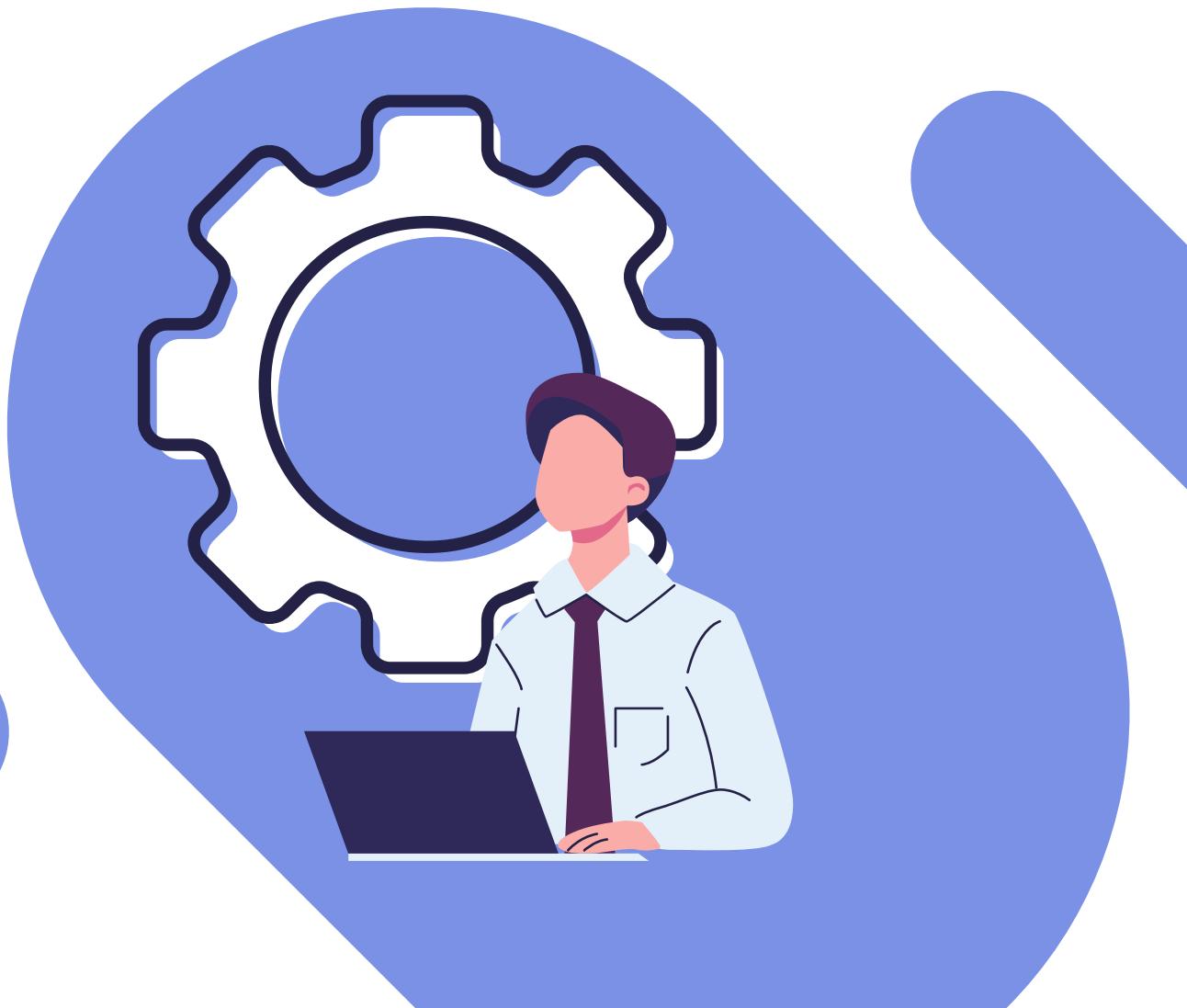


# Secure installation guide



## Description

The DataSecurity Plus installation directory contains crucial files that enable it to start and stop, such as files containing database configuration information and the license file. The installation directory should be secured to prevent tampering, which could pose security risks, such as data theft, sensitive data exposure, and operational risks, and potentially render the product dysfunctional and unusable. By default, DataSecurity Plus will be stored in the C:\Program Files\ManageEngine\DataSecurity Plus folder, which grants Full Control access to non-admin users in the Authenticated Users group for the files and folders located in the DataSecurity Plus installation directory and allows content modification. To prevent this from happening, implement the measures below based on your DataSecurity Plus installation build.

**Note:** Removing **Authenticated Users** from the access control list (ACL) won't help, as this will render them unable to start DataSecurity Plus as a service or application.

## Solution

To overcome unauthorized access to the DataSecurity Plus installation directory, follow the steps below, based on the build version.

1. For new DataSecurity Plus Installations, builds 6126 and above
2. For existing DataSecurity Plus Installations, builds lower than 6126

### 1. For new DataSecurity Plus installations, builds 6126 and above

- i For new installations of builds 6126 and above, only the following users and groups are provided with access to the installation directory to ensure file security and integrity:
  - Local system account
  - User account used for DataSecurity Plus installation
  - Administrators group
  - Domain Admins group
- ii Permissions are removed for the following groups and users:
  - **CREATOR OWNER**
  - **BUILTINUSERS**
  - **Authenticated users**
  - **ALL APPLICATION PACKAGES**
  - **ALL RESTRICTED APPLICATION PACKAGES**
- iii By default, inheritance will be disabled for the DataSecurity Plus folder.

**Note:** If the product is installed as a service, right-click **ManageEngine DataSecurity Plus** in the **Windows Services** application. Click **Properties > Logon** and make sure that the account configured has been assigned Full Control permission for the installation directory.

## 2. For existing DataSecurity Plus installations, lower than build 6126

**Note:** The below instructions are applicable only for users who have installed DataSecurity Plus before 6126 build and have upgraded to the latest version by applying service pack.

Unauthorized users can be prevented from accessing the DataSecurity Plus installation directory in two ways:

- i. Run the **setAppPermission.bat** file
- ii. Modify the required permissions manually

### i. Run the **setAppPermission.bat** file

With 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 6126 or above. Navigate to the **<Installation Directory>/bin** folder (by default, **C:\Program Files\ManageEngine\DataSecurity Plus\bin**) and run the **setAppPermission.bat** file using the elevated Command Prompt.

**Option 2:** Download the zip file from this [link](#). Extract the zip and move **setAppPermission.bat** to the **<Installation Directory>/bin** folder. Run the **setAppPermission.bat** file using the elevated Command Prompt.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22621.3447]
(c) Microsoft Corporation. All rights reserved.

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

C:\Program Files\ManageEngine\DataSecurity Plus\bin>setAppPermission.bat
Successfully processed 1 files; Failed processing 0 files
Successfully processed 15027 files; Failed processing 0 files
Successfully processed 15027 files; Failed processing 0 files

C:\Program Files\ManageEngine\DataSecurity Plus\bin>
C:\Program Files\ManageEngine\DataSecurity Plus\bin>
C:\Program Files\ManageEngine\DataSecurity Plus\bin>
C:\Program Files\ManageEngine\DataSecurity Plus\bin>
```

## ii. Modify the required permissions manually

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

1. Disable inheritance for the installation directory (by default, **C:\Program Files\ManageEngine\ DataSecurity Plus**). Refer to the [Appendix](#) for step-by-step instructions.
2. Remove access permissions for all 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. Provide Modify permissions to the Domain Admins group for the product's installation directory. Refer to the [Appendix](#) for step-by-step instructions.
5. Assign Full Control permission to users who can start or stop the product. Refer to the [Appendix](#) for step-by-step instructions.
6. If the product is installed as a service, right-click **ManageEngine DataSecurity Plus** in the **Windows Services** application. Click **Properties > Logon** and make sure that the account configured has been assigned Full Control permission for the installation directory.

**Note:** 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

### i 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 then **OK**.

### ii Steps to remove unnecessary accounts from the 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**.

### iii To assign Full Control or 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 User* section, check the box under the *allow* column for the **Full Control** or **Modify** permission.
6. Click **Apply** and then **OK**.

ManageEngine  
DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It also analyzes file storage and security permissions, deletes junk files, and detects file security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing PII, PCI, and ePHI. It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage.

\$ Get Quote

Download