ManageEngine
M365 Security Plus

Guide to secure your M365 Security Plus installation

www.microsoft365securityplus.com

Description

The M365 Security Plus 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. Unauthorized access to the installation directory could indicate a user is tampering with the directory's contents, which could result in potential security threats such as confidential information disclosure or rendering the product inoperable. This document discusses the measures to prevent unauthorized users from accessing the M365 Security Plus installation directory and modifying its contents.

For new M365 Security Plus installations

For new installations of builds 4538 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.

- To allow other users to access the installation directory, they have to be assigned **Full Control** permission for the same. Refer to the appendix for step-by-step instructions.

For existing M365 Security Plus instances

Unauthorized users can be prevented from accessing the M365 Security Plus installation directory for builds older than 4539 in two ways:

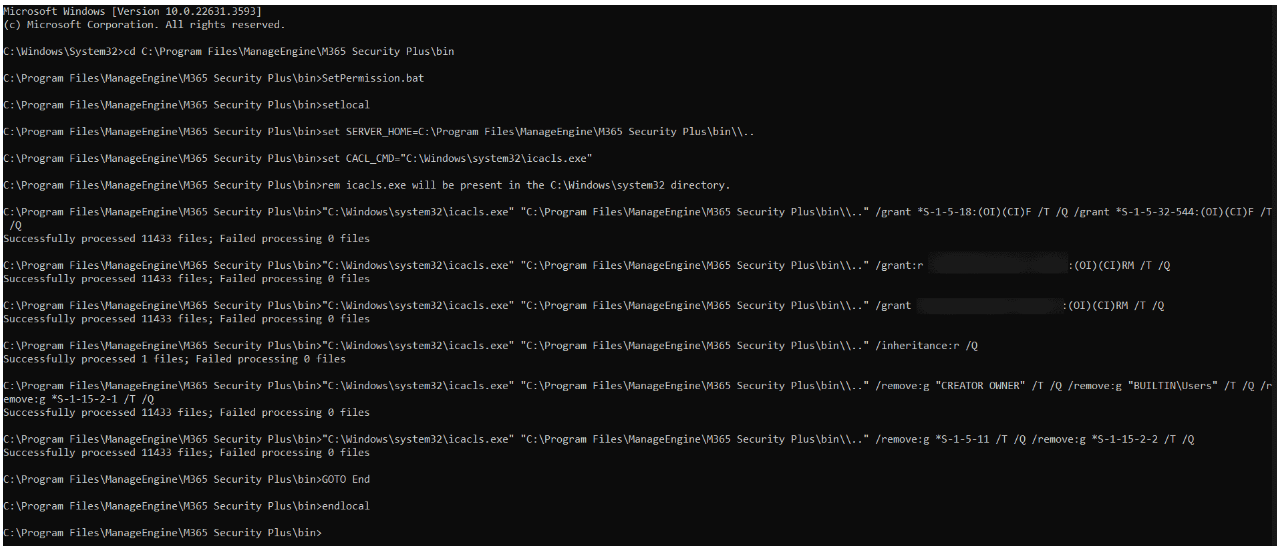
i. Run the SetPermission.bat file
ii. Remove unnecessary permissions manually

I. Run the SetPermission.bat file

By this method, access to the installation directory is automatically restricted to only the necessary accounts.

Update to build 4539 or higher using service packs.

Open **Command Prompt** as an administrator, and navigate to ***<installation directory>/bi***n folder (by default ***C:\Program Files\ManageEngine\M365 Security Plus\bin.)*** Run the **SetPermission.bat** file.



```
Microsoft Windows [Version 10.0.22631.3593]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\Program Files\ManageEngine\M365 Security Plus\bin

C:\Program Files\ManageEngine\M365 Security Plus\bin>SetPermission.bat

C:\Program Files\ManageEngine\M365 Security Plus\bin>setlocal

C:\Program Files\ManageEngine\M365 Security Plus\bin>set SERVER_HOME=C:\Program Files\ManageEngine\M365 Security Plus\bin\\..

C:\Program Files\ManageEngine\M365 Security Plus\bin>set CACL_CMD="C:\Windows\system32\icacls.exe"

C:\Program Files\ManageEngine\M365 Security Plus\bin>rem icacls.exe will be present in the C:\Windows\system32 directory.

C:\Program Files\ManageEngine\M365 Security Plus\bin>"C:\Windows\system32\icacls.exe" "C:\Program Files\ManageEngine\M365 Security Plus\bin\\.." /grant *S-1-5-18:(OI)(CI)F /T /Q /grant *S-1-5-32-544:(OI)(CI)F /T
 /Q
Successfully processed 11433 files; Failed processing 0 files

C:\Program Files\ManageEngine\M365 Security Plus\bin>"C:\Windows\system32\icacls.exe" "C:\Program Files\ManageEngine\M365 Security Plus\bin\\.." /grant:r [redacted]:(OI)(CI)RM /T /Q
Successfully processed 11433 files; Failed processing 0 files

C:\Program Files\ManageEngine\M365 Security Plus\bin>"C:\Windows\system32\icacls.exe" "C:\Program Files\ManageEngine\M365 Security Plus\bin\\.." /grant [redacted]:(OI)(CI)RM /T /Q
Successfully processed 11433 files; Failed processing 0 files

C:\Program Files\ManageEngine\M365 Security Plus\bin>"C:\Windows\system32\icacls.exe" "C:\Program Files\ManageEngine\M365 Security Plus\bin\\.." /inheritance:r /Q
Successfully processed 1 files; Failed processing 0 files

C:\Program Files\ManageEngine\M365 Security Plus\bin>"C:\Windows\system32\icacls.exe" "C:\Program Files\ManageEngine\M365 Security Plus\bin\\.." /remove:g "CREATOR OWNER" /T /Q /remove:g "BUILTIN\Users" /T /Q /r
emove:g *S-1-15-2-1 /T /Q
Successfully processed 11433 files; Failed processing 0 files

C:\Program Files\ManageEngine\M365 Security Plus\bin>"C:\Windows\system32\icacls.exe" "C:\Program Files\ManageEngine\M365 Security Plus\bin\\.." /remove:g *S-1-5-11 /T /Q /remove:g *S-1-15-2-2 /T /Q
Successfully processed 11433 files; Failed processing 0 files

C:\Program Files\ManageEngine\M365 Security Plus\bin>GOTO End

C:\Program Files\ManageEngine\M365 Security Plus\bin>endlocal

C:\Program Files\ManageEngine\M365 Security Plus\bin>
```

II. Modify required permissions manually

To 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\ M365 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 following accounts and groups for the product's installation directory:
   - Local system account
   - Domain Admins group
   - Administrators group
   - For users who can start the product

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 installation directory and select **Properties.**
2. Navigate 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 installation directory and select **Properties.**
2. Navigate 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 installation directory and select **Properties.**
2. Navigate to the **Security** tab and click **Edit.**
3. Click **Add.**
4. Enter the user or group name, 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.**