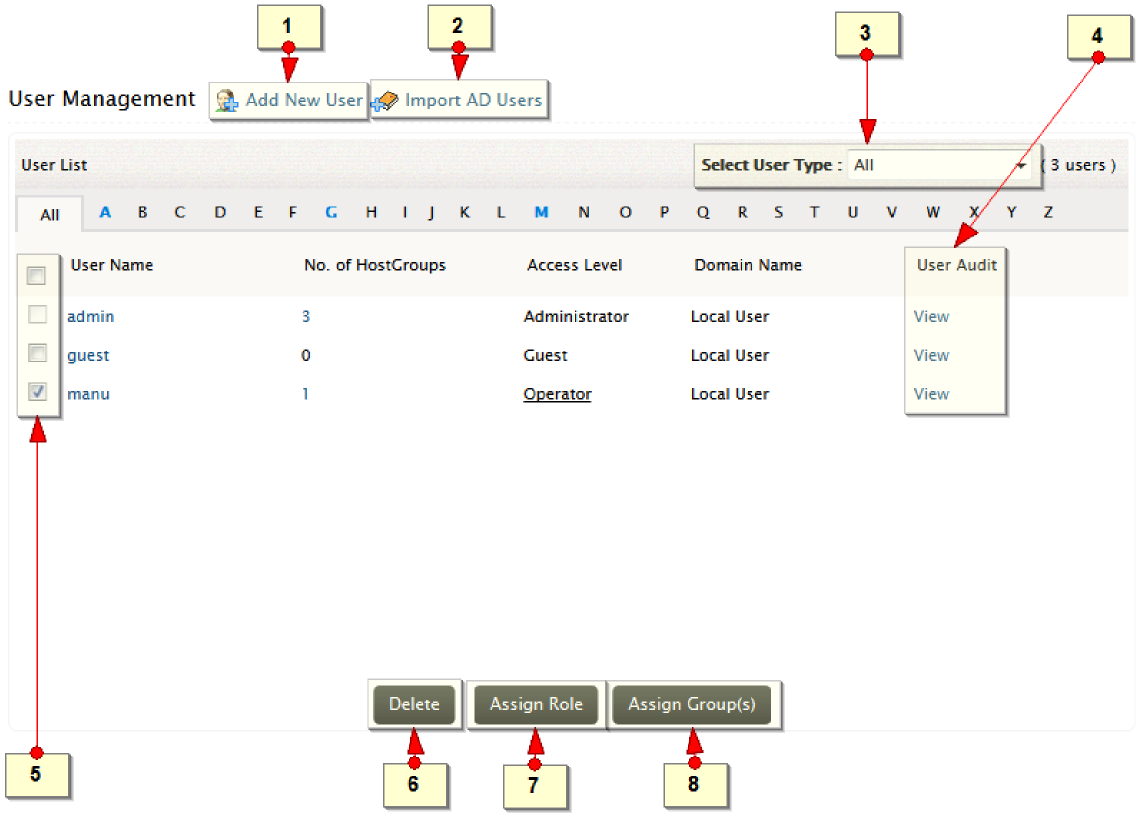


1. Enter a user name for the user as per the company policy.
2. The login name can be used as password. If it is used, the users should be asked to set the password of their choice. For temporary user and evaluation this facility can be used, but this is **not** recommended for permanent use as it will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

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

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

To manage the EventLog Analyzer users, use the following menu options:
Settings tab > Admin Settings: Manage User: **All Users**
In the user management screen all the users of EventLog Analyzer are listed with user's login name, the host group(s) to which they have access, the access level privilege, the domain in the network to which the users belongs to, and link to view the audit details of the users.



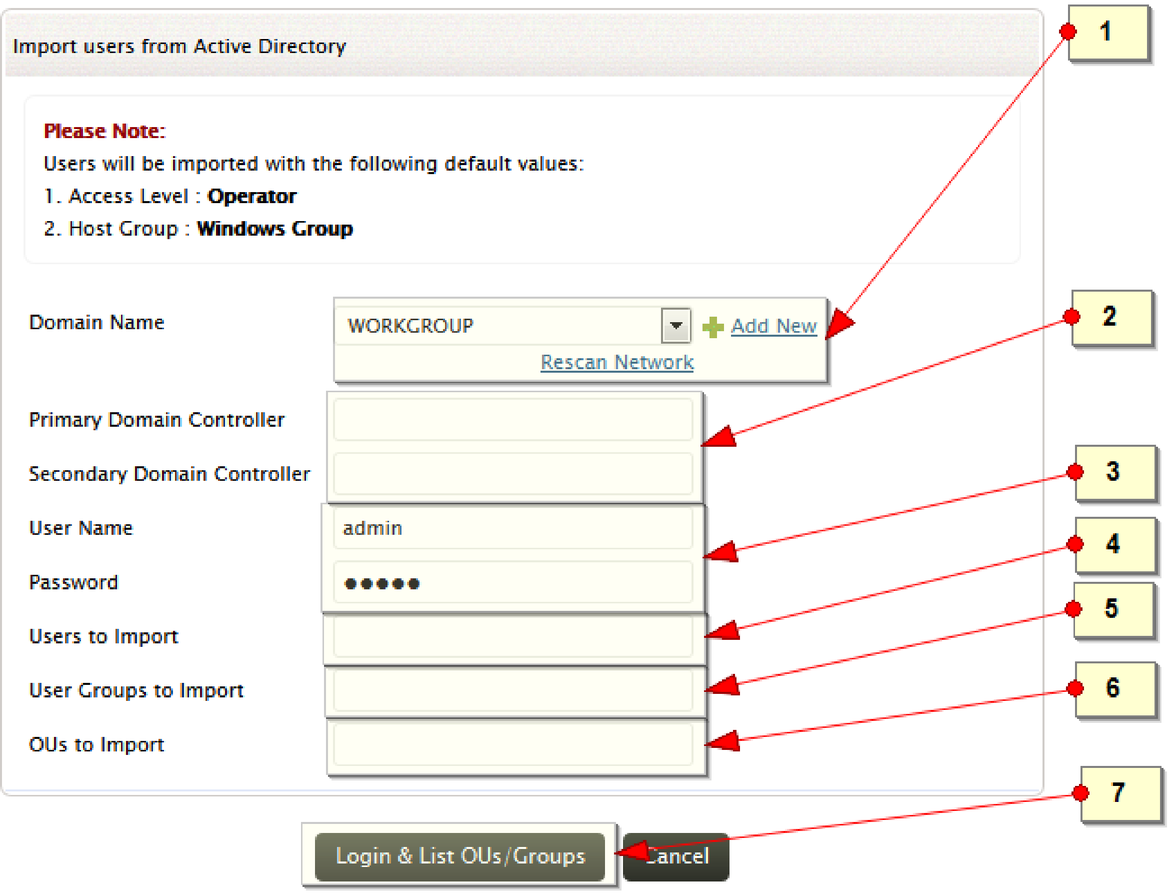
	User Name	No. of HostGroups	Access Level	Domain Name	User Audit
☐	admin	3	Administrator	Local User	View
☐	guest	0	Guest	Local User	View
☑	manu	1	Operator	Local User	View

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

How to import users from Active Directory in to EventLog Analyzer?

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

Settings tab > Admin Settings: Manage User: **Import AD Users** > User Management: **Import AD Users**
Settings tab > Admin Settings: External Authentication: > **AD Schedule/Enable** > Import users: **Import Users**
Import users from Active Directory window pops-up



Import users from Active Directory

Please Note:
Users will be imported with the following default values:
1. Access Level : **Operator**
2. Host Group : **Windows Group**

Domain Name	WORKGROUP
Primary Domain Controller	
Secondary Domain Controller	
User Name	admin
Password	●●●●●
Users to Import	
User Groups to Import	
OUs to Import	

Zoho Corporation Pvt. Ltd.

1. Select the network domain from which the AD users are to be imported. If there are domains displayed, rescan the network for domains using the **Rescan Network** link. Alternatively, add a new domain using **Add New** link
2. Specify the DNS name of the Primary and Secondary Domain Controller. If there are more than one secondary domain controller, enter the names separated by comma
3. Enter the user name and password of the domain controller
4. If you want to import only specific users, enter the respective user names. Separate multiple names by comma
5. If you want to import only users of specific user group(s), enter the respective user group name(s). Separate multiple names by comma
6. If you want to import only users of specific organizational unit(s) (OU), enter the respective user OU name(s). Separate multiple names by comma
7. Click **Login and List OUs** to fetch the Organizational Units (OUs) from the network domain

Database Storage Settings

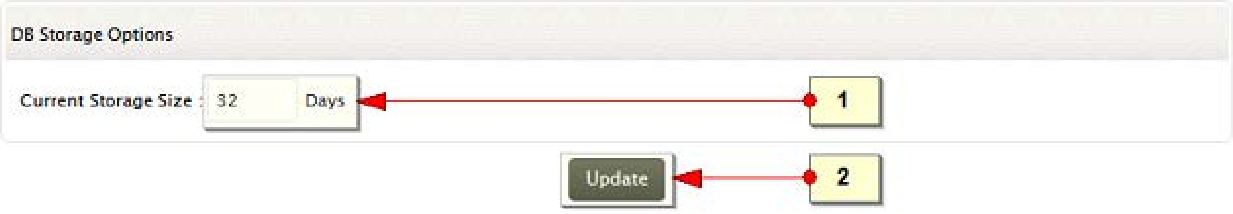
EventLog Analyzer retains the log data in the database for a limited period to process. After the period is over, the data is purged from the database. Keeping the logs in the database forever will eat up the memory space and will deteriorate the application performance.

How to set the database storage size?

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

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

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



DB Storage Options

Current Storage Size : 32 Days

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

External Authentication

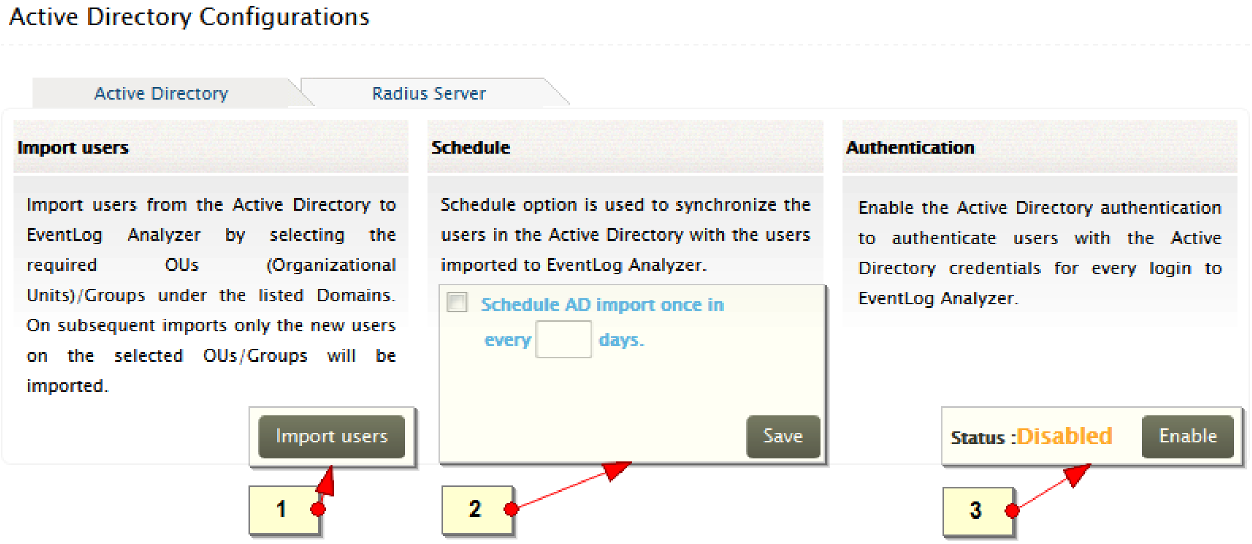
EventLog Analyzer provides two external user authentications apart from the local authentication. They are **Active Directory** authentication and **Remote Authentication Dial-in User Service (RADIUS)** authentication. Configure the Active Directory settings and RADIUS server settings

Active Directory configurations

To access Active Directory configurations, use the following menu options:

- **Settings** tab > Admin Settings: External Authentication: > AD: **Schedule/Enable**

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



Active Directory Configurations

Import users from the Active Directory to EventLog Analyzer by selecting the required OUs (Organizational Units)/Groups under the listed Domains. On subsequent imports only the new users on the selected OUs/Groups will be imported.

Schedule option is used to synchronize the users in the Active Directory with the users imported to EventLog Analyzer.

☐ Schedule AD import once in every ____ days.

Enable the Active Directory authentication to authenticate users with the Active Directory credentials for every login to EventLog Analyzer.

Status :Disabled

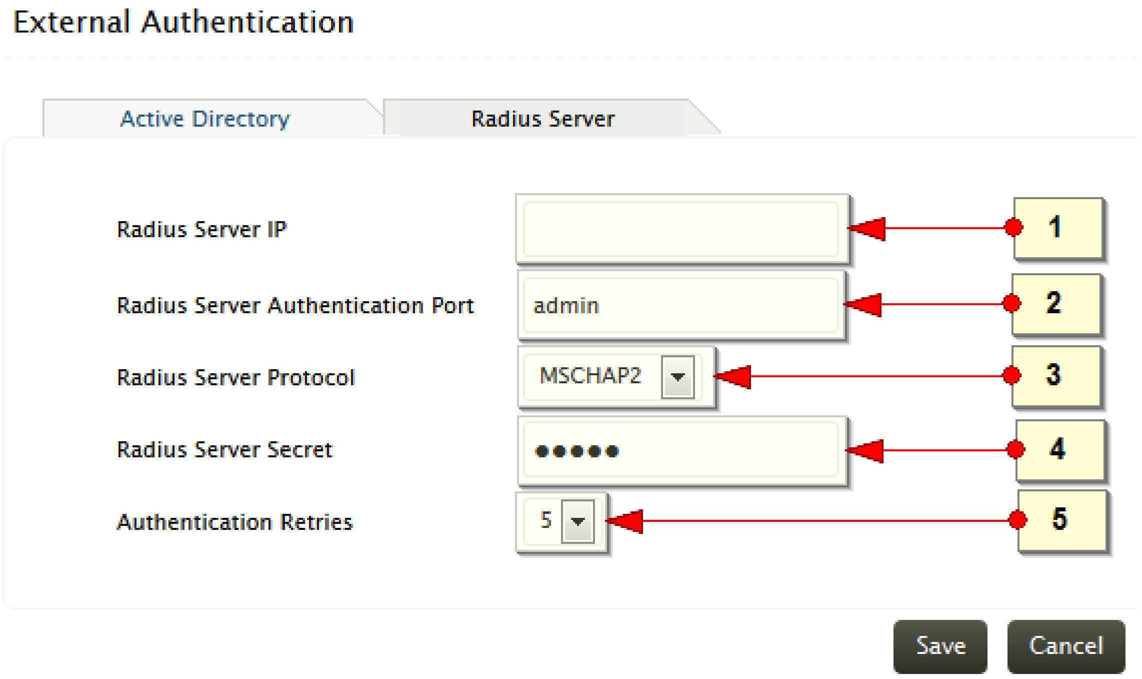
1. Import Active Directory users in to EventLog Analyzer. Refer the procedure given in User Management section.
2. To synchronize the current AD users in EventLog Analyzer, periodically import the users. Select the Schedule AD import once in every __ days option and enter the number of days and save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

RADIUS server configurations

To access RADIUS server configurations, use the following menu options:

- **Settings** tab > Admin Settings: External Authentication: > RADIUS: **Authentication**

How to configure RADIUS server authentication?



External Authentication

Radius Server IP
Radius Server Authentication Port: admin
Radius Server Protocol: MSCHAP2
Radius Server Secret: ●●●●●
Authentication Retries: 5

RADIUS server authentication can be set as default authentication for EventLog Analyzer.

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

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

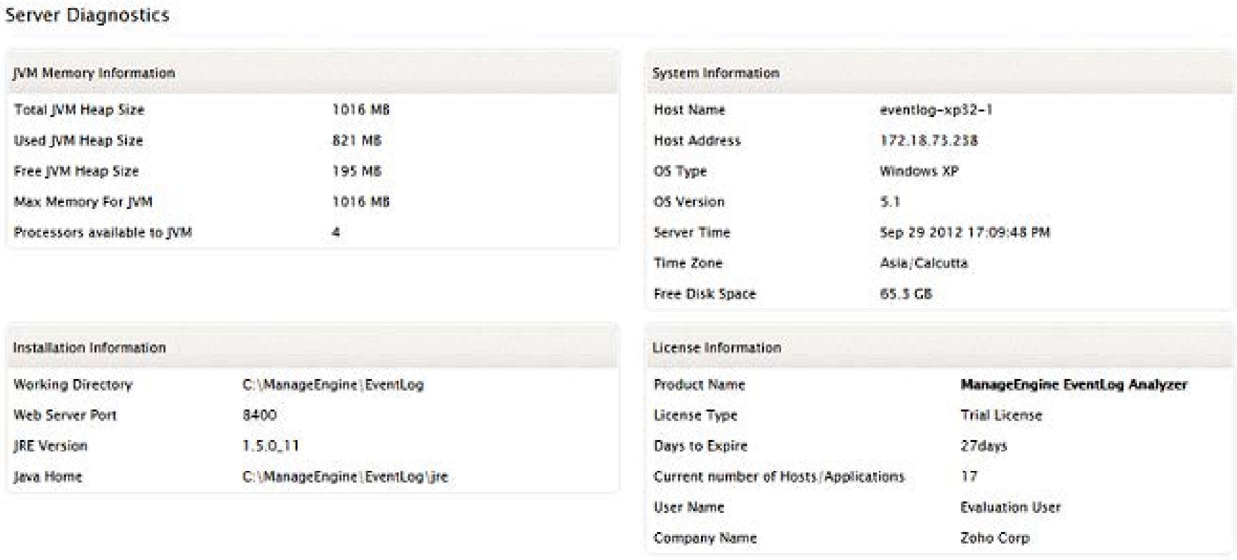
Server Diagnostics - EventLog Analyzer Distributed Edition Admin Server

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

How to get the EventLog Analyzer server health details?

Use the following menu option.

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



Server Diagnostics

JVM Memory Information	
Total JVM Heap Size	1016 MB
Used JVM Heap Size	821 MB
Free JVM Heap Size	195 MB
Max Memory For JVM	1016 MB
Processors available to JVM	4

System Information	
Host Name	eventlog-xp32-1
Host Address	172.18.73.238
OS Type	Windows XP
OS Version	5.1
Server Time	Sep 29 2012 17:09:48 PM
Time Zone	Asia/Calcutta
Free Disk Space	65.3 GB

Installation Information	
Working Directory	C:\ManageEngine\EventLog
Web Server Port	8400
JRE Version	1.5.0_11
Java Home	C:\ManageEngine\EventLog\jre

License Information	
Product Name	**ManageEngine EventLog Analyzer**
License Type	Trial License
Days to Expire	27days
Current number of Hosts/Applications	17
User Name	Evaluation User
Company Name	Zoho Corp

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

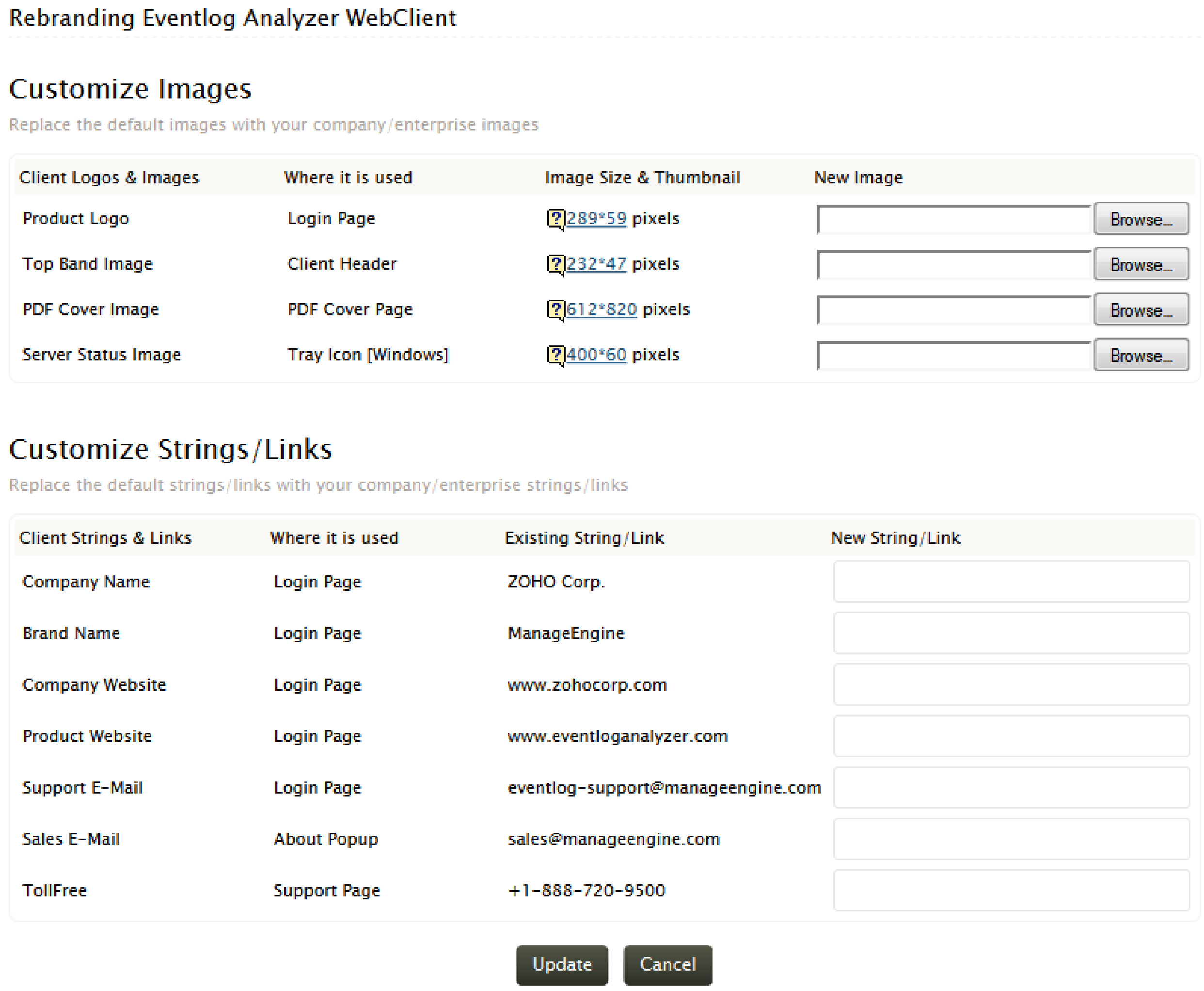
Rebranding EventLog Analyzer Distributed Edition Admin Client

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

How to rebrand the EventLog Analyzer client?

Use the following menu option.

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



Rebranding Eventlog Analyzer WebClient

Customize Images

Replace the default images with your company/enterprise images

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

Customize Strings/Links

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

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

Customize Images

Replace the default images with your company/enterprise images

Client Logs & Images	Where it is used	Image Size & Thumbnail	New Image
Product Logo	Login Page	289*59 pixels	
Top Band Image	Client Header	232*47 pixels	
PDF Cover Image	PDF Cover Page	612*820 pixels	
Server Status Image	Tray Icon (Windows)	400*60 pixels	

Customize Strings/Links

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

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

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

Note:

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

Help, Questions, and Tips

EventLog Analyzer Help

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

- Upgrade
- Support
- About
- User Guide
- Feedback

Upgrade

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

Support

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

About

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

User Guide

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

Feedback

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

Frequently Asked Questions - EventLog Analyzer Distributed Edition Admin Server

General

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

   We recommend distributed setup (Distributed Edition):

   - If yours is a **large enterprise**, which have hundreds of security devices (like Windows hosts, Linux hosts, servers), Switches and Routers to manage across different geographical locations.
   - If you are a **Managed Security Service 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** or later. To convert, you need download the EventLog Analyzer 6.0 or later exe/bin and install as **Admin Server** and then you need to convert the existing installation of EventLog Analyzer 6.0 or later to **Managed Server**. Refer the procedure in the below help link:

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

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

   Once you have deleted the **Managed Server**, to re-add follow the procedure given below:

   - Reinitialize the Managed Server.

- Re-register the Managed Server with Admin Server by executing the *<EventLog Analyzer Home>\troubleshooting\***registerWithAdminServer.bat/sh** file.
- 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.

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

Troubleshooting Tips - EventLog Analyzer Distributed Edition Admin Server

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

Troubleshooting - 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 hasbeen configured?
      iii. Are the **Ports** required areopened/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.

Troubleshooting - 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

Additional Utilities

EventLog Analyzer - Additional Uitilites

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

Working with SSL

Configuring Secure Communication - SSL

The SSL protocol provides several features that enable secure transmission of Web traffic. These features include data encryption, server authentication, and message integrity.

You can enable secure communication from web clients to the EventLog Analyzer server using SSL.

Note: The steps provided describe how to enable SSL functionality and generate certificates only. Depending on your network configuration and security needs, you may need to consult outside documentation. For advanced configuration concerns, please refer to the SSL resources at http://www.apache.org and http://www.modssl.org

- **Generating a valid certificate**
- **Disabling HTTP**
- **Enabling HTPPS (SSL)**
- **Verifying SSL Setup**
- **Configuring HTTPS Configuration Parameters for 64 bit/128 bit encryption**
- **Using the existing SSL certificate**
- **How to install SSL certificate for EventLog Analyzer**

Generating a valid certificate

Stop the server, if it is running.

Follow the instructions given below for SSL Installation:
If you have a keystore file for using HTTPS, place the file under *<EventLog Analyzer Home>\server\default\conf* directory and rename it as "**chap8.keystore**"

Disabling HTTP

When you have enabled SSL, HTTP will continue to be enabled on the web server port (default 8080). To disable HTTP follow the steps below:

1. Edit the **server.xml** file present in <*EventLog Analyzer Home*>/server/default/deploy/jbossweb-tomcat50.sar directory.
2. Comment out the HTTP connection parameters, by placing the <!-- tag before, and the --> tag after the following lines:

```
<Connector port="8080" address="${jboss.bind.address}"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" redirectPort="8443" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true"/>
```

Enabling HTPPS (SSL)

- In the same file, enable the HTTPS connection parameters, by removing the <!-- tag before, and the --> tag after the following lines:

```
<!--
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
keystorePass="rmi+ssl" sslProtocol = "TLS" />
-->
```

Note: While creating keystore file, you can enter the password as per your requirement. But ensure that the same password is configured, in the **server.xml** file. Example password is configured as '**rmi+ssl**'.

Verifying SSL Setup

1. Restart the EventLog Analyzer server.
2. Verify that the following message appears in the command window after the EventLog Analyzer application is started:

Server started.
Please connect your client at https://localhost:8500

3. Connect to the server from a web browser by typing https://<*hostname*>:8500 where <*hostname*> is the machine where the server is running

Configuring HTTPS Configuration Parameters for 64 bit/128 bit encryption

If you want to configure the HTTPS connection parameters for 64 bit/128 bit encryption, add the following parameter at the end of the SSL/TLS Connector tag:

```
SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
keystorePass="rmi+ssl" sslProtocol = "TLS"
SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"/>
```

Using the existing SSL certificate

- You can export the Wild card certificate to a **.pfx** file and then follow the instructions given below to configure the same in EventLog Analyzer.
- Stop ManageEngine EventLog Analyzer service
- Copy the **.pfx** file to the location *<EventLog Analyzer Home>\server\default\conf*

- Go to the location *<EventLog Analyzer Home>\server\default\deploy\jbossweb-tomcat50.sar* and open the file **server.xml** in word pad, and locate the entries in the file as below:

```
<!-- 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"/>
```

- Replace the file name *chap8.keystore* with the pfx file name (**<pfx file name>.pfx**) and also enter the **keystoreType="pkcs12"** after the file name and also replace the **keystorePass** value '*rmi+ssl*' with the password for the **.pfx** file.

- The entries should be as given below:

```
<!-- 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/<pfx file name>.pfx"
keystoreType="pkcs12"
keystorePass="<password for the .pfx file>" sslProtocol = "TLS"
SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"/>
```

- Restart EventLog Analyzer service.

How to install SSL certificate for EventLog Analyzer

Follow the instructions given below for SSL Installation:

Step 1: Create a new Keystore

1. You will be using the keytool command to create and manage your new Keystore file. When you are ready to create your keystore go to the directory where you plan to manage your Keystore and certificates (*<EventLog Analyzer Home>\jre\bin\*). Enter the following command:

   keytool -genkey -alias <our_alias_name> or [Domain Name] -keyalg RSA -keystore chap8.keystore
   (For example: keytool -genkey -alias tomcat -keyalg RSA -keystore chap8.keystore)

2. You will be prompted to choose a password for your keystore. You will then be prompted to enter your Organization information. When it asks for first and last name, DO NOT mention your first and last name, but rather it is your Fully Qualified Domain Name for the site you are securing say, helpdesk.yourdomain.com. If you are ordering a Wildcard Certificate this must begin with the * character say, *.yourdomain.com)

3. After you have completed the required information confirm that the information is correct by entering 'y' or 'yes' when prompted. Next, you will be asked for your password to confirm. Make sure to remember the password you choose. Your keystore file named **chap8.keystore** is now created in your current working directory.

Step 2: Generate a CSR from your new keystore

1. Next, you will use keytool to create the Certificate Signing Request (CSR) from your Keystore. Enter the following command

   keytool -certreq -alias <your_alias_name> or [Domain Name] -file csr.txt -keystore chap8.keystore
   (For example: keytool -certreq -alias tomcat -file csr.txt -keystore chap8.keystore)

2. Type the keystore password that you chose earlier and hit Enter.
3. Your CSR file named **csr.txt** is now created in your current directory. Open the CSR with a text editor, and copy and paste the text (including the BEGIN and END tags) into the CA web order form. Be careful to save the keystore file (chap8.keystore) as your certificates will be installed to it later.

Step 3: How to install your SSL Certificate

1. Download your Certificate files from the email from CA to the directory where your keystore (chap8.keystore) was saved during the CSR creation process. The certificate must be installed to this exact keystore. If you try to install it to a different keystore it will not work. The certificates you downloaded must be installed to your keystore in the correct order for your certificate to be trusted. If the certificates are not installed in the correct order, then the certificate will not authenticate properly.
2. Install the Root Certificate file:
   - Each time you install a certificate to your keystore you will be prompted for the keystore password, which you chose when generating your CSR.
   - Type the following command to install the Root certificate file:

   keytool -import -trustcacerts -alias root -file TrustedRoot.crt -keystore chap8.keystore
   NOTE: Choose 'Yes' if you get prompted with a message that says "Certificate already exists in system-wide CA keystore under alias <entrustsslca> Do you still want to add it to your own keystore? [no]:"
   You will get a confirmation stating that the "Certificate was added to keystore".

3. Install the intermediate certificates if any. (Follow the instructions provided by the CA)
4. Install the Primary Certificate file:
   - Type the following command to install the Primary certificate file:

   keytool -import -trustcacerts -alias tomcat -file <your_domain_name>.crt -keystore chap8.keystore

This time you should get a slightly different confirmation stating that the "Certificate reply was installed in keystore" If it asks if you want to trust the certificate. Choose y or yes. Your Certificates are now installed to your keystore file (keystore.key) and you just need to configure your server to use the keystore file.

Convert EventLog Analyzer Standalone Server to Managed Server

To convert existing Standalone Server to Distributed - 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
```

Technical Support

EventLog Analyzer Technical Support

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

Procedure to resolve EventLog Analyzer issue with EventLog Analyzer support
Best in the industry technical support and other informal means to get EventLog Analyzer issues resolved.
Adopt the following ways progressively.

Knowledge Base & Community

- Go through the FAQ
- Look out in the trouble shooting tips
- Browse through the EventLog Analyzer forum

Best in the industry technical support

- Send email to eventlog-support@manageengine.com
- Call toll free telephone number (**+1-888-720-9500**)
- Ask for a meeting (**Zoho Meeting**) – web conference

EventLog Analyzer Support Channels

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

The support page can access using the following menu:

- **Help** > **Support**

Link	Description
Request Technical Support	Click this link to submit a form from the EventLog Analyzer website, with a detailed description of the problem that you encountered
Create Support Information File [SIF]	Click this link to create a ZIP file containing all the server logs that the Technical Support team will need, to analyze your problem. You can then send this ZIP file to eventlog-support@manageengine.com or upload the ZIP file to our ftp server by clicking on Upload to **FTP Server**, in the pop-up window provide your email ID and browse for the zipped SIF file and then press **Upload** button. The procedure to create SIF without web client and send it EventLog Analyzer is also given.
Reset LogCollector	This menu is used for running EventLog Analyzer in the debug mode. Please contact eventlog-support@manageengine.com before resetting log collector.
Troubleshooting Tips	Click this link to see the common problems typically encountered by users, and ways to solve them
Need a Feature	Click this link to submit a feature request from the EventLog Analyzer website
Log Level Setting	Click this link to set the granualarity level of server logs to be stored in the log files
Toll-free Number	Call the toll-free number +1 888 720 9500 to talk to the EventLog Analyzer Technical Support team directly
User Forums	Click this link to go to the EventLog Analyzer user forum. Here you can discuss with other EventLog Analyzer users and understand how EventLog Analyzer is being used across different environments
Join Meeting	Click this link to join a meeting with EventLog Analyzer team if it is in progress and if you have a invitation with Meeting Key or Meeting Number or register for a future meeting. There will be two meeting services available viz., ZOHO Meeting and Webex.

The Support page also displays the latest announcements and discussions in the EventLog Analyzer user forum

Create EventLog Analyzer SIF and Send

Procedure to create a Support Information File (SIF) and send the SIF to EventLog Analyzer support

We would recommend the user to create a **Support Information File** (**SIF**) and send the SIF to eventlog-support@manageengine.com The SIF will help us to analyze the issue you have come across and propose a solution.

The instructions for creating the SIF is as follows:

- Login to the web client and click the **Help** > **Support** menu.
- Click the **Create Support Information File** link show in that page.
- Wait for 30-40 Secs and again click the **Support** menu.
- Now you will find new links **Download** and **Upload to FTPServer**.
- You can either download the SIF by clicking on the **Download** link and then send the downloaded SIF to eventlog-support@manageengine.com or click the **Upload to FTPServer** and provide the details asked and upload the file.

Procedure to create SIF and send the file to ZOHO Corp., if the EventLog Analyzer server or web client is not working

If you are unable to create a SIF from the web client UI, you can zip the files under '*log*' folder, which is located in *<EventLog Analyzer Home>\server\default\log* (default path) and send the zip file by upload it in the following ftp link: http://bonitas.zohocorp.com/upload/index.jsp?to=eventloganalyzer-support@manageengine.com

Reset EventLog Analyzer Log Collector

Reset Log Collector

The Reset LogCollector is used for troubleshooting EventLog Analyzer. This provision is used for running EventLog Analyzer in the debug mode. Please contact eventlog-support@manageengine.com before resetting log collector.

Log Level Settings - EventLog Analyzer

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

1. Select the **Server Log Filter Settings** (values from 2 to 5) from the combo box.

2. Select the **Level of Log data to be stored** from the combo box. The values available are:
   a. ALL
   b. FINEST
   c. FINER
   d. FINE
   e. CONFIG
   f. INFO
   g. WARNING
   h. SEVERE
   i. OFF

3. Select the **Logger Name** from the list. The loggers available are given below. For each available logger or set of loogeres, you can set the log filter level and log level independently.

4. Click **Save Settings** button to save the log level settings. Setting completion message with details appears on top of the screen. Click **Cancel** button to cancel the log level setting action

The loggers available are given below:

1. com.adventnet.la
2. com.adventnet.la.RSDatasetModel
3. com.adventnet.la.DepartmentUtil
4. com.adventnet.la.DefaultDataFormatter
5. com.adventnet.la.GLinkGenerator
6. com.adventnet.la.HtmlTimePack
7. com.adventnet.la.RunQuery
8. com.adventnet.la.SQLConstructor
9. com.adventnet.la.SyslogQueryHandlerImpl
10. com.adventnet.la.TableDatasetModel
11. com.adventnet.la.GraphTag
12. com.adventnet.la.ReportDS
13. com.adventnet.la.QueryHandlerImpl
14. com.adventnet.la.DefaultToolTipGenerator
15. com.adventnet.la.store.DBHashMap
16. com.adventnet.la.TableTag
17. com.adventnet.la.webclient.SupportAction
18. com.adventnet.la.webclient.ScheduleUtil

19. com.adventnet.la.SQLGenerator
20. com.adventnet.la.LaUtil
21. com.adventnet.la.util.MetaTableCache
22. com.adventnet.la.util.DNSResolverThread
23. com.adventnet.la.util.SimulateRecords
24. com.adventnet.la.util.ResourceCheckerUtil
25. com.adventnet.la.util.dm.DMConfigurationPopulator
26. com.adventnet.la.util.dm.DMTask
27. com.adventnet.la.util.dm.ErrHostProcessHandler
28. com.adventnet.la.util.dm.DMPreProcessHandler
29. com.adventnet.la.util.dm.TblMgmtTask
30. com.adventnet.la.util.dm.ExceptionCreator
31. com.adventnet.la.util.dm.MssqlProcessHandler
32. com.adventnet.la.util.dm.SiblingPreProcessor
33. com.adventnet.la.util.dm.DMProcessor
34. com.adventnet.la.util.dm.MetaTableCacheProcessor
35. com.adventnet.la.util.dm.DMContext
36. com.adventnet.la.util.dm.DMTaskGroup
37. com.adventnet.la.util.dm.AppPreProcessor
38. com.adventnet.la.util.dm.DataManagement
39. com.adventnet.la.util.dm.DMTaskGroupConfig
40. com.adventnet.la.util.dm.DMProcessHandler
41. com.adventnet.la.util.FixedHashMap
42. com.adventnet.la.util.QueryUtil
43. com.adventnet.la.util.TransactionHandler
44. com.adventnet.la.ReportTask
45. com.adventnet.la.ReportExporter
46. com.adventnet.la.ExportCleanup
47. com.adventnet.la.SupportZipUtil
48. com.adventnet.la.ReportUtil
49. com.adventnet.sa.webclient.AddScheduleActionSa
50. com.adventnet.sa.webclient.ViewReport
51. com.adventnet.sa.webclient.util.SaUtil
52. com.adventnet.sa.webclient.EditFilterAction
53. com.adventnet.sa.util.dm.LuceneIndexProcessor
54. com.adventnet.sa.SyslogReportTask
55. com.adventnet.sa.server.DomainDiscovery
56. com.adventnet.sa.server.imp.ImportDMCrunch
57. com.adventnet.sa.server.imp.ImportAppLogManager
58. com.adventnet.sa.server.imp.ImportSysEvtLogManager
59. com.adventnet.sa.server.imp.FTPUtil
60. com.adventnet.sa.server.imp.ImportAppLogTask
61. com.adventnet.sa.server.imp.ImportLogManager
62. com.adventnet.sa.server.alert.MailAlert
63. com.adventnet.sa.server.parser.RecordWriter
64. com.adventnet.sa.server.parser.DbUtil
65. com.adventnet.sa.server.ELSInitializer
66. com.adventnet.sa.server.EAService
67. com.adventnet.logsearch.search.BatchSearch
68. com.adventnet.logsearch.index.api.ArchiveIndex
69. com.adventnet.logsearch.index.api.LogIndexingAPI
70. com.adventnet.logsearch.index.util.DBUtil