ManageEngine
EventLog Analyzer

# Guide to secure your EventLog Analyzer installation

www.eventloganalyzer.com

If a user belongs to the Authenticated Users group, it's possible for them to tamper with the EventLog Analyzer installation directory. To circumvent this and improve the security of your EventLog Analyzer deployment, follow the steps in this document.

# Description

The EventLog Analyzer installation directory contains important files required for it to function properly, including files that are used to start and stop the product and the license file. By default, EventLog Analyzer will be installed in the **C:\ManageEngine** folder. This will grant even non-admin users belonging to the **Authenticated Users** group **Full Control** permission over the files and folders in the product's installation directory, meaning any domain user can access the folder and modify its contents, potentially making the product unusable.

Simply removing **Authenticated Users** from the Access Control List (ACL) won't help, as this will render them unable to even start EventLog Analyzer as a service or application.

# Solution

To overcome this issue, follow the steps outlined below based on where EventLog Analyzer is installed.

1. If EventLog Analyzer is installed in C:\ManageEngine folder
2. If EventLog Analyzer is installed in C:\Program Files folder

## 1. Steps to perform if EventLog Analyzer is installed in the C:\ManageEngine folder.

By default, the C: directory in a Windows Client OS has **Authenticated Users** with the **Modify** permission for subfolders. However, the C: directory in a Windows Server OS does not have **Authenticated Users** in its ACL. So, based on the OS in which EventLog Analyzer is installed, the steps may vary.

**a)** If EventLog Analyzer is installed in a client OS

**b)** If EventLog Analyzer is installed in a server OS

### a. If EventLog Analyzer is installed in a client OS:

1. **Disable Inheritance** for the C:\ManageEngine\EventLog Analyzer folder. Refer to the Appendix below for step-by-step instructions.
2. Remove **Authenticated Users** from the folder's ACL. Refer to the Appendix for step-by-step instructions.
3. Remove the **Authenticated Users** permission for the folders listed below from the product's installation directory.

    1. <product home>\bin
    2. <product home>\lib
    3. <product home>\tools
    4. <product home>\..\elasticsearch

4. Assign the **Modify** permission for the C:\ManageEngine\EventLog Analyzer folder to users who can start the product. Refer to the Appendix for step-by-step instructions.

5. If the product is installed as a service, make sure that the account configured under the **Log On** tab of the service's properties has been assigned the **Modify** permission for the folder.

### b. If EventLog Analyzer is installed in a server OS:

1. Remove the **Authenticated Users** permission for the folders listed below from the product's installation directory. Refer to the Appendix for step-by-step instructions.

   1. <product home>\bin
   2. <product home>\lib
   3. <product home>\tools
   4. <product home>\..\elasticsearch

2. Assign the **Modify** permission for the C:\ManageEngine\EventLog Analyzer folder to users who can start the product. Refer to the Appendix for step-by-step instructions.

3. If the product is installed as a service, make sure that the account configured under the **Log On** tab of the service's properties has been assigned the **Modify** permission for the folder.

## 2. Steps to perform if EventLog Analyzer is installed in C:\Program Files folder.

1. Remove the **Authenticated Users** permission for the folders listed below from the product's installation directory. Refer to the Appendix for step-by-step instructions.

   1. <product home>\bin
   2. <product home>\lib
   3. <product home>\tools
   4. <product home>\..\elasticsearch

2. Assign the **Modify** permission for the C:\Program Files\EventLog Analyzer folder to users who have can start the product. Refer to the Appendix for step-by-step instructions.

3. If the product is installed as a service, make sure that the account configured under the **Log On** tab of the service's properties has been assigned the **Modify** permission for the folder.

**Notes:**

- Microsoft recommends that software be installed in the Program Files directory. Based on your specific needs or organizational policies, you can choose a different location.
- The steps mentioned in this guide are applicable to all ManageEngine products installed in the C:\ManageEngine folder by default.

# Appendix

### Steps to disable inheritance

1. Right-click the **folder** and select **Properties.**
2. Go to the **Security** tab and click **Advanced.**
3. Click **Disable inheritance.**
4. Click **Convert inheritance permission to explicit permissions on this object.**

### Steps to remove Authenticated Users from ACL

1. Right-click the **folder** and select **Properties.**
2. Go to the **Security** tab and click **Edit.**
3. Select the **Authenticated Users** group and click **Remove.**
4. Click **Apply** and then **OK.**

### To assign modify permissions to users

1. Right-click the **folder** and select **Properties.**
2. Go to the **Security** tab and click **Edit.**
3. Click **Add.**
4. Enter the name of the user or group, and click **OK.**
5. Under the *Permission for Users* section, check the box under the **Allow** column for the **Modify** permission.
6. Click **Apply** and then **OK.**

ManageEngine
EventLog Analyzer

EventLog Analyzer is a web-based, real-time log management and IT compliance solution that combats network security attacks. With comprehensive log management capabilities, EventLog Analyzer helps organizations meet their diverse auditing needs. It also offers out-of-the-box compliance reports and alerts that meet stringent IT regulatory mandate requirements with ease.

$ Get Quote  Download