ManageEngine
ADSelfService Plus

Guide to secure your ADSelfService Plus installation

www.adselfserviceplus.com

Description

The ADSelfService Plus 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 ADSelfService Plus installation directory and modifying its contents.

For new ADSelfService Plus installations

For new installations of builds 6304 and above, only the following types of 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
- 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 ADSelfService Plus instances

Unauthorized users can be prevented from accessing the ADSelfService Plus installation directory for builds lower than 6304 in two ways:

i. Run the **SetPermission.bat** file

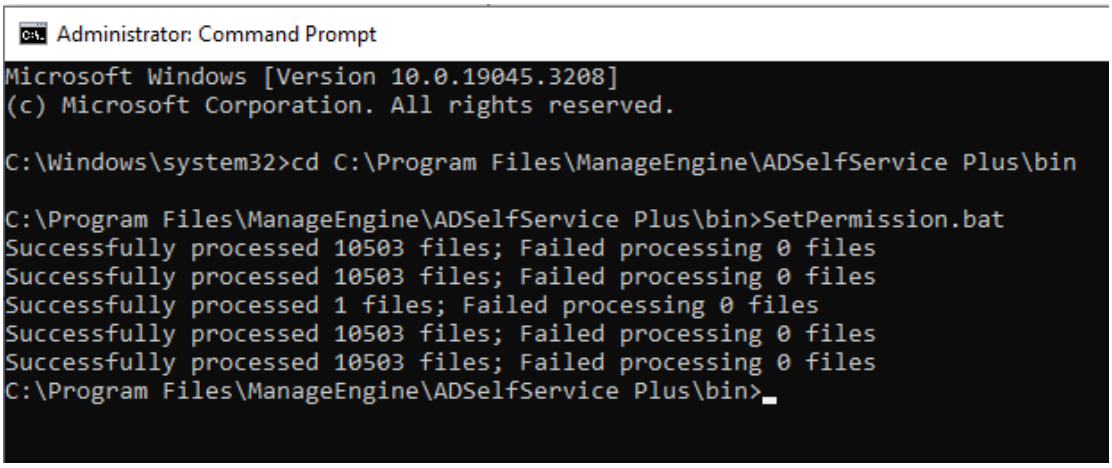
ii. Remove unnecessary permissions manually

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 6304. Navigate to the ***<installation directory>/bin*** folder (by default ***C:\Program Files\ManageEngine\ADSelfService Plus\bin***) and run the ***SetPermission.bat*** file from the elevated Command Prompt.

Option 2: Download the file using this link and move it to the ***<installation directory>/bin*** folder. Run the ***SetPermission.bat*** file from the elevated Command Prompt.



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\ADSelfService Plus***). 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

AD360 | Log360 | ADManager Plus | ADAudit Plus | RecoveryManager Plus | M365 Manager Plus

ManageEngine
ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement, and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets, and empowers remote workforces.
For more information about ADSelfService Plus, visit www.manageengine.com/products/self-service-password.

$ Get Quote | Download | Support