FlightSim Developers
Flying high in digital aviation

INSTALLATION TROUBLESHOOTING GUIDE

A resource for resolving problems during the installation process

Table of Contents

Introduction

Software installers, in general, write files to the necessary areas on your hard disk and registry to make program work. They also add startup menu shortcuts and other things to help it operate and work with Windows. Most software for *Microsoft® Flight Simulator* (*FS*) requires an installation program to get the right files into the right place. When files or registry entries are misplaced or missing, chances are the software will not work, or will result in an error or Crash to Desktop (CTD).

This guide is intended to help you troubleshoot problems during and after installation, so you can get the most of your *FS* experience.

Installation Requirements

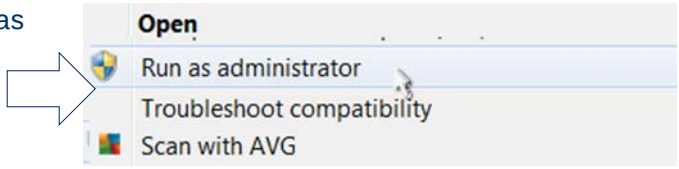
Because installation programs require access to a wide variety of Windows services, and the ability to create/write files and registry entries, which most applications do not necessarily require.

Administrative Permissions

All installation programs *must* have full access to the registry and folder/file structure. Without this access, the program will not be able to create and/or install the files and registry entries required for the software to operate. In Windows terminology, this access is called Permissions. A more detailed description of Permissions can be found on page 9, and in our Windows Permissions publication.

RUN AS ADMINISTRATOR

In order to insure that the installation program has the permissions it needs to do its job, we recommend that when running ***any*** installer, you ***always*** right click on it and select *Run As Administrator*.



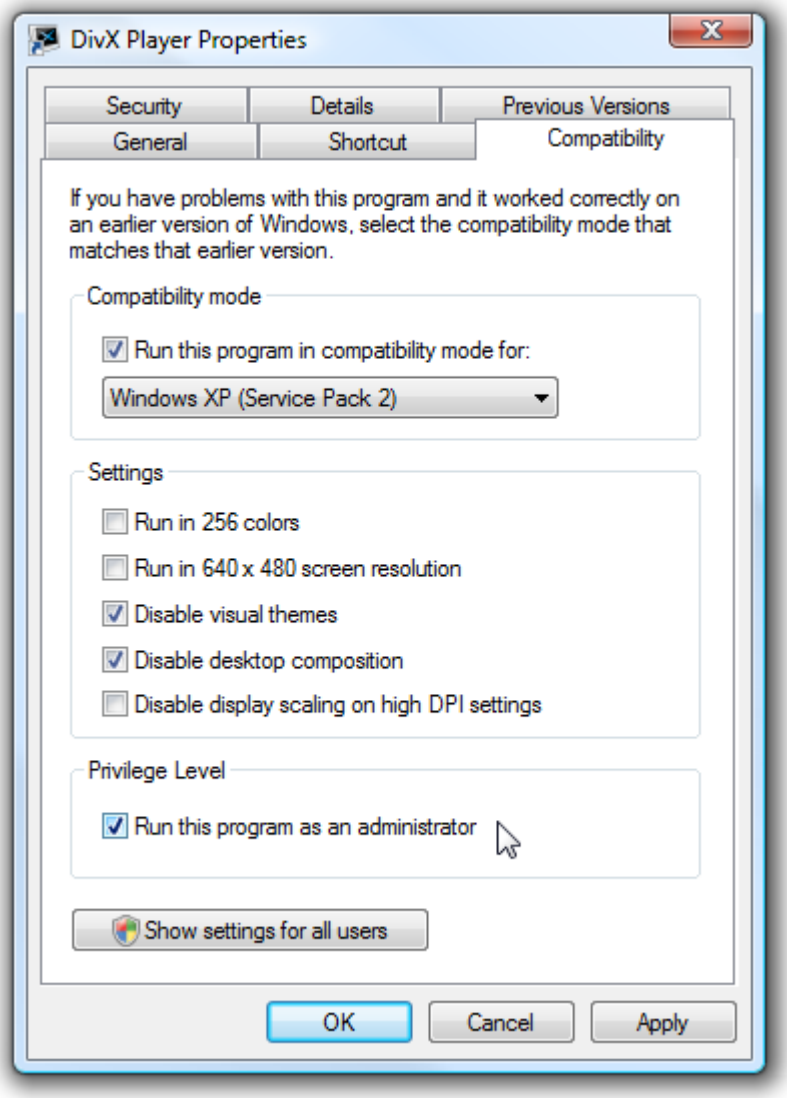
Keep in mind that even if your *Windows Login* Account has administrative level *Permissions*, that does not mean that you automatically have full administrative rights. This is how Windows is designed. You need to perform this step to be sure you are running a program with full *Administrator* level *Permissions*.

XP Compatibility Mode

This step is typically not necessary, however, in the more restrictive environments of Windows 7, 8 and Vista, depending on how your security environment is set up, it is sometimes advantageous to run installation programs in *XP Compatibility Mode*.

To configure the compatibility mode for an application, just locate the installation directory and right click on the .exe, selecting Properties from the menu.

Select the Compatibility tab:



Configuration Recommendations

Where you run the installer from, and the location where FS resides, are very critical factors in both addon installation and functionality. The following is intended as a guideline to help you experience the best results in installing and running addon software.

Background Programs

It is normal to have quite a few programs running in Windows at all times. All installers recommend you close as many programs as possible before running an installation program. This is because you may need as many system resources as you can muster when installing a new program. If you have lots of system RAM, this is not quite as critical, but if not, it is essential. Otherwise, problems are almost guaranteed to result, which include installation errors and Crash to Desktop (CTD). Our recommendation is that you always reboot your computer to a clean startup before running any installation program.

You always want to save and exit any programs, text files, etc. before running a software installer. If you experience problems during the procedure, and your computer has to reboot for any reason, you will not lose any unsaved work or data.

File Location

Make sure you are ***not*** attempting to run the installer over the Internet instead of downloading it first and then running it from your hard drive. Some browsers give you the open to open a file over the Internet, or Download it.

Depending on your browser and/or operating system, this option is sometimes given to you when you click on a link to an installer or other program.

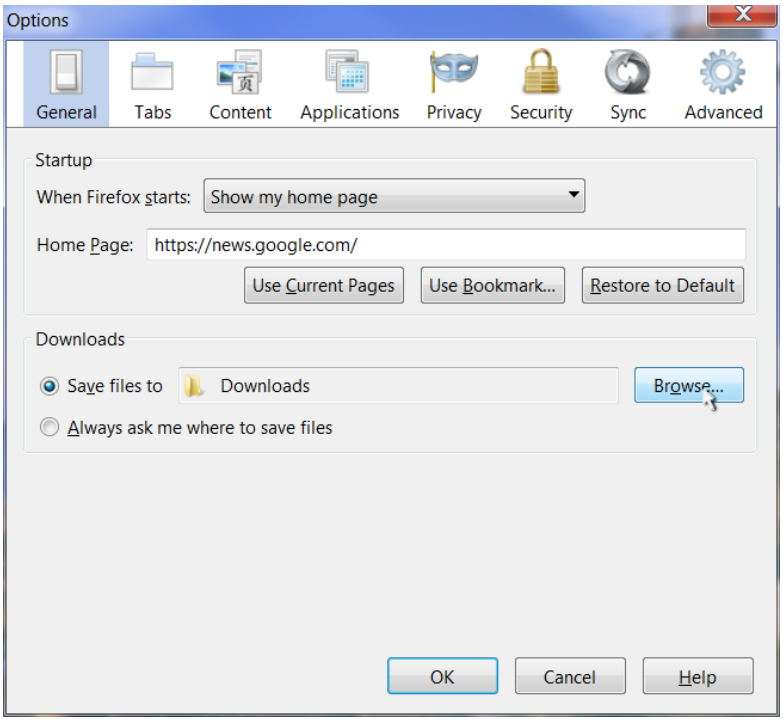
Installation programs, unless otherwise specified by the publisher, should ***always*** be run from a directory on your local hard drive and not from across the Internet or a network. Do not select the "*Run*" button.

Always click "*Save*" and download the file, the file goes to a folder in Windows that should allow you to run it with full administrator permissions and system access. Some browsers allow you to choose this location, where you can specify where the setup file goes (My Downloads or the desktop).

Many browsers, like Firefox, automatically send the file to a predetermined directory (usually your Downloads folder).

The Options menu for that browser will give you the ability to choose that location. Make sure the directory you select is one to which your Windows Login has full access, preferably, Ownership. Otherwise, running programs from this location could give you access and *permissions* issues that you would not otherwise have.

When choosing "*Run*", the setup file is downloaded to your temporary internet file. This location on your computer typically has restricted permissions and system access, which will lead to unnecessary installation problems.



FOLDER PERMISSIONS/OWNERSHIP

Your Windows login needs to have full ownership of the folder/directory from where the installer is run, and where *FS* is installed. If *FS* is installed in a directory that has restricted permissions, for example, the Program Files(x86) folder, it is possible that that location severely limits permissions for programs within that file structure, regardless of how your login permissions are set. This can be a particular problem when running the installer from, or having *FS* in a different drive or partition than where your operating system is installed. Downloading or installing from or to an external drive or a Solid State Drive (SSD) can also be highly problematic with respect to the advanced security features in Windows 7 or Vista. This does not mean you cannot run *FS* from an external drive. We are simply pointing out that this introduces a higher layer of security configuration that must be addressed.

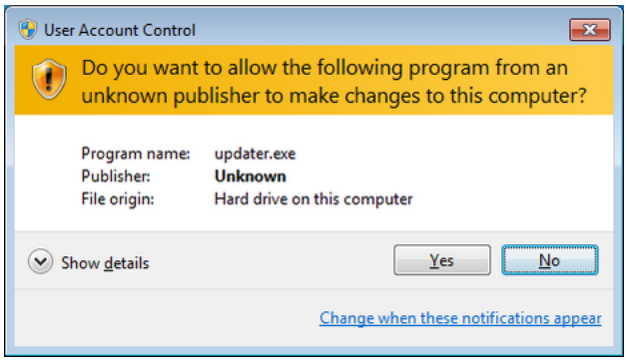
Regardless of whether the location is on the same drive as your operating system, or whether it is on a secondary or external drive, the folder where the installer resides needs to have full permissions and access to your Windows drivers. Otherwise, installation problems will result. If that location is on an external drive, it is strongly recommended that your Windows Login account have ownership of that drive as well. See page 4 of our Windows Permissions publication for more information on determining and/or changing ownership of a drive or directory.

With respect to installing *FS* on a "*dedicated drive*", which has been advocated in some Internet forums; this is really an urban legend. It really just depends on the speed of your drive. If your external drive is faster than your primary drive, you really need a new primary drive. The more critical parameters for performance in FS are your CPU speed, amount of system RAM, and the speed and memory on your video card.

User Account Control (UAC)

User account control (UAC) may be interfering with the installer. Shutting it off would relieve this problem. User Account Control (UAC) was implemented first in Windows Vista, and was designed to prevent unauthorized changes to your computer. UAC notifies you when changes are going to be made to your computer that requires administrator-level permission. UAC works by adjusting the permission level of your user account. If you are doing most tasks, like installing software, you have the permissions of a standard user—even if you are logged on as an administrator. Microsoft advocates this as a good thing, and when it comes to blocking malware, it is. However, when it comes to running software installers, it can introduce a layer of complexity and restrictions that will prevent the program from doing its job. Installers need much more broad system access than most programs, and absolutely must have full *administrator permissions* to create, modify, and add files or registry keys.

Microsoft claims that by simply pressing "*Yes*" on the dialog box that appears when running a program; it will then have administrative access to your computer. Experience has shown that this is not necessarily the case. UAC is known to affect a lot of the security protocols on your system, particularly when 3rd part security software has been installed.



This is not intended to advocate that you permanently disable UAC on your system. It does a good job at preventing access to your system from unknown malware and spyware. However, the operating word here is unknown. Installation programs that you intentionally run that need administrative access to your system do not need to be treated the same way. We ***strongly*** recommend that you shut this feature down when running any installation program (not just ours). See page 16 of our Windows Permissions publication for more information on how to configure UAC.

Data Execution Prevention (DEP)

Data Execution Prevention (DEP) is a security feature first introduced in Windows Vista that protects against some program errors, and helps prevent certain malicious exploits. Nevertheless, when it was first implemented in Windows, there were issues with software compliance and many users ran into errors that prevented them from running certain programs on their computers, particularly, installation programs.

We will leave it to you as to whether you want this running in your software environment. However, during the installation of *any* software, we *strongly* recommend that this feature is degraded. You can find more information on page 21 of our Windows Permissions publication.

Anti-Virus and Security Software

These programs are known to cause issues with *all* software installers. This is why all installation programs (not just ours) recommend that you shut these programs down temporarily during the installation process. This is because installation programs need full administrative access to your system, and must be able to create, delete or modify files or registry keys in order to do their job. Exactly the find of thing that malware does, and security software is designed to contain. When active, depending on the security program and how it is configured, it may also *contain* your software installer. Malware is software that runs on your system *without your knowledge*. Installation software is run specifically by you to make these changes on your system.

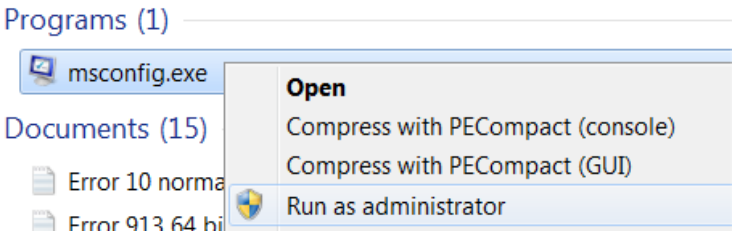
If suspending your security software or firewall does not solve installation problems, sometimes, depending on which security/firewall software you are using, it may not be easy to simply "*switch off*". If you continue experiencing problems it may be a case where these program's services are still running in Windows regardless of the fact that you shut them off, in which case the best way to close all the background applications is by rebooting your computer using Diagnostic Startup method.

When the computer reboots, Windows will usually prompt you that a custom startup configuration is being used, and give you an option to not show the message again. Do not select this option. Once the software is installed you will want to repeat this process and restore the original options.

DIAGNOSTIC STARTUP FOR WINDOWS 7 AND WINDOWS 8

1. Click the Windows Start Menu
2. Type *msconfig* in the search box. A link to the file msconfig.exe should appear.

3. Right click on the msconfig.exe link and select *Run As Administrator*.

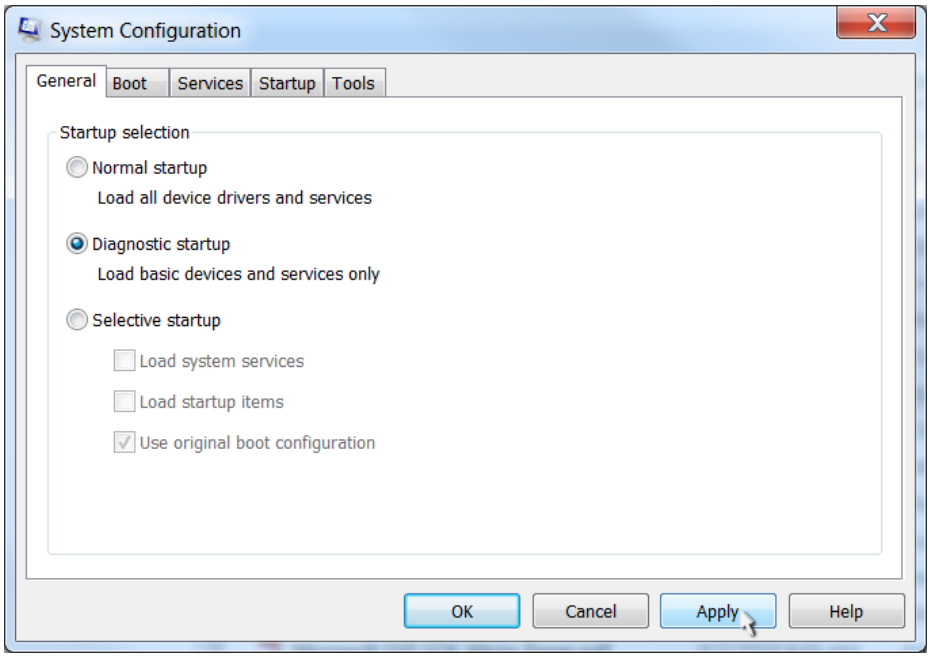


4.
On the General tab, under the Selective Startup section, uncheck Load System Services and Load Startup Items boxes.

5.
The Diagnostic startup option should be checked.

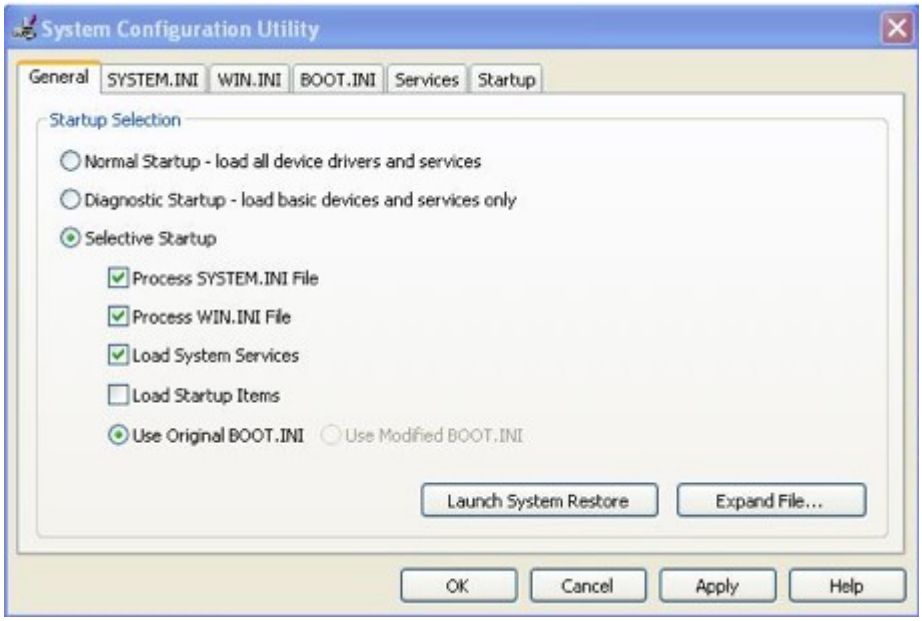
6.
Press Apply and/or OK.

7.
If not prompted to restart your computer, do so manually.



DIAGNOSTIC STARTUP FOR WINDOWS XP

1. On the Start menu, click Run. A Run window (command prompt) appears.
2. Type msconfig in the Open field and click OK. The System Configuration Utility opens.
3. Click the General tab.
4. Select the "Selective Startup" option.
5. Deselect the "Load Startup Items" checkbox.
6. Press OK.



Reference

The following topics are expanded descriptions of what is being presented in this document.

Permissions

Rules associated with objects on a computer or network, such as files and folders. Permissions 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 shared folder 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.

The following table lists the permission levels that are typically available for files and folders.

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.

TO CHECK THE PERMISSIONS OF A FILE OR FOLDER

1. Right-click the file or folder, and then click Properties.
2. Click the Security tab.
3. Click a user name or group under Group or user names.

The permissions for the selected user or group are shown in the lower portion of the properties dialog box.

TO CHECK THE PERMISSIONS OF A REGISTRY KEY

1. Open Registry Editor. From the Windows *Start Menu*, in the *Search* box, type *regedit*. The program will appear on the available programs list. Right click on it and select *Run As Administrator*.
2. Right click the key to which you want to check permissions.
3. Click *Permissions*.

More information on *Permissions* is available in our Windows Permissions publication.

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 our Windows Permissions publication, page **Error! Bookmark not defined.** for more details.

Crash to Desktop (CTD)

A CTD is a computer program crash which occurs when a program unexpectedly quits, abruptly taking the user back to the desktop. Usually, the term is applied only to crashes where no error is displayed with no apparent action. This is a highly unusual situation during product installation, and is usually preceded by the program freezing for a short period.

Since they frequently display no error message, it can be very difficult to track down the source of the problem, especially if the times they occur and the actions taking place right before the crash do not appear to have any pattern or common ground. The most common cause of these problems are:

- Low system resources.
- A background program, such as security software.
- Any program that is running in Windows at the time that encounters a problem, which will often cascade to the installation program.

In the case of a CTD during the install process, we strongly recommend you reboot your computer in Selective Startup Mode, as outlined on page 7.

The Blue Screen of Death (BSOD)

Also known as a stop error, bluescreen, Blue Screen of Doom, BSOD, bug check screen, or Stop screen. It is an error screen displayed by operating systems after a crash.

In Windows XP and forward, the BSOD occurs when the kernel or a driver running in kernel mode encounters an error from which it cannot recover. This is usually caused by an illegal operation being performed. The only safe action the operating system can take in this situation is to restart the computer. As a result, data may be lost, as users are not given an opportunity to save data that has not yet been saved to the hard drive.

Problems such this are (obviously) *not normal*, during installation of addon software or its use in *FS*. It is likely not a problem with the software you are using, the installation program, or FS. The most likely causes are problems with your system RAM, hardware or driver related. Most BSODs show a STOP code that can be used to help figure out the root cause.