

ManageEngine[®]
AD360

Guide to secure your AD360 installation

Description

The AD360 installation directory contains important files required for it to function properly, including files that are used to start and stop the product, files containing database configuration information, 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 like sensitive data exposure, or even making the product unusable. This document discusses the measures to prevent unauthorized users from accessing the AD360 installation directory and modifying its contents.

For new AD360 installations

For new installations of builds 4319 and above, only the following types of user accounts are automatically provided access to the installation directory to ensure file security and integrity:

- Local system account
- User account used during product installation Domain
- Admins group
- 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.

For existing AD360 instances

Unauthorized users can be prevented from accessing the AD360 installation directory for builds lower than 4319 in two ways:

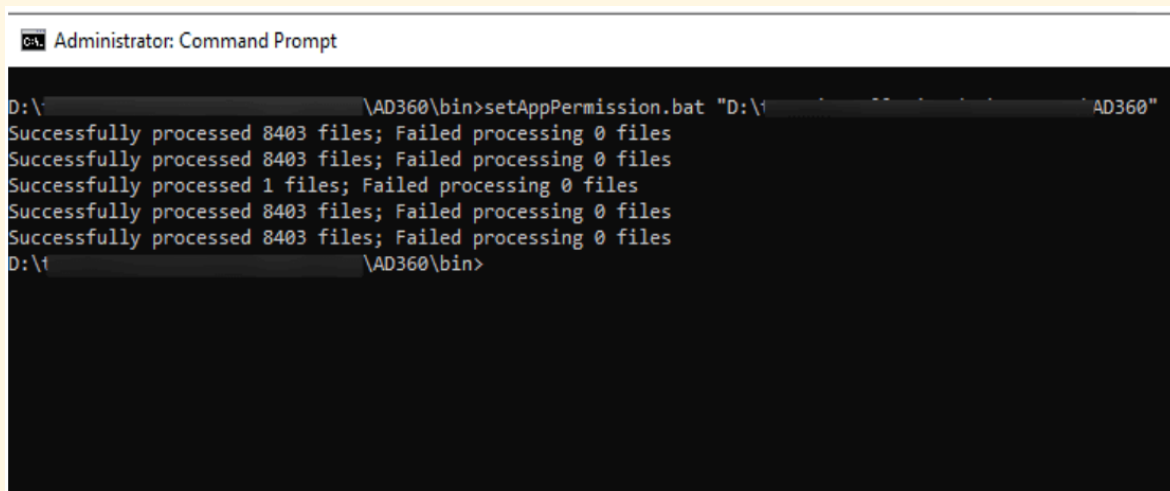
1. [Run the SetPermission.bat file](#)
2. [Remove unnecessary permissions manually](#)

I. Run the SetPermission.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 [4319 or higher](#). Open Command Prompt as an administrator and navigate to the *<installation directory>/bin folder* (by default *C:\Program Files\ManageEngine\AD360\bin*). Run the *SetPermission.bat* file.

Option 2: Download the file using this [link](#) and move it to the *<installation directory>/bin* folder. Open Command Prompt as an administrator and navigate to the *<installation directory>/bin* folder (by default *C:\Program Files\ManageEngine\AD360\bin*). Run the *SetPermission.bat* file.



```
Administrator: Command Prompt
D:\AD360\bin>setAppPermission.bat "D:\AD360\bin"
Successfully processed 8403 files; Failed processing 0 files
Successfully processed 8403 files; Failed processing 0 files
Successfully processed 1 files; Failed processing 0 files
Successfully processed 8403 files; Failed processing 0 files
Successfully processed 8403 files; Failed processing 0 files
D:\AD360\bin>
```

II. Modify required permissions manually

To manually remove access permissions for unnecessary groups, such as Authenticated Users and Domain Users, follow the steps outlined below.

1. Disable Inheritance for the **installation directory** (by default *C:\Program Files\ManageEngine\AD360*). 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. Domain Admins group
 - iii. Administrators group

Refer to the [Appendix](#) for step-by-step instructions.

4. Assign the Full Control permission for the installation directory 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, ensure that the account configured under the Log On tab of the service's properties has been assigned the Full Control 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.

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 **Apply** and **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 **OK**.

To assign full control 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, in the *Allow column*, check the box to allow **Full Control** permission.
6. Click **Apply** and **OK**.

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus
Exchange Reporter Plus | RecoveryManager Plus

ManageEngine AD360

ManageEngine AD360 is a unified identity and access management (IAM) solution that helps manage identities, secure access, and ensure compliance. It comes with powerful capabilities like automated identity life cycle management, access certification, risk assessment, secure single sign-on, adaptive MFA, approval-based workflows, UBA-driven identity threat protection and historical audit reports of AD, Exchange Server and Microsoft 365. AD360's intuitive interface and powerful capabilities make it the ideal solution for your IAM needs, including fostering a Zero Trust environment. For more information, please visit www.manageengine.com/active-directory-360/.

\$ Get Quote

↓ Download