ManageEngine
ADManager Plus

Guide to **enhance the protection** for ADManager Plus installation

www.admanagerplus.com

This document provides the steps needed to improve the security for your ADManager Plus instance.

Issue:

ADManager Plus bin folder can be tampered with by a user with a malicious intent, if the user belongs to the Authenticated Users group.

Description: By default, ADManager Plus will be installed in **C:\ManageEngine** folder. This will grant even non-admin users belonging to the **Authenticated Users** group, **Full Control** permission over the files in the bin directory. So, any domain user can access the folder, and start or stop the product

Removing **Authenticated Users** from ACL will not help since non-admin users will not be able to start ADManager Plus, as a service or application, due to lack of privileges.

Solution:

There are two ways to tackle this problem. You can either manually modify the permission settings or use the SecureDeployment.exe file which will automatically modify the settings.

1. Using SecureDeployment.exe
2. Manually modifying permissions
    a. When ADManager Plus is installed in C:\ManageEngine folder
    b. When ADManager Plus is installed in C:\Program FIles folder

1. Using SecureDeployment.exe

Benefits

The **SecureDeployment.exe** file in the bin directory will automatically:

- Prevent users in **Authenticated Users** group from accessing the ADManager Plus installation folders.
- Assign **Full** permissions for the given account.
- Configure 'log-on as' account credentials if ADManager Plus is accessed as a service.

The **SecureDeployment.exe** file will ensure that the deployment environment is secured.

2. Manually modifying permissions

a. Steps to perform if ADManager Plus is installed in C:\ManageEngine folder

i. If ADManager Plus is installed in a client OS

ii. If ADManager Plus is installed in a server OS

By default, the client OS C: directory has Authenticated Users with Modify permission for subfolders. However, C: directory in the server OS does not have Authenticated Users in the ACL.

i) If ADManager Plus is installed in a client OS

To allow users with less privileges to start or stop ADManager Plus on the client OS, follow the steps:

1. Disable Inheritance for the C:\ManageEngine\ADManager Plus folder.
2. Remove **Authenticated Users** from the ACL.
3. Remove **Authenticated Users** permission for these folders from the product's installation folder: bin\licenses, lib\licenses, temp, webapps\adsm\temp
4. Assign **Modify** permission to the C:\ManageEngine\ADManager Plus folder for users who have the responsibility of starting the product.
   If the product is installed as a service with 'log-on as' account, ensure this account has the **modify** permission.

ii) If ADManager Plus is installed in a server OS

1. Remove **Authenticated Users** permission for these folders from the product's installation folder: bin\licenses, lib\licenses, temp, webapps\adsm\temp
2. Assign **Modify** permission to the C:\ManageEngine\ADManager Plus folder for users who have the responsibility of starting the product.
   If the product is installed as a service with 'log-on as' account, ensure this account has the **modify** permission.

Note: The steps mentioned in both the above cases hold good for any location of your choice besides C:\ManageEngine.

b. Steps to perform if ADManager Plus is installed in C:\Program Files folder

1. Remove **Authenticated Users** permission for these folders from the product's installation folder: bin\licenses, lib\licenses, temp, webapps\adsm\temp
2. Assign **Modify** permission to the C:\Program Files\ADManager Plus folder for users who have the responsibility of starting the product.
   If the product is installed as a service with 'log-on as' account, ensure this account has the **modify** permission.

Note:

- Microsoft recommends that any software should 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 which have 'C:\ManageEngine' as the default installation location.