Granting AIMS users the correct permissions in Windows 7 or Vista

When installing AIMS in Windows 7 or Vista operating systems, you need to ensure that both the person installing the software and all users have been granted the correct level of security rights.

AIMS Users need "modify" level permissions so they can make changes to the database file and create and write objects in other AIMS sub-folders. This is a short guide showing how to set up this permissions level. You will need to know your administrator level log in and password, and in complex network environments you will need to talk to your Network Administrator.

In Windows 7 and Vista, the UAC (User Account Control) function will, unless you specify otherwise, only grant users standard permission levels. By amending the permissions as specified below you will not need to remember to "run as administrator" every time you open the database.

If after trying to install AIMS user sees the error message below when trying to log into AIMS or when attempting to add a client or work then, the most likely problem is that their permission level is wrong.
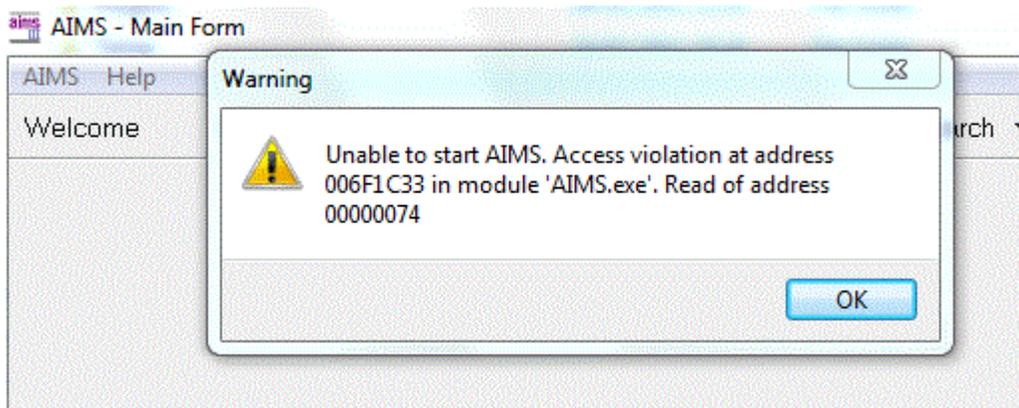
How to grant modify permissions:

1.   Installing software requires Windows 7 or Vista users to have administrator level permissions. Once installed, you must ensure that all those wanting access to the database are granted the correct level of permissions via their normal log in (i.e. without needing to log in as an administrator).

2.   With AIMS closed, in Windows Explorer navigate to the installation directory. On the folder that contains the AIMS.EXE file, (probably called either AIMS SA or AIMS NS) right click the folder and select properties.

This will bring up the screen below. Select the Security tab.
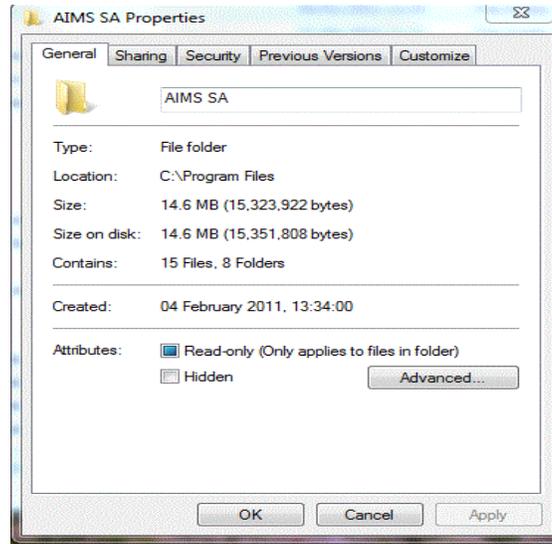
3.   Select and amend the security level.

From the "Group or user names:" window click on the group that starts "Users". In the example below the remainder (WINDOWS-9Afz5gX\Users) is the machine name and will be different on your system. Note the permissions level in the lower window does not have modify or full control ticked.
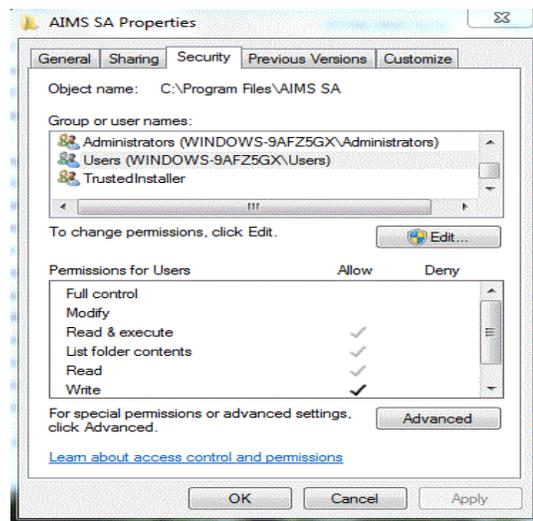
Now click on the Edit button.

4.   Editing a Users security level.

At this point you may be asked for your administrator log in and password as you are making a system wide amendment. Once you have supplied the details you will see the window below.

Once again highlight the "Users (WINDOWS-…\Users)" in the top window and in the "Permission for users" window tick the Modify and Full Control boxes in the Allow column.

Now click Apply.
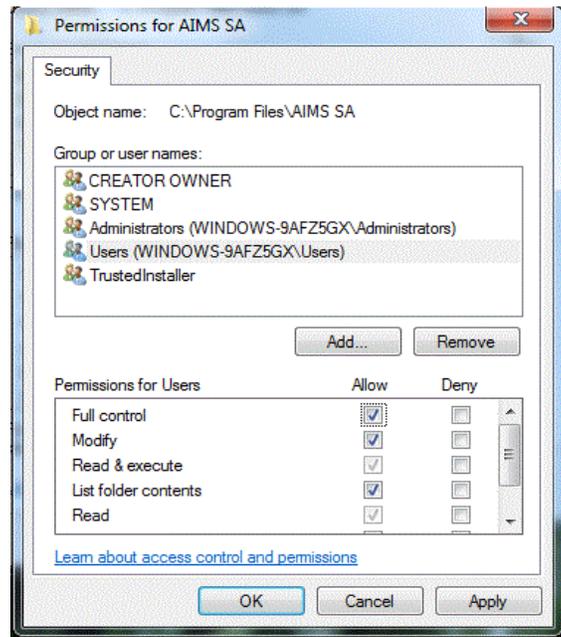
5.   Double check your inheritance.

Now check that the level of permissions you have granted to the top level AIMS folder has been inherited by the sub folders. In particular AIMS needs to be able to modify the Data folder, Temp folder and Error Log folder.

Having applied the permission change above, OK out of that window and return to the security tab window. Now click on the Advanced button. You should see something like the screen below.

Make sure the "Users (WINDOWS…\Users)" shows that Full control permissions Apply to "This folder, sub folders and files".

If not, highlight the permission you wish to change and click the change permissions button, make the amendment and apply.

Advanced Security Settings for AIMS SA

Permissions | Auditing | Owner | Effective Permissions

To view details of a permission entry, double-click the entry. To modify permissions, click Change Permissions.

Object name: C:\Program Files\AIMS SA

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Users (WINDOWS-9AFZ...	Full control	<not inherited>	This folder, subfolders and...
Allow	TrustedInstaller	Special	C:\Program Files\	This folder and subfolders
Allow	SYSTEM	Full control	C:\Program Files\	This folder, subfolders and...
Allow	Administrators (WINDOW...	Full control	C:\Program Files\	This folder, subfolders and...
Allow	Users (WINDOWS-9AFZ...	Read & execute	C:\Program Files\	This folder, subfolders and...
Allow	CREATOR OWNER	Special	C:\Program Files\	Subfolders and files only

Change Permissions...

☑ Include inheritable permissions from this object's parent

Managing permission entries

OK | Cancel | Apply

6.   All users should now be able to log on to AIMS using their normal log in.