ManageEngine
EventLog Analyzer

Guide to secure your EventLog Analyzer installation

www.eventloganalyzer.com

Description

The EventLog Analyzer installation directory contains important files required for it to function effectively. This includes files that are used to start and stop the product, and the license file.

Unauthorized access to the installation directory could mean a user is tampering with the directory's contents, leading to security risks such as sensitive data exposure, and operational risks such as making the product unusable. This document discusses the measures to prevent unauthorized users from accessing the EventLog Analyzer installation directory and modifying its contents.

Solution

For Windows OS

To overcome unauthorized access to the EventLog Analyzer installation directory for Windows Operating System, follow the steps below, based on the build versions of EventLog Analyzer.

1. For New EventLog Analyzer Installations, builds 12336 & above
2. For Existing EventLog Analyzer Installations, builds lower than 12336

1. For New EventLog Analyzer Installations, builds 12336 & above

For new installations of builds 12336 and above, only the following types of user accounts are automatically provided access to the installation directory:

- Local system account
- User account used during product installation
- Administrators group

This is done to ensure file security and integrity.

Important: If the product is installed as a service, ensure that the account configured under the **Log On** tab of the service's properties has been assigned Full Control permission for the installation directory.

2. For Existing EventLog Analyzer Installations lower than 12336

Unauthorized users can be prevented from accessing the EventLog Analyzer installation directory for builds lower than 12336 in two ways:

I. Run the setAppPermission.bat file

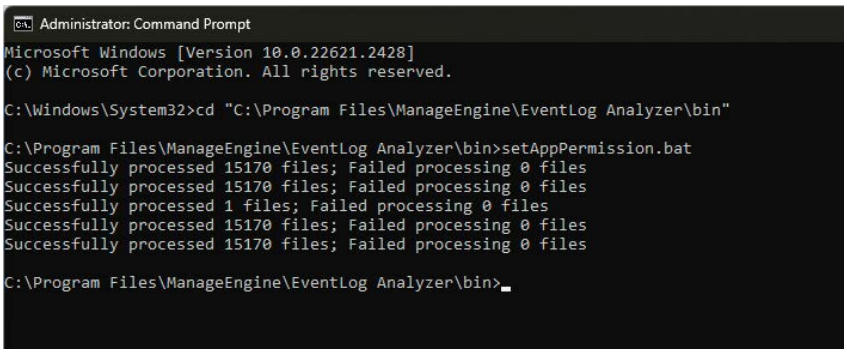
II. Modify required permissions manually

I. Run the setAppPermission.bat file

By this method, access to the installation directory is automatically restricted to only the necessary accounts. There are two ways to do this:

Option 1: Update to build 12336. Navigate to the "<**Installation Directory>/bin**" folder (by default **C:\Program Files\ManageEngine\EventLog Analyzer\bin**) and run the **setAppPermission.bat** file from the elevated Command Prompt.

Option 2: Download the zip file using this link. Extract the zip and move "setAppPermission.bat" to the "<Installation Directory>/bin" folder. Run the setAppPermission.bat file from the elevated command prompt. (See figure below).



II. Modify required permissions manually

To modify access permissions on the EventLog Analyzer installation directory for unnecessary groups/user accounts manually, follow the steps below:

1. Disable Inheritance for the **installation directory** (by default **C:\Program Files\ManageEngine\EventLog Analyzer**). Refer to the Appendix for step-by-step instructions.
2. Remove access permissions for all the unnecessary groups. Refer to the Appendix for step-by-step instructions.
3. Provide Full Control permissions to the Local System Account and the Administrators Group for the product's installation directory. Refer to the Appendix for step-by-step instructions.
4. Assign Full Control permission for the installation directory folder to users who can start or stop the product. Refer to the Appendix for step-by-step instructions.
5. If the product is installed as a service, ensure that the account configured under the **Log On** tab of the service's properties has been assigned Full Control permission for the installation directory.

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.

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.**
5. Click **Apply** and then **OK.**

Steps to remove unnecessary accounts from ACL

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

Steps to assign Full control permissions to Users/Groups

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 Full Control permission.

For Linux OS

To overcome unauthorized access to the EventLog Analyzer installation directory for Linux Operating System, follow the steps below, based on the build versions of EventLog Analyzer.

1. For New EventLog Analyzer Installations, builds 12445 & above
2. For Existing EventLog Analyzer Installations, builds lower than 12445

1. For New EventLog Analyzer Installations, builds 12445 & above

For new installations of builds 12445 and above, only the following types of user accounts are automatically provided access to the installation directory:

- Root user.
- User account used during product installation.

2. For Existing EventLog Analyzer Installations lower than 12445

Unauthorized users can be prevented from accessing the EventLog Analyzer installation directory for builds lower than 12445 by running the setAppPermission.sh file.

I. Run the setAppPermission.sh file

By this method, access to the installation directory is automatically restricted to only the necessary accounts. This can be done using either of the below options:

Option 1: Upgrade to build 12445 or above

- Update EventLog Analyzer to build 12445 or above.
- Navigate to the "<Installation Directory>/bin" folder (by default **/opt/ManageEngine/EventLog/bin**).
- Run the **setAppPermission.sh** file from the terminal.

Option 2 : Manual script execution

- Download the zip file using this link.
- Extract the zip and move "setAppPermission.sh" to the "<Installation Directory>/bin" folder.
- Run the setAppPermission.sh file from the terminal.

Setting permissions for the ES folder

To configure access permissions for the ES directory within the EventLog Analyzer installation folder, please follow the steps below based on your application build version:

1. For new EventLog Analyzer installations - builds 12.5.6.0 and above:

For new installations of builds 12.5.6.0 and above, the ES folder is automatically configured with the revised file permissions. Therefore, no manual action is required.

2. For existing EventLog Analyzer installations - builds below 12.5.6.0:

For existing installations of builds lower than 12.5.6.0, the access permissions for the ES folder can be set by executing the setESdirPermission.sh script using one of the following options:

Option 1: Upgrade to build 12.5.6.0 or above

- Upgrade EventLog Analyzer to build 12.5.6.0 or above.
- Navigate to the <Installation Directory>/ES/bin folder (default: /opt/ManageEngine/EventLog).
- Run the *setESdirPermission.sh* with elevated privileges using sudo in the terminal.

Option 2: Manual script execution

- Download the required ZIP file from here.
- Extract the content and copy the *setESdirPermission.sh* file to the <Installation Directory>/ES/bin folder.
- Run the *setESdirPermission.sh* with elevated privileges using **sudo** in the terminal.