

ManageEngine 
EventLog Analyzer

Quick Start Guide



ManageEngine EventLog Analyzer Quick Start Guide

Contents

Installing and starting EventLog Analyzer	1
Connecting to the EventLog Analyzer server	2
Adding devices for monitoring	3
Adding Windows devices	3
Adding Syslog devices	4
Importing logs	5
Using predefined reports	5
Creating custom reports	6
Searching through logs	6
Creating alert profiles	7
Configuring email and SMS alerts	7
Advanced configurations	8

Installing and starting EventLog Analyzer

Download the EXE file from the [download](#) page.

Before starting the installation, check the [system requirements](#).

To install EventLog Analyzer on a **Windows OS**, execute:

- **ManageEngine_EventLogAnalyzer.exe** for the 32-bit version
- **ManageEngine_EventLogAnalyzer_64bit.exe** for the 64-bit version

To install EventLog Analyzer on a **Linux OS**, execute:

- **ManageEngine_EventLogAnalyzer.bin** for the 32-bit version
- **ManageEngine_EventLogAnalyzer_64bit.bin** for the 64-bit version

Note:

Before installing EventLog Analyzer on a Linux OS,

- Execute the following commands in the Unix Terminal or Shell, **chmod +x ManageEngine_EventLogAnalyzer.bin**
- Now, run **ManageEngine_EventLogAnalyzer.bin** by double clicking or running **./ManageEngine_EventLogAnalyzer.bin** in the Terminal or Shell.

Upon starting the installation, you will be taken through the following steps:

- Select the **Agree to the terms and conditions** of the license agreement once you read them thoroughly.
- **Select the folder** in which the product should be installed.

The default installation location is *C:\ManageEngine\EventLog Analyzer*. The location can be changed with the **Browse** option.

- Enter the **web server port**. The default port number is 8400. Ensure that the default or the selected port is not being used.

- Select the **Install EventLog Analyzer as service** option to install the product as a Windows or Linux service. By default this option is selected. Unselect this option to install as an application. Alternatively, you can also install as an application and later change it to a service. We recommend that you install it as service.
- Enter the folder name in which the product will be shown. The default name is **ManageEngine EventLog Analyzer**.
- Enter your personal details to get technical assistance.

After the installation is complete, the wizard displays the ReadMe file and starts the EventLog Analyzer server.

Before you run the product, check if the [prerequisites](#) are met.

Connecting to the EventLog Analyzer server

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

- Open a supported web browser. Type the URL as *http://<devicename>:8400* (where <devicename> is the name of the machine running EventLog Analyzer and 8400 is the default web server port)
- Log in to EventLog Analyzer using the default username/password combination of **admin/admin** and select one of the three options in **Log on to (Local Authentication, Radius Authentication, or Domain Name)**.
- Click the **Login** button.

Adding devices for monitoring

Adding Windows devices

In all Windows devices, ensure that WMI, DCOM are enabled, and logging is enabled for the respective modules/objects. To [forward the Windows event logs in syslog format, use a third party utility like SNARE](#).

(a) Adding Windows devices from a domain

1. Select the **domain** from the drop-down menu in the Settings tab. The Windows devices in the selected domain will be automatically discovered and listed.
2. Select the necessary **device(s)** by clicking on the respective checkbox(es). You can locate any device using the built-in search option or the OU filter.
3. Click on the **Add** button.

(b) Adding Windows devices from a workgroup

You can add a device from a workgroup by clicking on the **Add workgroup device** link. This will list out the devices from your workgroups.

1. Choose the **workgroup** from the Select Workgroup drop-down menu in the Settings tab.
2. Select the required **device(s)** by clicking on the respective checkbox(es).
3. Click on the **Add** button.

Note: You have the option to **update**, **reload**, and **delete** a workgroup by clicking on the respective icons next to the **Select Domain** drop-down menu.

(c) Adding Windows devices manually

Optionally, you can also manually add the device as shown below by clicking on the **Configure Manually** link.

1. Enter the **Device name** or **IP address**.
2. Enter the **Username** and **Password** with administrator credentials, and click on the **Verify login** link.
3. Click on the **Add** button.

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

Adding Syslog devices

In the **Device Management** page, navigate to the **Syslog Devices** tab and click on the **+Add Device(s)** button. Enter the **device name** or **IP address** in the Device(s) field and click on the **Add** button.

Follow the steps below to automatically discover and add the Syslog devices in your network:

1. Click on the **Discover & Add** link in the **Add Syslog Devices** window. You can discover the Syslog devices in your network based on the **IP range (Start IP to End IP)** or **CIDR**.
2. Enter the **Start IP** and **End IP** or the **CIDR range** in order to discover the Syslog devices.

3. Choose the **SNMP credentials** to automatically discover the Syslog devices in your network. By default, the public SNMP credentials can be used to scan the Syslog devices in your network.

Alternatively, you can add a SNMP credential by clicking on the **+Add Credential button**. Once you pick the SNMP credential, click on the **Scan button** to automatically discover the Syslog devices in the specified IP or CIDR range.

4. Select the **device(s)** by clicking on the respective checkbox(es). You can easily search for a device using the search box or by filtering based on the Device type and vendor.

5. Click on the **Add Device(s)** button to add the devices for monitoring.

To add other devices such as print servers, terminal servers, Oracle devices, VMware devices and more, refer the [Add Devices](#) page.

Importing logs

EventLog Analyzer gives you the option to import any flat log files and provides predefined reports for Windows (EVTX format), syslog devices, applications, and archived files. To learn how to import logs, refer the [Import log file](#) section.

Using predefined reports

EventLog Analyzer offers canned reports to help analyze network security and audit the activity of internal users. The reports provide information on approximately 750 log sources including:

- Network devices such as firewalls, routers, switches, IDS/IPS

- Applications including Oracle and MS SQL Server databases
- Web servers
- Windows and Linux/Unix machines
- IBM AS400 systems

The report groups are Windows, Applications, Network Devices, Vulnerability, vCenter, My reports, Favourites and User based reports.

Creating custom reports

The custom reports created by you are listed in the My Reports section. New reports can be added, existing reports can be scheduled, edited or deleted. Refer the [Create Custom Reports](#) section to learn how to create a custom report.

Searching through logs

EventLog Analyzer's log search functionality is very easy and allows you to search for any information. By default, the entered search term is looked-up in the log message. The search results can be saved in the PDF and CSV formats.

To know more about the search feature, refer the [How to Search](#) section, which explains how a search can be performed, and the [How to Extract Additional Fields](#) section, to learn how to extract fields from raw logs.

Creating alert profiles

EventLog Analyzer can be configured to generate an alert when a specific security event occurs. You can:

- Choose from over 500 predefined alert criteria or define custom alerts.
- Get real-time notifications through email or SMS when any event of interest occurs.
- Assign a program to be run upon alert generation.
- Configure which device or device groups are to be monitored for the events.
- Specify how many times, and within how many minutes, an event should occur for the alert to be triggered.
- Be alerted for any compliance policy specific events.
- Receive alerts for correlations, such as the occurrence of two or more events calls for further investigation.

Refer the [Create Alert Profiles](#) section to learn how to set up an alert.

Configuring email and SMS alerts

EventLog Analyzer can notify you instantly when a critical security incident occurs in your network.

- To receive email alerts and scheduled reports, you need to configure the mail server in EventLog Analyzer.
- To receive alerts on your mobile phone you need to configure the SMS Settings.

Refer the [help document](#) for the configuration steps.

Advanced configurations

- **Database migration:** Apart from the PostgreSQL database, EventLog Analyzer supports Microsoft SQL Server as the back end database. If you already have a Microsoft SQL Server in your enterprise, you can utilize the same. To know more, refer the [Migrate data from PostgreSQL to MS SQL database](#) section of the help document.
- **Archive settings:** EventLog Analyzer archives log files periodically. The archival interval and retention period of logs can be configured. The archived log data is also encrypted and timestamped.

About EventLog Analyzer

EventLog Analyzer is a comprehensive IT compliance and log management software for SIEM. It provides detailed insights into your machine logs in the form of reports to help mitigate threats in order to achieve complete network security.

\$ Get Quote

↓ Download