

Administrative Permission: PDM & SolidWorks

Question:

Necessary permissions for installation and daily use of PDM and SolidWorks

PDM.....	2
SolidWorks	5
Antirus:	7
Antirus Daily Use:	7

Administrative Permission: PDM & SolidWorks

PDM

Users can face many different challenges if the PC does not meet minimum requirements.

First, it's important to understand the difference between installation and daily use. These are two completely different worlds and are not necessarily taken care of by the daily user, but an administrator who only helps with installation and setup.

First, PDM Installation based on a Windows 10 Workstation

3 absolutely essential things for proper installation.

1. Be Local Administrator.

One way to see if the conditions are met is in Computer Management to have the rights to add other users to the Administrators group

2. User Account Control must be turned off during installation.

UAC is a technology that Microsoft introduced with Microsoft Windows Vista and is a security level for your user accounts to prevent malicious software and malware from infecting the system files. UAC prevents unauthorized changes to the operating system, otherwise such changes could be made by applications, users, viruses or other forms of malware.

3. Anti virus must be turned off during installation. This is because AV often blocks proper registration of DLLs in the computer's registration database. This means that programs do not work properly, and users experience crashes, and troubleshooting often ends in a clean uninstall, which is a time-consuming process. DLLs from SolidWorks is digitally signed, but error-free registration is locally dependent on the Anti Virus program and its configuration.

NB! Applies to all types of installation and also to updates and graphics card drivers. Likewise, this applies to the creation of "Local Vault View" and Repair operations

These three things are mandatory. Whatever is said!

Turn off Antivirus, during installation, follow SolidWorks Recommendations.

The user (Local Administrator) used during installation must meet the following:

1. MUST have write / read rights to

HKEY_LOCAL_MACHINE\

This right also applies when performing a repair or upgrade. Also by "SNL" to set up license server.

Administrative Permission: PDM & SolidWorks

Daily use.

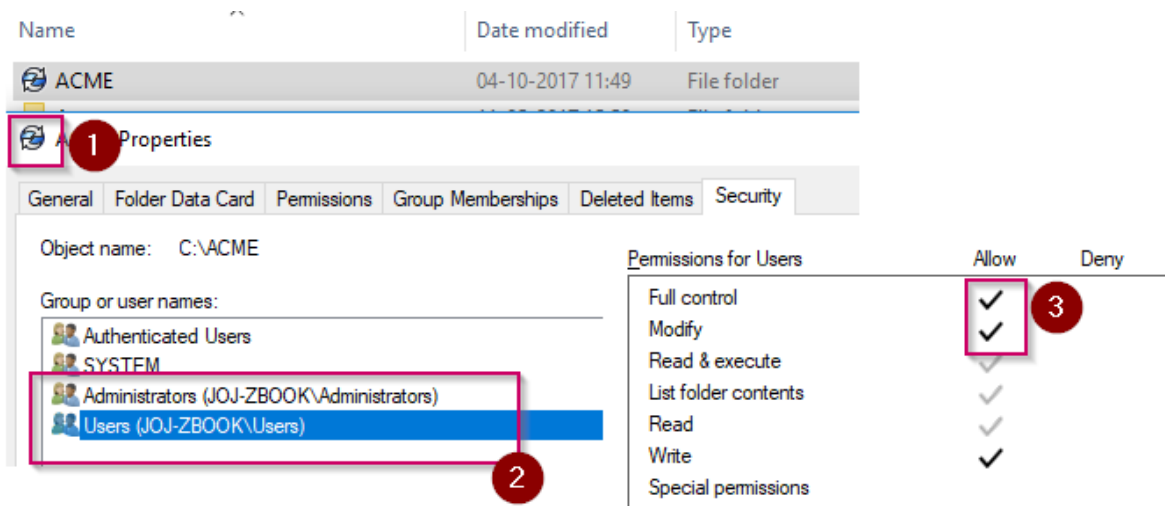
Basically follow SolidWorks and the solution S-053819

Which gives the following recommendations, which sound roughly like this:

SolidWorks PDM will work fine with the standard Microsoft user level (Administrator Power user) for a non roaming profile. Which means that there are no policies that change the rights of a normal user. Any deviation from standard setup needs extra attention.

1. The profile (user) logged in must have Read and Write Rights to Vault View (**Blueberry**) "

This is done by RMB on "**Blueberries**" and put "**Full control**" and "**Modify**"



Administrative Permission: PDM & SolidWorks

2. The profile logged in, **MUST have Read and Write rights to**

HKCU SolidWorks Enterprise PDM registry section –

HKEY_CURRENT_USER\Software\Solidworks\ Applications\PDMWorks Enterprise

3. The profile logged in, **MUST have Read to**

HKEY_LOCAL_MACHINE\SOFTWARE\SolidWorks\ Applications\PDMWorks Enterprise

4. The profile logged in, **MUST have Read and Write rights to the profile's "local Appdata Folder"**

In Start menu type **"%localappdata%\solidworks"** and test it is possible to create a text file

5. The profile logged in, **MUST have Read and Write rights to**

Profile's %temp% folder

In Start menu type **"%temp%"** and test it is possible to create a text file

Administrative Permission: PDM & SolidWorks

SolidWorks

3 absolutely essential things for proper installation.

1. Be Local Administrator.
One way to see if the conditions are met is in Computer Management to have the rights to add other users to the Administrators group
2. User Account Control must be turned off during installation.
3. Anti virus must be turned off

The user (Local Administrator) used during installation must meet the following:

1. The profile logged in, **MUST have Read and Write rights to** HKEY_LOCAL_MACHINE\

This right also applies when performing a **repair or upgrade**.
Also by "SNL" to set up license server.

Daily use

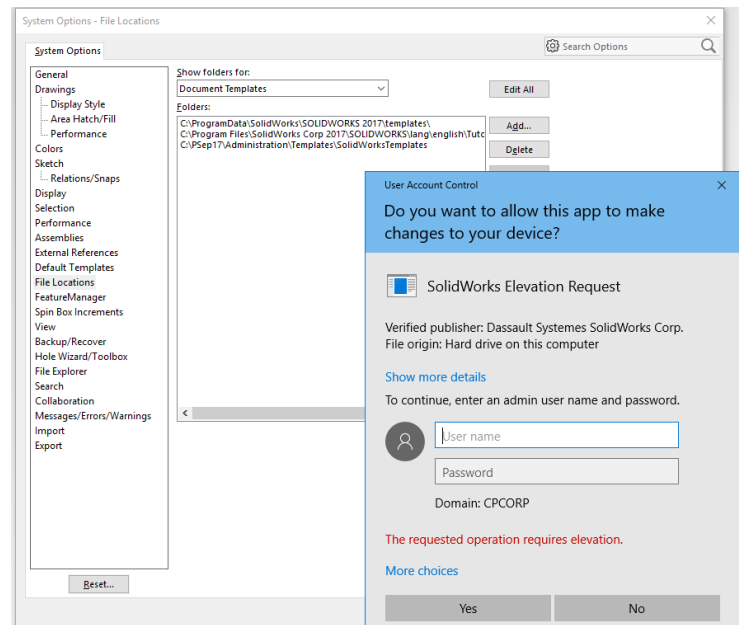
The user (Client) used for normal daily work:

1. The profile logged in, **MUST have Read and Write rights to** HKEY_CURRENT_USER,
If there is no write access to this key, it will not be possible to change the setup of solidworks, for example. paths in "File locations".
2. The profile logged in, **MUST have Read and Write rights to** HKEY_LOCAL_MACHINE\Software\SolidWorks\ and all subkeys.
If there is no write access to this key, it will not be possible to change the user interface setup.

Administrative Permission: PDM & SolidWorks

Example

Missing rights to set template path. If this happens, rights must be reviewed again.



Administrative Permission: PDM & SolidWorks

Antirus:

Antivirus blocks access to the mentioned keys in this document:

Therefore, SolidWorks always recommends disable Antivirus during installation, unless there is an exception in the antivirus program.

As with UAC, Antivirus can be re-activated after installation.

Antirus Daily Use:

There may be problems with different ANTI Virus systems during daily use.

One of the known problems is that SolidWorks is a very long time to launch because the installation folder is scanned, and SolidWorks, for example. takes very long time to load registry settings

There are different SPR's ec.. SPR-990482

That deals especially Kapersky og AVG
And SolidWorks Solution S-038577

One solution is to make exceptions in Anti Virus Settings.

In the anti-virus application, add scan exceptions to the SOLIDWORKS installation folder and add SLDWORKS.exe, swShellFileLauncher.exe, sldProcMon.exe, and sldworks_fs.exe to the "trusted applications list".