

WINDOWS PERMISSIONS AND SECURITY

A description of problems often encountered while installing and running addon software with Microsoft Flight Simulator.

A troubleshooting guide

Table of Contents

Introduction	2
Scope	2
Terminology	2
Your Windows Login	2
What are permissions?	2
Problems associated with permissions issues	3
What is Ownership?	3
Trusted Software	3
Software Security Environment	3
Problem Resolution	4
Additional Drives and Partitions	4
Taking Ownership	5
Check/Change Ownership of a Drive, File or Folder in Windows 7 and Vista	5
Registry Permissions	11
Reference	15
Permissions Levels	15
Windows Account Type	15
Setting your Windows Account Type	15
User Account Control	17
UAC access in Windows 7	18
UAC access in Windows Vista.	20
UAC Access in Windows 8	21
Data Execution Prevention	22
Safe Mode	24
Starting Windows In Safe Mode	24

Introduction

Scope

The purpose of this publication is to try to help you troubleshoot problems you are encountering running addons in Flight Simulator. This includes installation problems and/or lack of functionality of the aircraft, avionics, utilities, or any other programs you have added to your Flight Simulator environment.

Since Microsoft released Windows XP, the security safeguards built into the operating system have become more and more complex, and in some cases, restrictive. Beginnings with Windows Vista, and going forward, the operating systems have incorporated a much more restrictive software environment in order to combat the increasing threats of hacking, viruses/Trojans, and spyware. It does this through control of object Permissions and Ownership that are linked to your Windows login account.

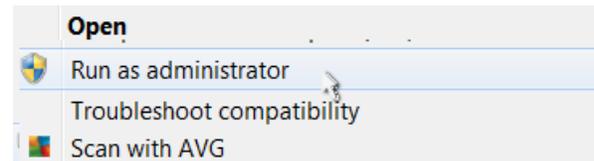
Terminology

Within this article, and in general, in the use of your computer, a number of terms come into play, such as *Windows Login*, *Permissions* and *Ownership*. A brief outline of these terms is in order.

Your Windows Login

A user account determines how you interact with your computer. For example, your account determines which apps, files, and folders you can use, the changes you can make to the PC, and your personal preferences, such as your Start screen layout, desktop background, or screen saver. See Windows Account Type on page 15 for more details.

Keep in mind that if your Windows Login Account has administrative level permissions, that does not mean that you automatically have full administrative rights. In many cases, you need to start programs, particularly installation programs, by right clicking on them and selecting *Run As Administrator*.



What are permissions?

Permissions are rules associated with objects on a computer or network, such as files and folders. They determine whether you can access an object and what you can do with it. For example, you might have access to a document on a different drive on a network. Even though you can read the document, you might not have permissions to make changes to it. System administrators and people with administrator accounts on computers can assign permissions to individual users or groups, according to the table of permissions levels on page 15.

PROBLEMS ASSOCIATED WITH PERMISSIONS ISSUES

The types of problems one may expect to encounter when permissions issues arise are:

- Problems with installation programs not being able to function without errors.
- Inability to write to files, such as text files, etc.
- Programs being unable to retrieve stored data on your system.
- "Access Denied" or "You need permission to perform this action" error messages from Windows when trying to use a program.
- General lack of functionality in the programs you use.

What is Ownership?

The owner of a file or folder is the user who has complete and full control over that file or folder in terms of being able to grant access to the resource, and have full control over the folder/file(s). Ownership of a file or folder may be taken by any user with administrator level privileges.

Trusted Software

When you load a Flight Simulator X add-on for the first time, the simulator should ask you if you trust the software *.dll or *.gau driver. If you do not accept the driver, or if the simulator does not ask you to accept the driver, the software may not work properly, and the simulator can become unstable.

To correct this problem, open the FSX.CFG file, which is usually located at

```
C:\Users\[username]\AppData\Roaming\Microsoft\FSX
```

and delete all references to the software be found under the [TRUSTED] section.

Next, you need to check a problematic registry setting that Windows uses for third party DLL trust policy selection. Check if the key:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing\State
```

is set to 0x63c00. This value is Microsoft's WinTrust policy selection flags, as described here. If that key is set to 0x40000, or any other value, this means "Allow only items in personal trust database", which clashes with the simulator's ability to allow manual authorization of unrecognized DLLs, telling it instead to never trust anything outside the user's personal trust. Unsetting this flag (putting it back to its default 0x23c00 value) returns all operations to normal and Flight Simulator X will once again be able to ask the user to designate addon DLL modules as 'Trusted' software.

Software Security Environment

Since Windows XP, Windows has incorporated more and more security schemes to help prevent malware, spyware and rogue programs from running on your system without knowledge. The problem is that, sometimes this results in a software environment that also restricts or blocks the operation of programs you do want to run.

In Windows Vista forward, by default, *User Account Control* (UAC) prevents certain actions even though you actually have an administrator account. See page 17 for more details.

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help protect against malicious code exploits. As is the case with UAC, this feature is not totally reliable and can work *overtime*, blocking the programs you want to run. See page 22 for more details.

Problem Resolution

Additional Drives and Partitions

Creating additional partitions on your drive to differentiate between data storage and actual programs, for example, can speed performance, but not necessarily since you are still using the same physical drive. However, it can also lead to problems with user permissions, directory/file ownership and file access.

If the drive is actually another physical drive, such as an external or backup hard drive, this can be very problematic, as this can lead to permissions and ownership issues and problems with Windows programs not having full access to your core Windows drivers. For this reason we strongly recommend that you never install Flight Simulator on an external or backup hard drive. Best results are obtained by running Flight Simulator on the same drive as your operating system. Running Flight Simulator on the same partition as well is generally accepted as being a good idea as well, as it decreases the probability of ownership and permissions issues.

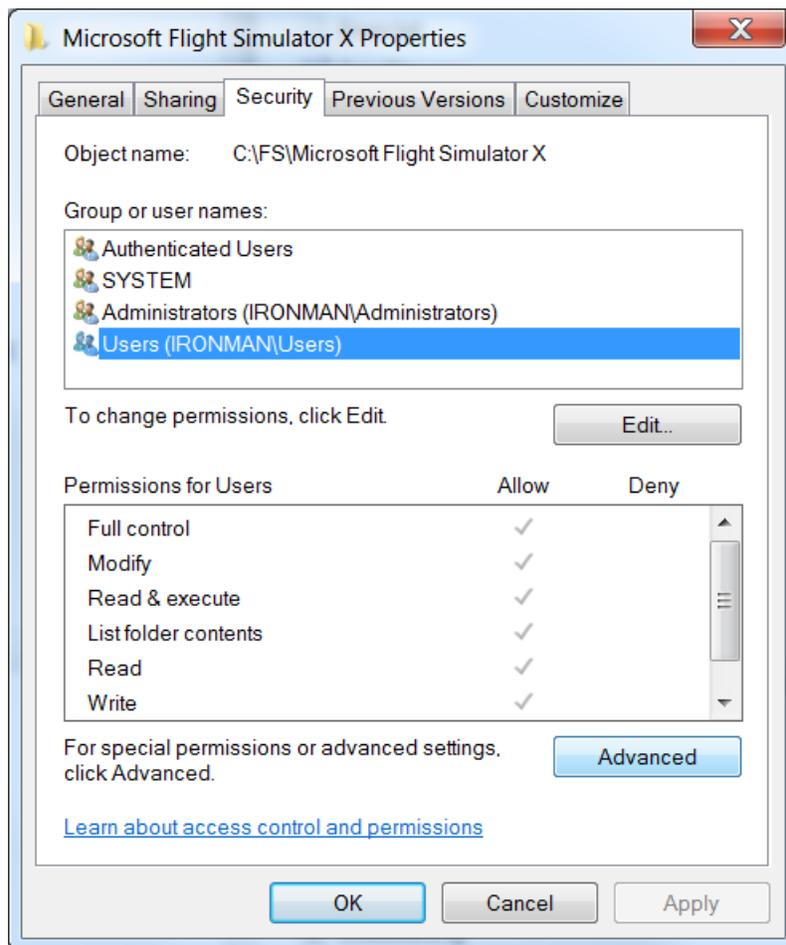
Taking Ownership

Whether you have installed Flight Simulator on a drive or partition different from your operating system 'C' drive, you need to have full control over the root folder where Flight Simulator resides. Also, you need to run installation programs and support utilities for your addons from a folder over which you have full control. Otherwise, lack of functionality, errors and installation problems can occur.

CHECK/CHANGE OWNERSHIP OF A DRIVE, FILE OR FOLDER IN WINDOWS 7 AND VISTA

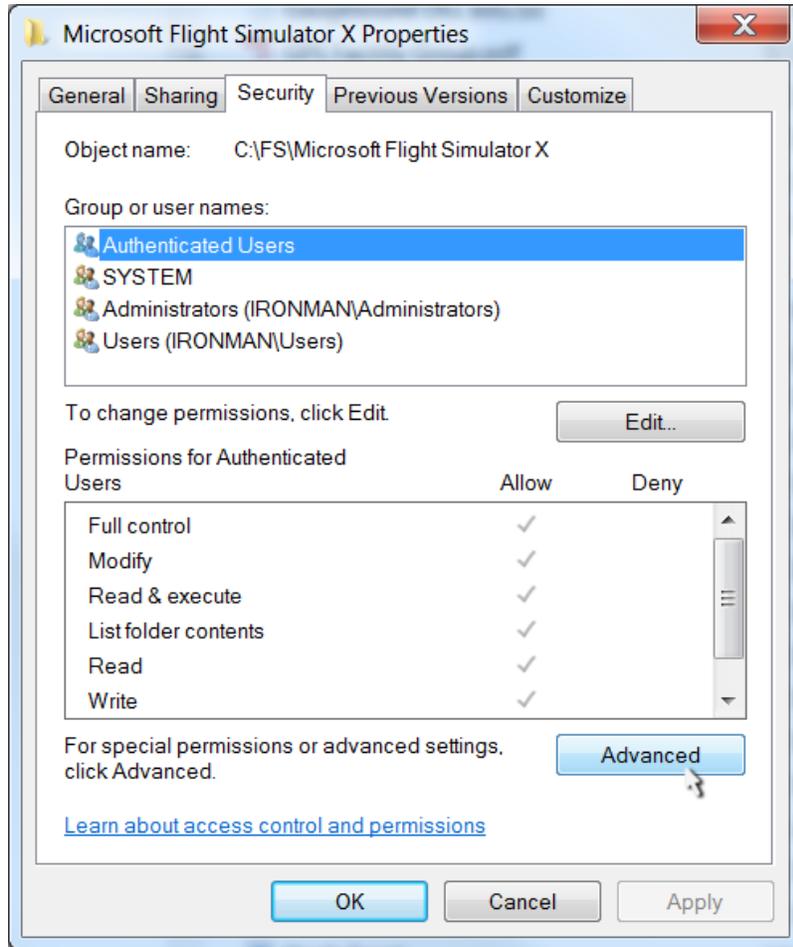
To check/change the ownership of a drive, file or folder, perform the following steps.

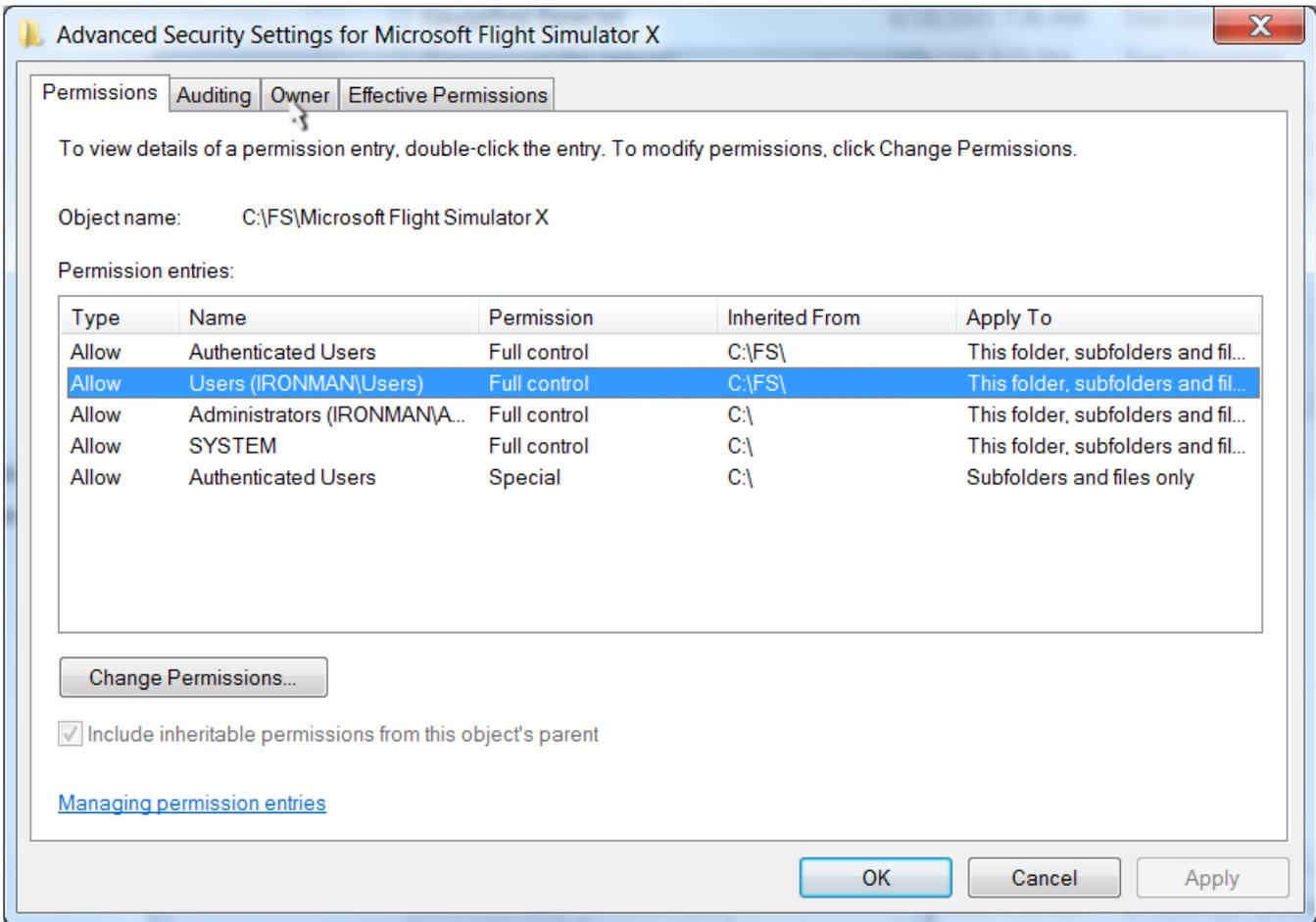
1. Navigate to the target drive, file or folder using Windows Explorer.
2. Right-click on the object and choose Properties.
3. Click the "Security" tab



See if your current user is listed in the "Group or user names" list. If not, your [Windows Login](#) account may not have a sufficient permissions level to read/change permissions and access on this computer.

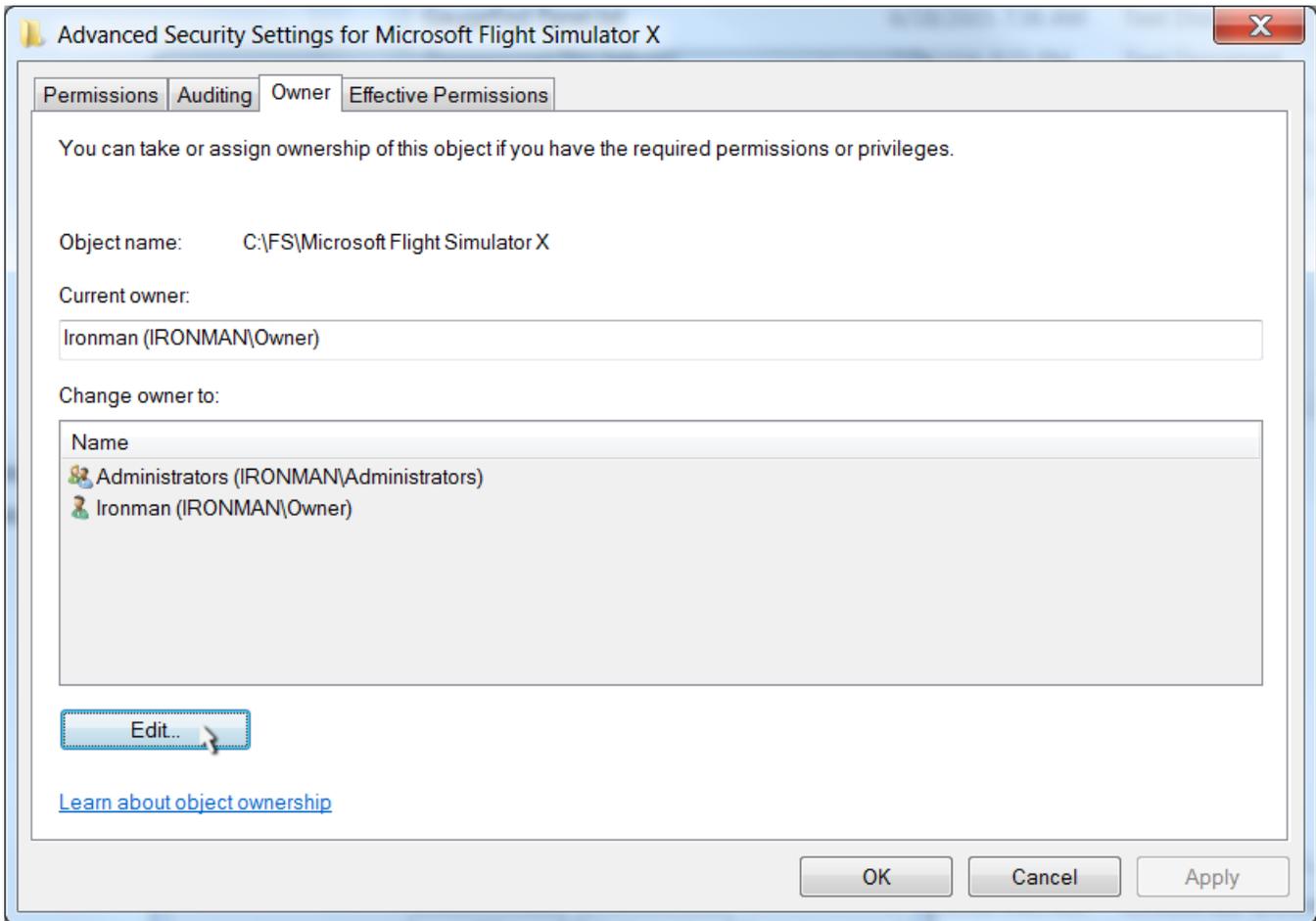
Click the *Advanced* button.



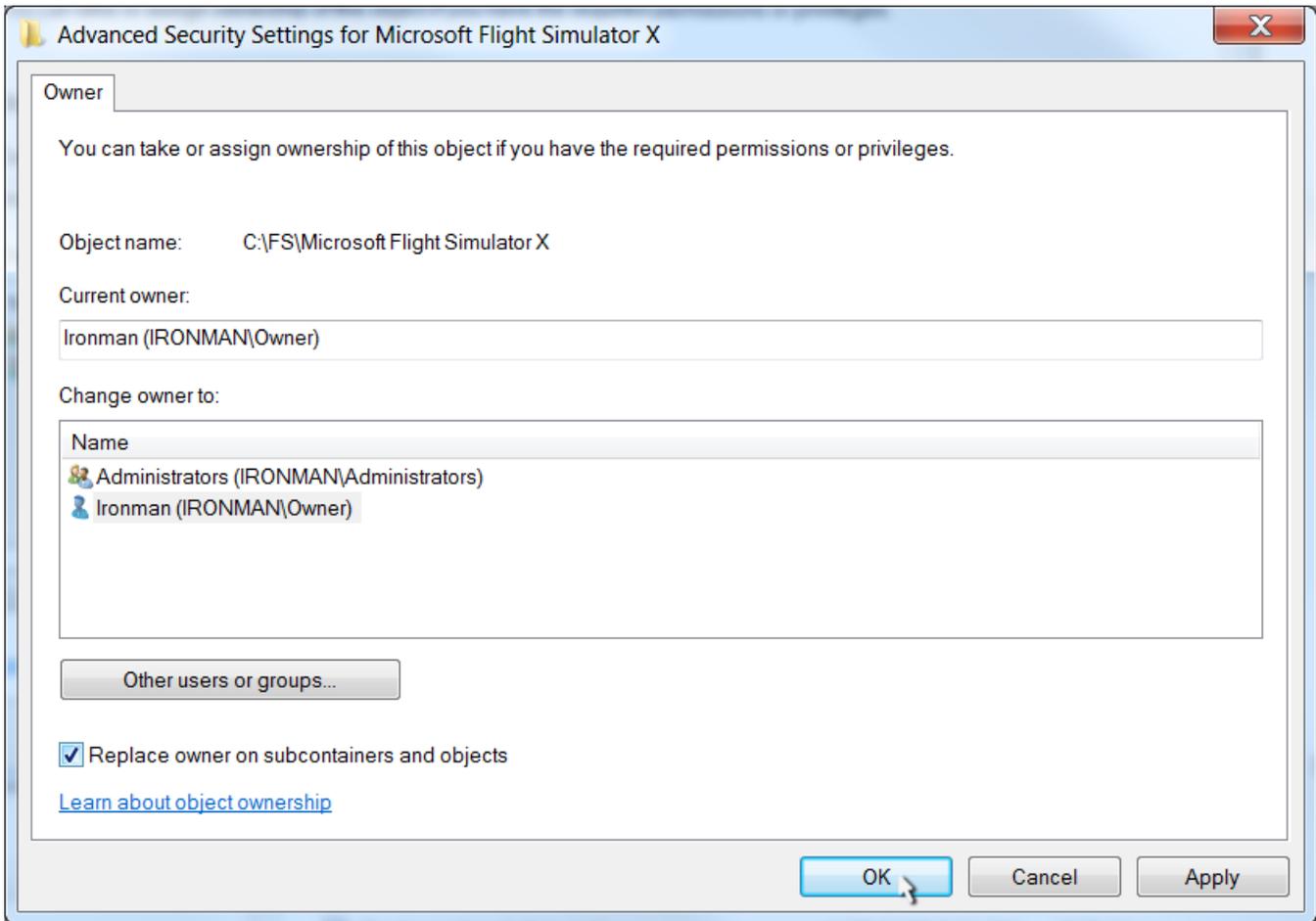


The Windows accounts on the computer will be listed, along with their access level. If your login account does not have "Full Control" specified, take ownership of the object as follows.

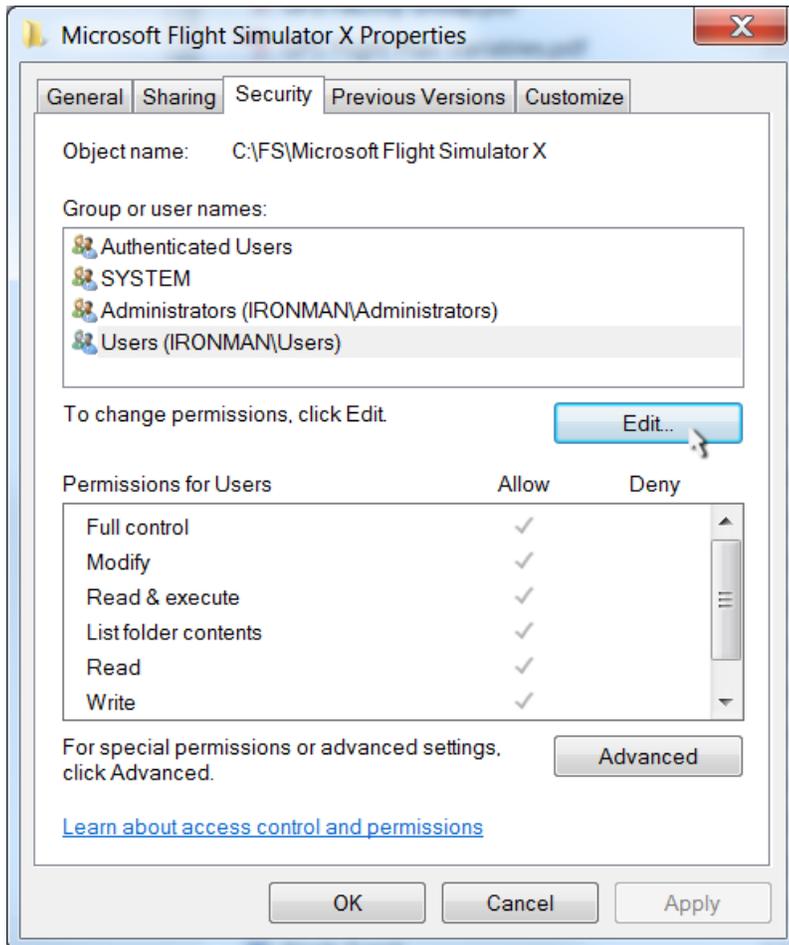
and then the *Owner* tab.



Press the *Edit* button.



Select your login account and press *OK*.



This will take you back to the Security Menu. Highlight your account name and press *Edit*. Select *Allow Full Control* on the popup menu.

To take ownership of a drive or a folder in Windows XP

To take ownership of a drive or folder, follow these steps:

1. Right-click the folder that you want to take ownership of, and then click Properties.
2. Click the Security tab, and then click OK on the Security message (if one appears).
3. Click Advanced, and then click the Owner tab.
4. In the Name list, click your user name, or click Administrator if you are logged in as Administrator, or click the Administrators group. If you want to take ownership of the contents of the folder, select the Replace owner on subcontainers and objects check box.
5. Click OK, and then click Yes when you receive the following message: *You do not have permission to read the contents of directory folder name. Do you want to replace the directory permissions with permissions granting you Full Control?* All permissions will be replaced if you click Yes.
6. Click OK, and then reapply the permissions and security settings that you want for the drive/folder and its contents.

Registry Permissions

One problem that can occur in the more recent operating system is restricted permissions in the system registry. This may manifest itself by problems installing programs, inability of an addon package to store and retrieve settings/data, or problems loading the addon software. Therefore, it is a good idea to know what your windows login's permissions level is in your registry. This can also help you running software other than Flight Simulator and its addons.

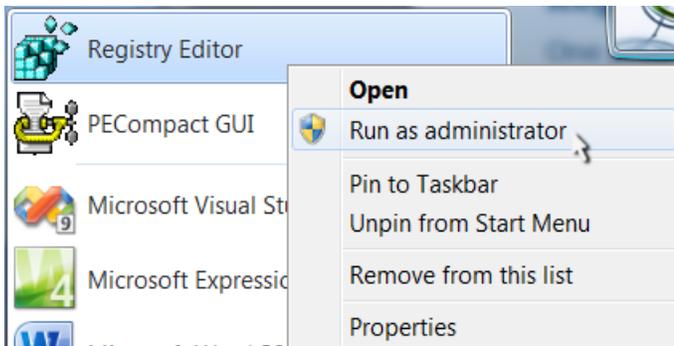
Most addon software will install any registry keys in the registry at:

HKEY_CURRENT_USER

HKEY_LOCAL_MACHINE

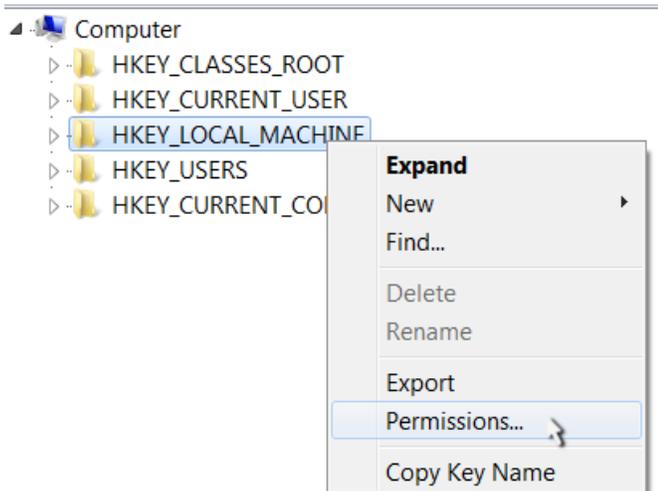
Programs commonly use this area of the registry to store and access data. You need to have full access to those keys. Depending on how Windows was setup, and what changes may have been made by any security software you have installed, your *Windows Login Account* may have restricted access to important areas of the registry that your programs need.

To check your registry permissions, and if necessary, change them.

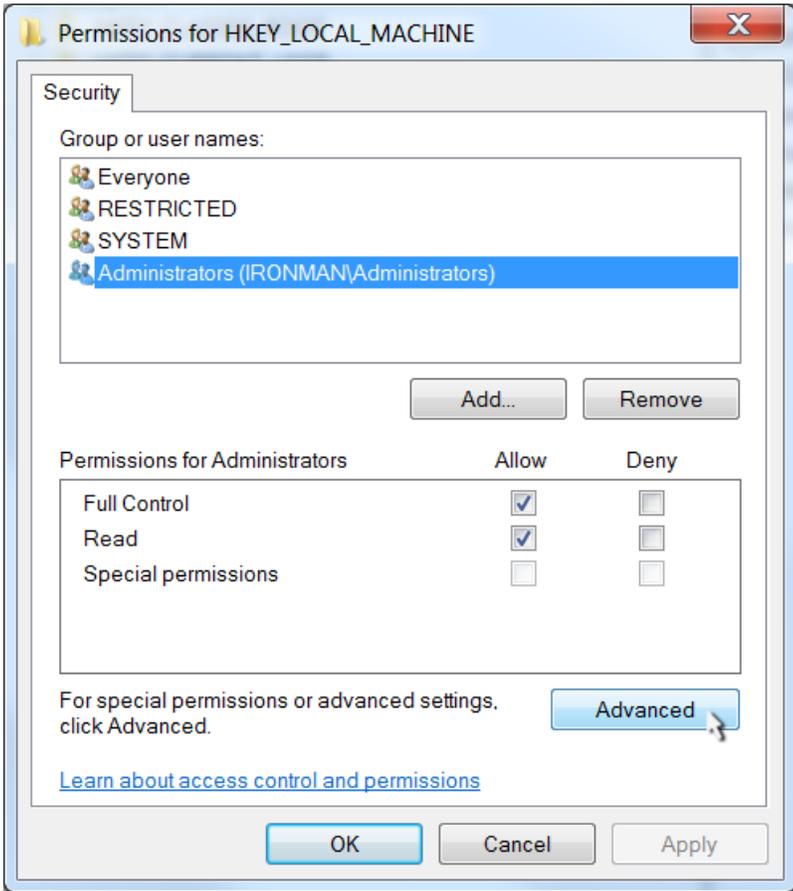


From your Windows Start menu, enter *regedit* in the search box. The program will appear in your available programs. Right click on it and select Run As Administrator.

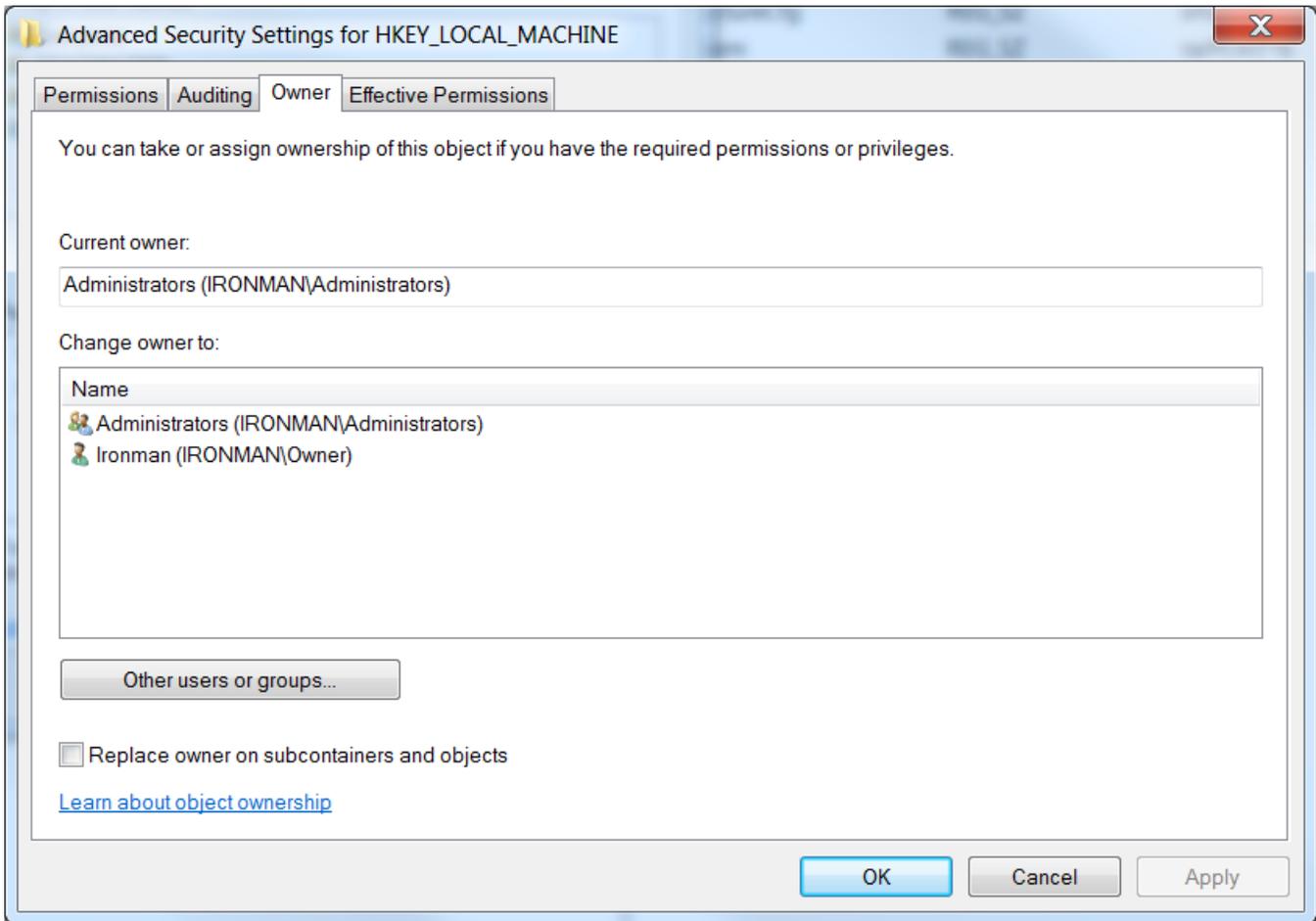
Changes can only be made to the registry permissions if you open the program with full administrative rights.



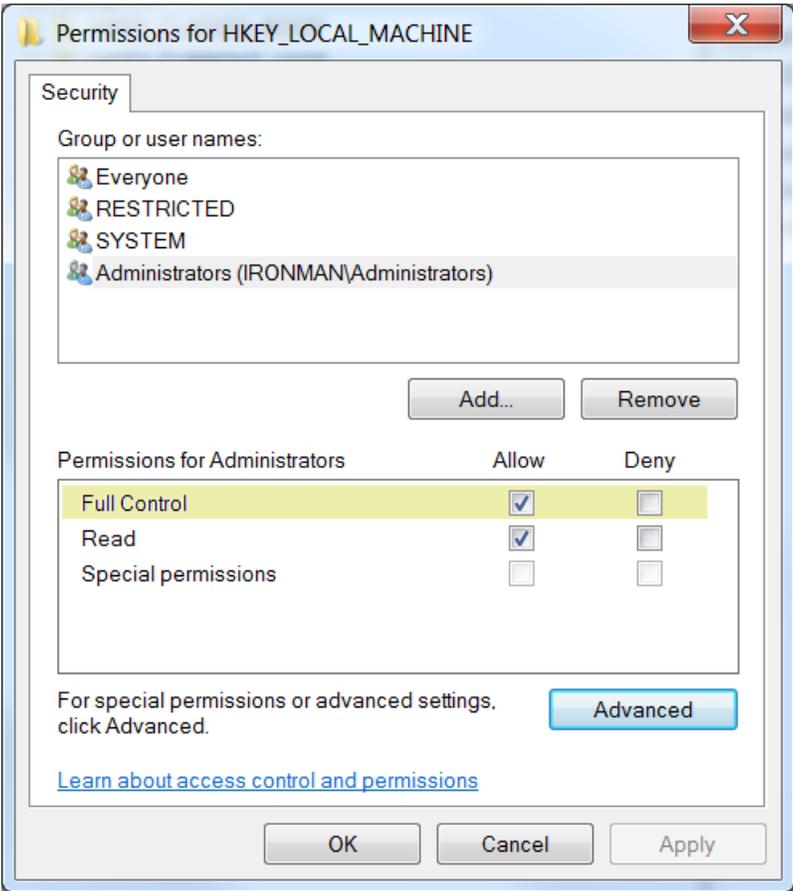
Right click the registry key and select *Permissions*.



Click the advanced button.



Go to the Owner tab and select your login account. Check the box Replace owner on subcontainers and objects. Click Apply. Then press OK.



This will take you back to the Permissions dialog box. Make sure your login account has *Full Control*.

If Windows will not allow you to make these changes, you may need to login to your computer in Safe Mode. See page 22 for more details.

Reference

Permissions Levels

Permission level	Description
Full control	Users can see the contents of a file or folder, change existing files and folders, create new files and folders, and run programs in a folder.
Modify	Users can change existing files and folders, but cannot create new ones.
Read and execute	Users can see the contents of existing files and folders and can run programs in a folder.
Read	Users can see the contents of a folder and open files and folders.
Write	Users can create new files and folders and make changes to existing files and folders.

Windows Account Type

The type of login account you are using can be critical to how you can access programs, and their functionality. There are three types of accounts. Each type gives you a different level of control over the PC:

1. *Administrator accounts* have full control over the system. They can install software programs and hardware drivers, and they can create and modify new users and groups. Additionally, they can reset passwords, set policies, and edit the Registry. The OS identifies tasks that require administrator permissions with a *Windows security icon*.
2. *Standard accounts* are permitted to log on to the computer, run programs, customize their accounts, and save files in their user folders. Users are restricted from making system-wide changes.

 *Windows Security Icon*

Keep in mind that an administrative account level does not necessarily give you access of all of the files and folders on your computer. Windows deliberately restricts access and rights to several folders and files on your system. These are called *Protected Folders*, and generally contain system information or data. Depending on how the computer was setup, this could include other folders, such as your Program Files and Program Files (x86) on 64 bit operating systems.

SETTING YOUR WINDOWS ACCOUNT TYPE

Once you have an account, you can customize it further by editing.

Windows Vista/Windows 7

 Sync Center

 User Accounts

 Windows Firewall

To edit an account, open Control Panel and select User Accounts

Control Panel Home

Manage your credentials

Create a password reset disk

Link online IDs

Configure advanced user
profile properties

Change my environment
variables

Make changes to your user account

[Change your password](#)

[Remove your password](#)

[Change your picture](#)

 [Change your account name](#)

 [Change your account type](#)



 [Manage another account](#)

 [Change User Account Control settings](#)

This takes you to the Manage Accounts window. Select *Change Your Account Type*.

Simply select the account type and press *Change Account Type*.

Select your new account type



My Account

Administrator

Password protected

You must assign another user on this computer to have an administrator account before you can change this user's account type. This ensures that there is always at least one user with a computer administrator account on this computer.

Standard user

Standard account users can use most software and change system settings that do not affect other users or the security of the computer.

Administrator

Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users.

We recommend that you protect every account with a strong password.

[Why is a standard account recommended?](#)

Change Account Type

Cancel

If you are logged in as a standard user, Windows will prompt you to authenticate your administrator account so that you won't need to log on with it. If you are unable to do so, your

login account has been set by the computer administrator, which in most cases is the *First User Account*. You may need to login using that account in order to perform this task.

When Windows first installs, it asks you for a user name and password, which it then uses to create your first account. This account joins the Administrators group, which has the highest set of privileges. From this account, you can create and manage all other user accounts. When one person is the sole user of a computer, this first account is sometimes the only one ever created.

If you accidentally deleted your Administrator Account, Windows 7 has a built-in Administrator account that has no password and is hidden by default. Like all other administrator accounts, it has full control of the system; for you to use it, however, it must be the only remaining administrator account, and you must start the computer in Safe Mode. You can find instructions on page 22.

Windows XP

You must be logged on as an administrator or a member of the Administrators group in order to complete this procedure. If your computer is connected to a network, network policy settings may also prevent you from completing this procedure.

1. Open User Accounts in Control Panel.
2. Click the user's account name.
3. Click Change the account type.
4. Click the type of account you want, and then click Change Account Type.

You must have a computer administrator account on the computer to change another user's account type.

User Account Control

User Account Control (UAC) was introduced with Microsoft's Windows Vista and is present in Windows 7 and Windows 8 as well. UAC is intended to improve the security by limiting application software to standard user privileges until an administrator authorizes an increase or elevation. With UAC on, only applications trusted by the user may receive administrative privileges, and malware should be kept from compromising the operating system. In other words, a user account may have administrator privileges assigned to it, but applications that the user runs do not inherit those privileges unless they are approved beforehand or the user explicitly authorizes it.

The down side is that it is intrusive, and prevents normal operation of your programs by blocking the permissions levels they need for normal operation. You will also have constant popup prompts asking you to assign the needed permissions levels as they operate. While it does a good job in blocking malware, it is often found to block just about everything else. Many people have opted to turn this feature OFF in Windows. Here is a short guide on how to do this.

UAC ACCESS IN WINDOWS 7

Open Control Panel from your Windows Start menu. Then select *User Accounts*.

You will find the Change User Account Control option on the right hand pane.

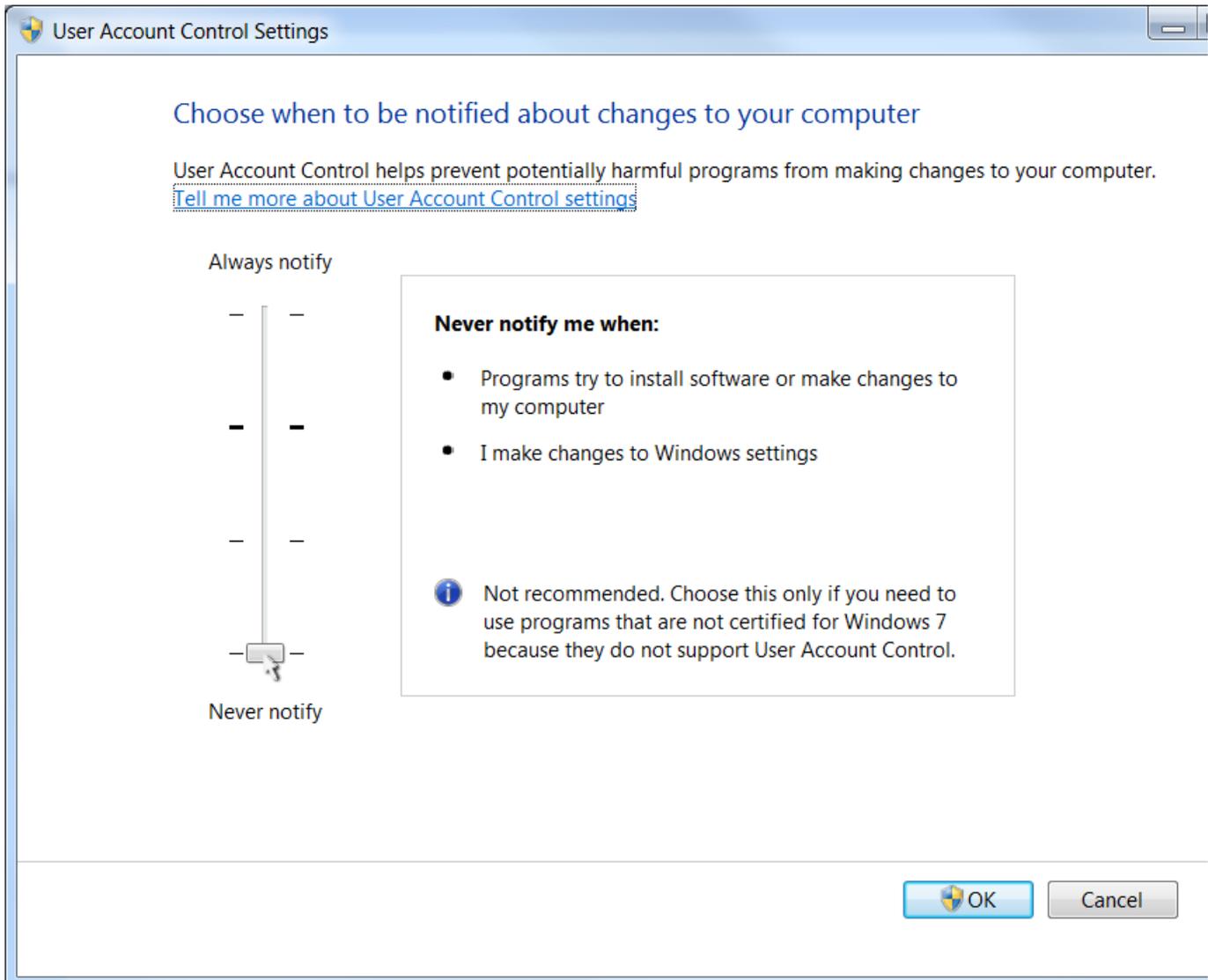
Control Panel Home
Manage your credentials
Create a password reset disk
Link online IDs
Configure advanced user profile properties
Change my environment variables

Make changes to your user account

- Change your password
- Remove your password
- Change your picture
-  [Change your account name](#)
-  [Change your account type](#)

-  [Manage another account](#)
-  [Change User Account Control settings](#)



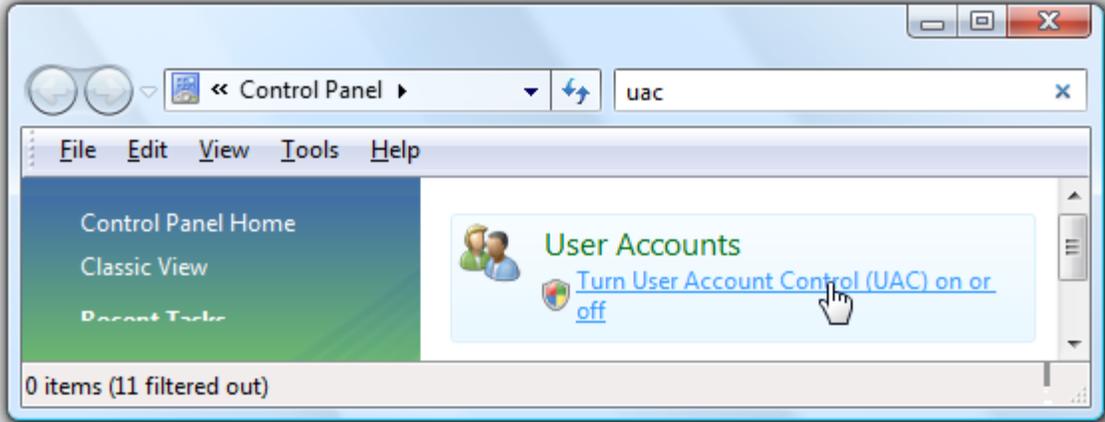


The slider control gives you several levels of activity for UAC. If you want to shut it off completely, move the slider to *Never Notify*.

Press OK.

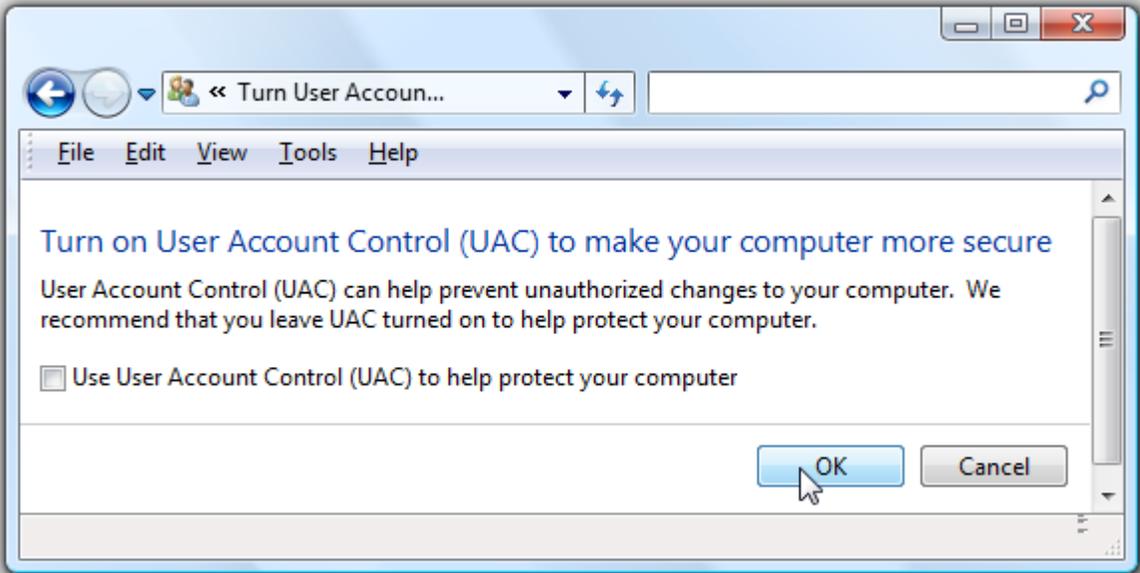
UAC ACCESS IN WINDOWS VISTA.

Open Control Panel from your Windows Start menu. Then select *User Accounts*. The selection *Turn User Account Control (UAC) on or off* selection will appear in the right hand pane.



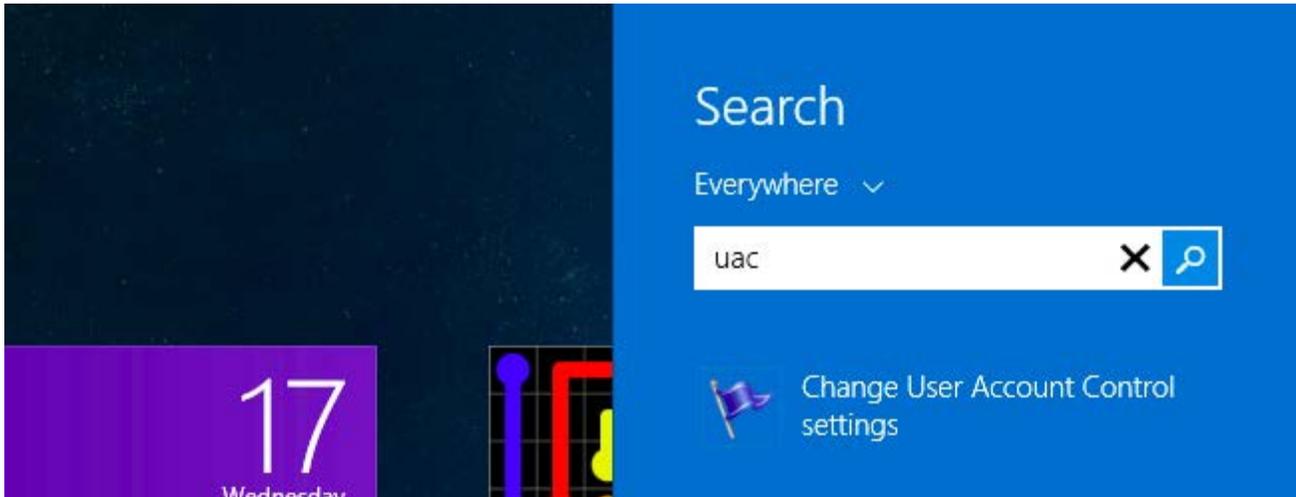
Here your option is simply ON or OFF. To turn it OFF, uncheck the box that says *User Account Control (UAC) to help protect your computer*. To turn it ON, check the box.

Press OK.



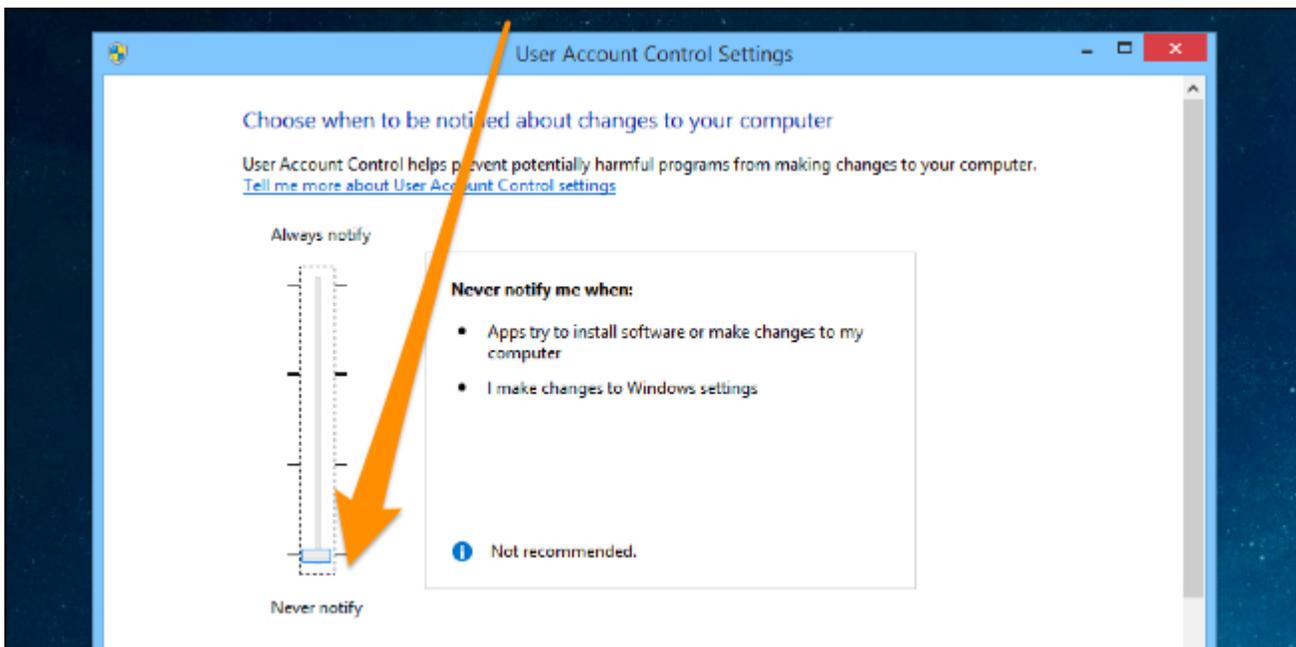
UAC ACCESS IN WINDOWS 8

Open up the Start screen, search for UAC, and you should see an option for User Account Control settings. If you don't, you'll need to change to search through your Settings first, but then you should see it.



The slider control gives you several levels of activity for UAC. If you want to shut it off completely, move the slider to Never Notify.

Press OK.



Data Execution Prevention

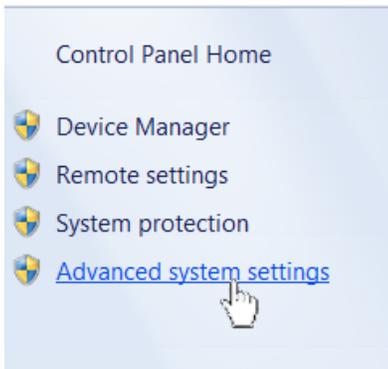
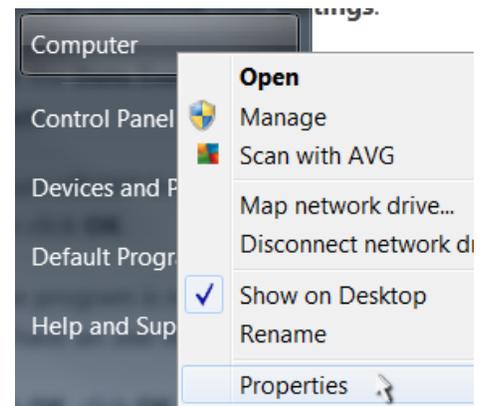
Data Execution Prevention (DEP) is a security feature that protects against some program errors, and helps prevent certain malicious exploits, those that store executable instructions in a data area via a buffer overflow for example. It does not protect against attacks that do not rely on execution of instructions in the data area.

DEP monitors programs and running processes to determine if they are using system memory safely. DEP is not a security fail safe. It is merely an added layer of protection. But when it was first implemented in Windows XP, there were issues with software compliance and many users ran into errors that prevented them from running certain programs on their computers.

Problems with DEP are typically only experienced when attempting to install, run, modify or uninstall applications. Microsoft claims that these applications may not yet comply with the new DEP standard of "safe memory use". However, experience has shown that this feature in Windows is known to interfere with many programs that you normally run. Fortunately, DEP can be modified to accommodate your needs.

Open System by clicking the *Start* button Picture of the Start button, right-clicking *Computer*, and then clicking *Properties*.

Click Advanced system settings. Administrator permission required If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

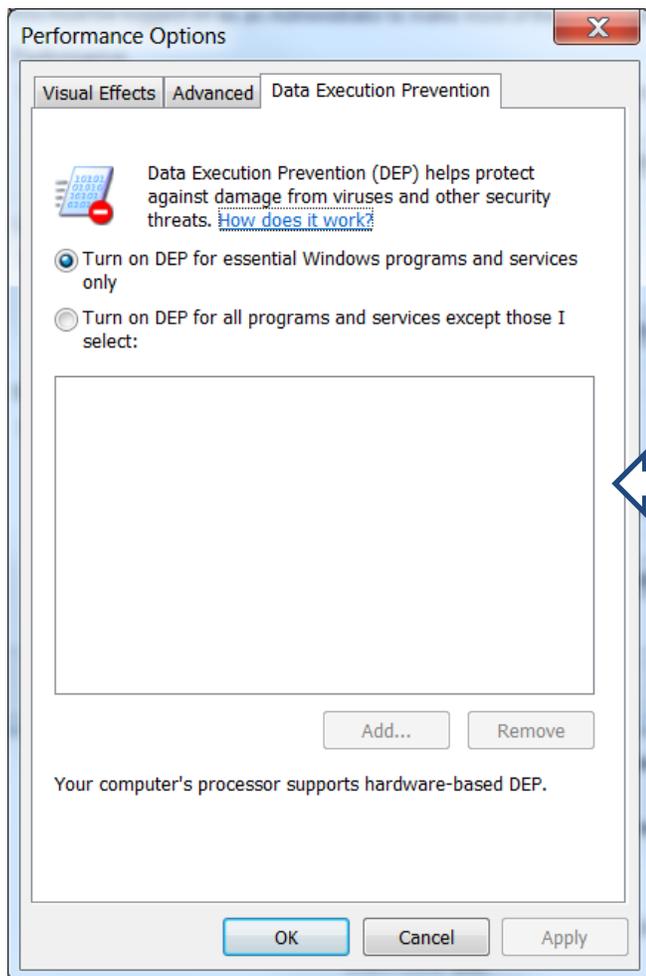
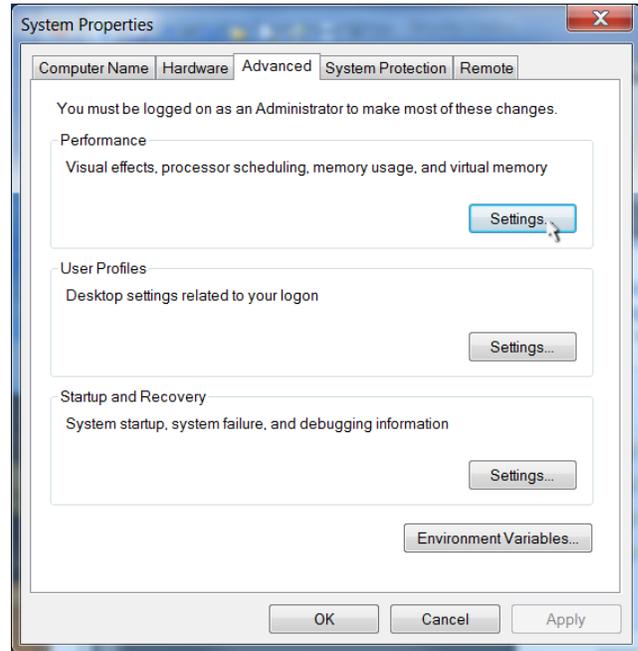


Under *Performance*, click *Settings*.

Click the *Data Execution Prevention* tab.

To turn off DEP select *Turn on DEP for essential Windows programs and services only* and press OK.

To have DEP active for all programs click *Turn on DEP for all programs and services except those I select*.



If the program is not in the list, click Add. Browse to the Program Files folder, find the executable file for the program (it will have an .exe file name extension), and then click Open.

Click OK, click OK in the System Properties dialog box if it appears, and then click OK again. You might need to restart your computer for the changes to take effect.

Safe Mode

Safe mode is a diagnostic mode in Windows. Safe mode is intended to fix most, if not all problems within an operating system. In safe mode, Windows will have reduced functionality, but the task of isolating problems is easier because many non-core components are disabled.

STARTING WINDOWS IN SAFE MODE

As the computer is booting press and hold your "F8 Key", which should bring up the "Windows Advanced Options Menu". Use your arrow keys to move to "Safe Mode" and press your Enter key.

Note: With some computers if you press and hold a key as the computer is booting you will get a stuck key message. If this occurs, instead of pressing and holding the "F8 key", tap the "F8 key" continuously until you get the startup menu.

Select Safe Mode or Safe Mode with Networking.

Choose Advanced Options for: Microsoft Windows Vista

Please select an option:

Safe Mode

Safe Mode with Networking

Safe Mode with Command Prompt

Enable Boot Logging

Enable low-resolution video (640x480)

Last Known Good Configuration (advanced)

Directory Services Restore Mode

Debugging Mode

Disable automatic restart on system failure

Disable Driver Signature Enforcement

Start Windows Normally

Description: Start Windows with only the core drivers and services. Use when you cannot boot after installing a new device or driver.