

UAC Virtualization

Basic Concepts

Certain program path under Windows 10 (in principle already since Windows VISTA) may not be written to with normal user rights. This restriction, that those files and path may only be altered with administrator rights, is part of the security concept of Windows and is called User Account Control (UAC).

Especially the following paths are involved

- C:\Windows
- C:\Program Files
- C:\Program Files (x86)

and maybe other system critical paths.

Moreover some file types may only be altered with administrator rights, thus among many more

- EXE
- VBA
- BAT

which are mostly executable files, which may contain malicious code in the worst. For information that is more detailed please look at the document of Mark Russinovich.

The Problem

By following this concept, it is not possible to take advantage of the established practice to save user data such as basic settings and options to the program path once the program does not run with administrator rights. The widely used workaround to save settings in the registry suffers from the same principle. It is even not enough to be logged in as an administrator but the program must be explicitly started with elevated rights by right mouse click and “run as administrator”.

For the program Metric it is now impossible to save basic settings like measure systems, calibration, exposure time or the connection of measure tables or motor drives – all save in Metric.opt within the program path – with one exception: It has to be started with elevated rights. This in turn would tear down the security wall of the system, if the normal user could start program with administrator rights.

To get rid of these problems, Microsoft established the technique called “UAC virtualization”. If a program does not have the rights to write or alter a file in the path of desire, a copy of this file is stored at a special location and this copy (or even not existing file in the destination directory) is virtually shown in the destination directory.

Example: You are logged in as „YouAsAUser“ with normal user rights and want to save the settings to Metric.opt. As you are not allowed to do that within „C:\Program files (x86)\Metric\Metric.opt“, Windows saves a copy of this file to

C:\Users\YouAsAUser\AppData\Local\VirtualStore\Program Files (x86)\Metric\Metric.opt

The UAC virtualization saves the file to a completely different location.

There is no difference if the administrator has altered your write permission to “C:\Program files (x86)\Metric”. Windows recognizes automatically the critical path and does the virtualization for you. As above mentioned the only exception is, when you explicitly start Metric with elevated rights, which is forbidden due to security reasons.

If you now go ahead and load your file from “C:\Program files (x86)\Metric\Metric.opt”, Windows loads this file from the virtual store.

For you as a single user this is extremely handsome. On one hand, you have the high security level by the UAC virtualization and on the other hand, you may keep your practice and save your files and settings where your program is installed.

If in this situation another user logs in as “YourColleague”, two things will happen:

1. Your colleague will read on the first start of Metric the originally installed file Metric.opt,
2. On saving, your colleague will create a new Metric.opt in his own VirtualStore, and this copy is only visible to him.

You now have three different Metric.opt: The one installed from the CD, your private copy and yours colleague private copy, although all of you will just see a single Metric.opt in the application path. The only difference will be presumably the size and the creation time.

You now have the advantage, that your colleague may not alter your settings. However, if some basic settings like calibration have to be changed, this has to be done for all workers separately, which may be a lot of work, if many workers do their jobs on this machine.

If in your case this UAC virtualization is a problem, you may work around as follows.

The solution UAC File Exclude

As mentioned above there are file types, which are not virtualized by the UAC. If you add OPT to the list of this file types, the virtualization for Metric.opt (and all other files with the extension opt) will no longer take place.

A simple user now must not change the settings any more. Only the administrator, who explicitly starts Metric with elevated rights, may alter the settings. If this is the desired solution in your case, you are done. The file “uac opt exclusion.reg” contains the registry entry, which does the job for you and adds the file extension OPT to the excluded extensions.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\luaflt  
\Parameters]  
"ExcludedExtensionsAdd"=hex(7):6f,00,70,00,74,00,00,00,00,00
```

Those hexadecimal characters code for the string “OPT” in DBCS format and an empty string. By double clicking this file and accepting all UAC questions this entry is made to the registry and a final reboot of the system lets the effects run on your system.

The extended solution “write permission”

If normal users should be allowed to change the Metric settings, they have to get write permission to the installation path of Metric (“C:\Program files (x86)\Metric”). In this case “alter/change” would be enough as saving a complete new set of settings in some different file is not necessary. The administrator may thus grant minimum rights and does not need to grant full access to the path.