ManageEngine
Cloud Security Plus

Guide to secure your Cloud Security Plus installation

www.cloudsecurityplus.com

Description

The Cloud Security Plus 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 Cloud Security Plus installation directory and modifying its contents.

Solution

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

- For new Cloud Security Plus installations 4201 & above
- For existing Cloud Security Plus Installations lower than 4201

1. For new Cloud Security Plus installations 4201 & above

The following 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
- 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 Cloud Security Plus Installations lower than 4201

Unauthorized users can be prevented from accessing the Cloud Security Plus installation directory for builds lower than 4201 in two ways:

i. Run the setPermission.bat file

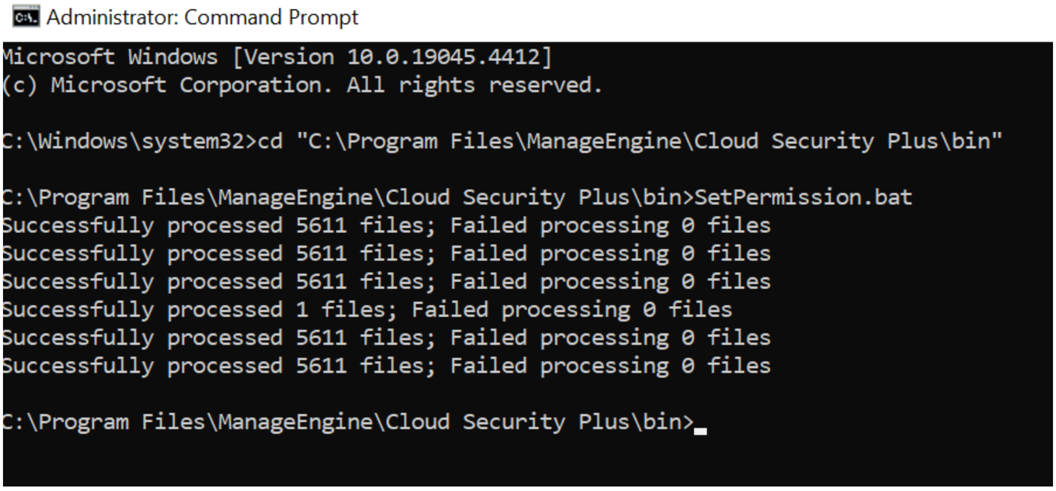
ii. Modify required permissions manually

i. Run the setPermissions.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 4200. Navigate to the "**<Installation Directory>/bin**" folder(by default **C:\Program Files\ManageEngine\Cloud Security Plus\bin)** and run the **SetPermission.bat** file from the elevated Command Prompt.

Option 2: Download the zip file using this link. Extract the zip and move "**SetPermission.bat**" to the "**<Installation Directory>/bin**" folder and run the same from the elevated Command Prompt.



Administrator: Command Prompt

```
icrosoft Windows [Version 10.0.19045.4412]
(c) Microsoft Corporation. All rights reserved.

:\Windows\system32>cd "C:\Program Files\ManageEngine\Cloud Security Plus\bin"

:\Program Files\ManageEngine\Cloud Security Plus\bin>SetPermission.bat
uccessfully processed 5611 files; Failed processing 0 files
uccessfully processed 5611 files; Failed processing 0 files
uccessfully processed 5611 files; Failed processing 0 files
uccessfully processed 1 files; Failed processing 0 files
uccessfully processed 5611 files; Failed processing 0 files
uccessfully processed 5611 files; Failed processing 0 files

:\Program Files\ManageEngine\Cloud Security Plus\bin>_
```

ii. Modify required permissions manually

To modify access permissions on the Cloud Security Plus installation directory for unnecessary groups/ user accounts manually, follow the steps below:

1. Disable Inheritance for the installation directory (by default **C:\Program Files\ManageEngine\** Cloud Security 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 Local System Account and the Administrators Group for the product's installation directory. Refer to the Appendix for step-by-step instructions.

4. Assign Full Control permission for the installation directory folder to users who can start or 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 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 **Change Permissions** and 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.**