

Guide to secure your Cloud Security Plus installation



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

Description

The Cloud Security 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, Cloud Security Plus 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 Cloud Security Plus as a service or application.

Solution

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

1. If Cloud Security Plus is installed in C:\ManageEngine folder
2. If Cloud Security Plus is installed in C:\Program Files folder

1. Steps to perform if Cloud Security Plus 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 Cloud Security Plus is installed, the steps may vary.

- a) If Cloud Security Plus is installed in a client OS
- b) If Cloud Security Plus is installed in a server OS

a. If Cloud Security Plus is installed in a client OS:

1. **Disable Inheritance** for the C:\ManageEngine\Cloud Security Plus 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.
 - i. bin\licenses
 - ii. temp
 - iii. webapps\spmp
 - iv. ES\temp
 - v. lib\license

4. Assign the **Modify** permission for the C:\ManageEngine\Cloud Security Plus 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 Cloud Security Plus 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.
 - i. bin\licenses
 - ii. temp
 - iii. webapps\spmp
 - iv. ES\temp
 - v. lib\license
2. Assign the **Modify** permission for the C:\ManageEngine\Cloud Security Plus 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 Cloud Security Plus 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.
 - i. bin\licenses
 - ii. temp
 - iii. webapps\spmp
 - iv. ES\temp
 - v. lib\license
2. Assign the **Modify** permission for the C:\Program Files\Cloud Security Plus 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**.

The easy deployment, adaptive scalability, and economical costs of cloud platforms have many organizations adopting it. However, meeting compliance needs and growing security concerns of data loss and unauthorized access, hinders the tapping of the platform's full potential. Cloud Security Plus is your silver lining, as it combats these security concerns. It gives complete visibility into AWS, Salseforce, Google Cloud Platform, and Microsoft Azure cloud infrastructures. The comprehensive reports, easy search mechanism, and customizable alert profiles enable you to track, analyze, and react to events happening in your cloud environments