Guide to secure your **Log360 installation**

ManageEngine
Log360

www.manageengine.com/log-management

Description

The Log360 installation directory contains important files required for the product to function properly, including the license file and files needed to start and stop the product. Unauthorized access to the installation directory could mean a user is tampering with the directory's contents, leading to security risks like sensitive data exposure, or even making the product unusable. This document discusses the measures to prevent unauthorized users from accessing the Log360 installation directory and modifying its contents.

Solution

For Product / For Product Installation

To overcome unauthorized access to the Log360 installation directory for Windows, follow the steps outlined below, based on the build versions of Log360 installed.

1. For new Log360 installations 5345 & above
2. For existing Log360 installations lower than 5345

1. For new Log360 installations 5345 & above

The following user accounts are automatically provided access to the installation directory to ensures file security and integrity:

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

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 Log360 installations lower than 5345

Unauthorized users can be prevented from accessing the Log360 installation directory for builds lower than 5345 in two ways:

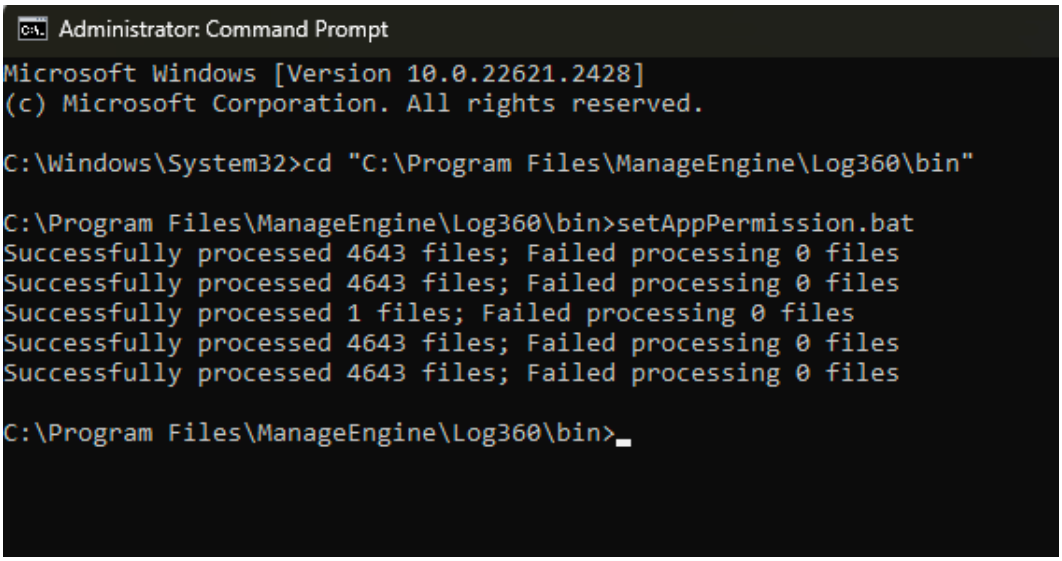
I. Run the **setAppPermission.bat** file
II. Modify required permissions manually

I. Run the SetPermission.bat file

With 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 5345. Navigate to the "**<Installation Directory>/bin**" folder (by default **C:\Program Files\ManageEngine\Log360\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.



II. Modify required permissions manually

To modify access permissions on the Log360 installation directory for unnecessary groups/user accounts manually, follow the steps outlined below.

1. Disable inheritance for the **installation directory** (by default **C:\Program Files\ManageEngine\Log360**). 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 following for the product's installation directory:
   i. Local system account
   ii. Administrators group
   Refer to the Appendix for step-by-step instructions.
4. Assign Full Control permission for the installation directory folder to users who can start/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 is 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 child products of Log360 installed inside **ManageEngine** folder (by default **C:\Program Files\ManageEngine**).

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.
6. Click **Apply** and then **OK.**

Securing search engine management (SEM) nodes

Follow the steps below to prevent unauthorized access to the SEM node installation directory, based on the installation of SEM node corresponding to build versions of Log360.

For Windows SEM nodes

New SEM node installation

The following user accounts are automatically granted access to the SEM node installation directory to ensure security and integrity:

- Local system account
- User account used for SEM node installation
- Administrators group

Existing SEM node installation

To restrict unauthorized access:

- **If the current build is 5538 or higher:**
  a. Navigate to **<SEM Node Installation Directory>/bin** and run **setESPermission.bat** from an elevated Command Prompt.

- **If the current build is lower than 5538**
  a. Download the **zip file** from here.
  b. Extract the **zip file** and move **setESPermission.bat** to *<SEM Node Installation Directory>/bin.*
  c. Run **setESPermission.bat** from an elevated Command Prompt.

For Linux SEM nodes

New SEM node installation

The following user accounts are automatically granted access to the SEM node installation directory:

- Root user
- User account used for SEM node installation

Existing SEM node installation

To restrict unauthorized access:

- I**f the current build is 5538 or higher:**
  a. Navigate to **<SEM Node Installation Directory>/bin** and run **setESPermission.sh** from an elevated terminal.

- **If the current build is lower than 5538**
  a. Download the **zip file** from here.
  b. Extract the **zip file** and move **setESPermission.sh** to *<SEM Node Installation Directory>/bin.*
  c. Run **setESPermission.sh** from an elevated terminal.

This ensures the security of the SEM node installation directory across all supported operating systems.

ManageEngine
Log360

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus

Exchange Reporter Plus | M365 Manager Plus

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, an analytical Incident Workbench, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote Download