

# Guide to secure your Log360 installation



ManageEngine   
Log360

If a user belongs to the **Authenticated Users** group, it's possible for them to tamper with the Log360 installation directory. To circumvent this and improve the security of your Log360 deployment, follow the steps in this document.

## Description

The Log360 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, Log360 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 Log360 as a service or application.

## Solution

To overcome this issue, follow the steps outlined below based on where Log360 is installed.

1. If Log360 is installed in C:\ManageEngine folder
2. If Log360 is installed in C:\Program Files folder

### 1. Steps to perform if Log360 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 Log360 is installed, the steps may vary.

- a) If Log360 is installed in a client OS
- b) If Log360 is installed in a server OS

#### a. If Log360 is installed in a client OS:

1. **Disable Inheritance** for the C:\ManageEngine\Log360 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\Log360 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 Log360 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\Log360 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 Log360 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\Log360 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**.

## Additional references

### EventLog Analyzer:

<https://download.manageengine.com/products/eventlog/secure-install-eventlog-analyzer.pdf>

### Office 365 manager plus:

<https://download.manageengine.com/office365-management-reporting/securing-o365-manager-plus-installation.pdf>



Log360, an integrated solution that combines ADAudit Plus, EventLog Analyzer, DataSecurity Plus, Exchange Reporter Plus, and O365 Manager Plus into a single console, is the one-stop solution for all log management and network security challenges. This solution offers real-time log collection, analysis, monitoring, correlation, and archiving capabilities that help protect confidential data, thwart internal security threats, and combat external attacks. Log360 comes with over 1,200 predefined reports and alert criteria to help enterprises meet their most pressing security, auditing, and compliance demands.

For more information about Log360, visit [manageengine.com/log-management](https://manageengine.com/log-management)

\$ Get Quote

↓ Download