How do I reset the permissions in an entire registry hive of a computer, rather than changing the permissions for each registry key individually?

Caution: Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.

SolidWorks Technical Support has encountered a number of occasions when users cannot access registry information through errors in the expected permissions. One example of this behaviour is seen in SolidWorks 2007, where SolidWorks has been installed using Product Activation; however, when SolidWorks 2007 is started the user is prompted for a registration code. See solution S-010765 for more information. Other examples of incorrectly set registry codes exist but these have not been reproduced with SolidWorks for deeper investigation. The behaviour is believed to exist where library files are not registered during the installation of software if a reboot is triggered as part of the installation process. SolidWorks technical support recommends that any user performing a software installation where a reboot is triggered should log onto the computer again after the reboot to complete the installation. Any CD/DVD used during the software installation should be left in the computer drive during the log-on process.

The logic of this theory is:

During a software installation a reboot is triggered.
The user performing the installation honours the reboot but does not log onto the computer following the reboot.
At this time the installation may not be fully completed. If this is the case the user performing the installation will have commands waiting in the run-once portion of their personal registry. If the installer cannot find the install media (say a DVD is no longer in the drive) then the installation process can also be interrupted.
If a different user with power user permissions runs the program that is installed but not completed they would automatically register any library files not registered at this time. During this registration process the registry keys will be added with the users permissions only. This would allow that user full control over the key but would deny access to the key for every other user including the system administrator. When this happens the solution is for the administrator to first take ownership of the registry keys and then reset the permissions on the registry keys.

The outcome of this behaviour is to recommend that any user performing an installation and having a reboot triggered must log-onto the computer following the reboot in case the installation has not fully completed. The source install media should be available to the user at log-on. System administrators are encouraged to consider the use of Active Directory or other software publishing systems for the distribution of software installations to overcome this limitation.
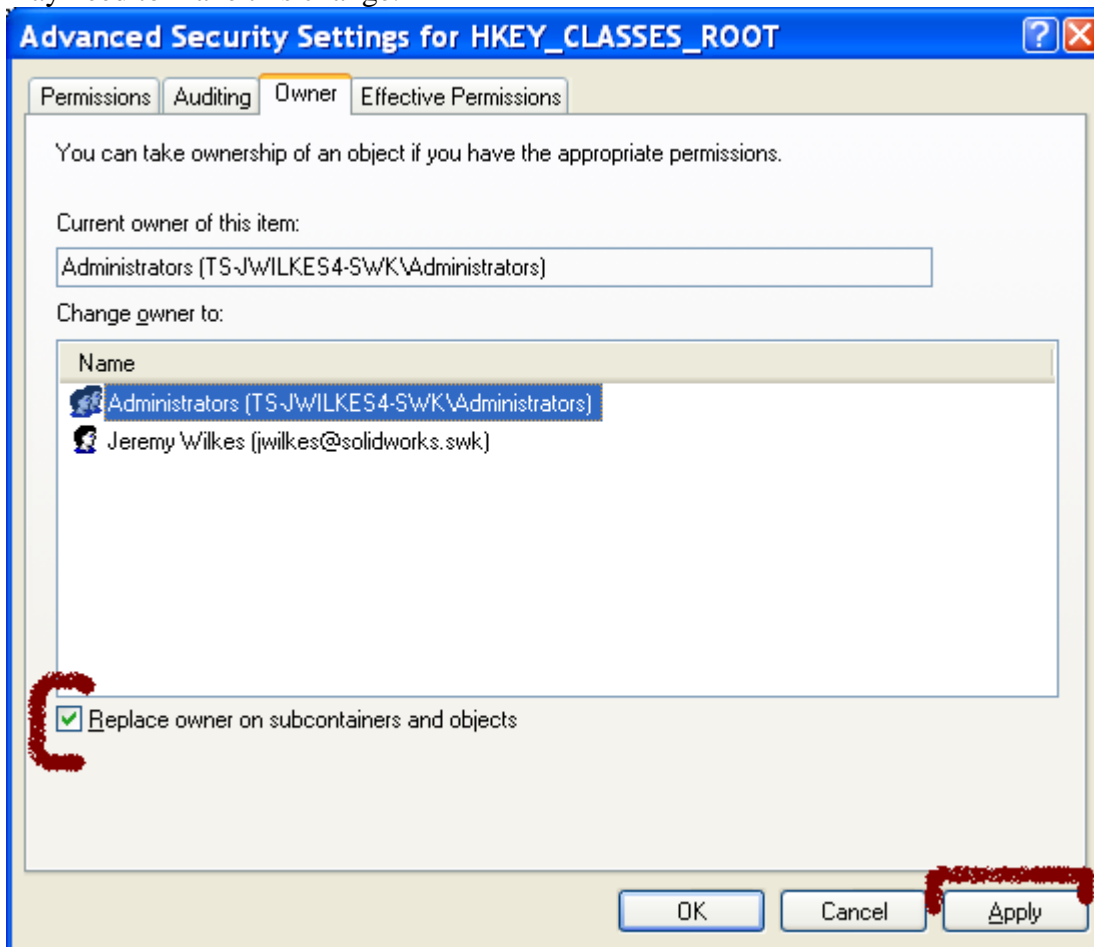
Taking ownership and resetting permissions:
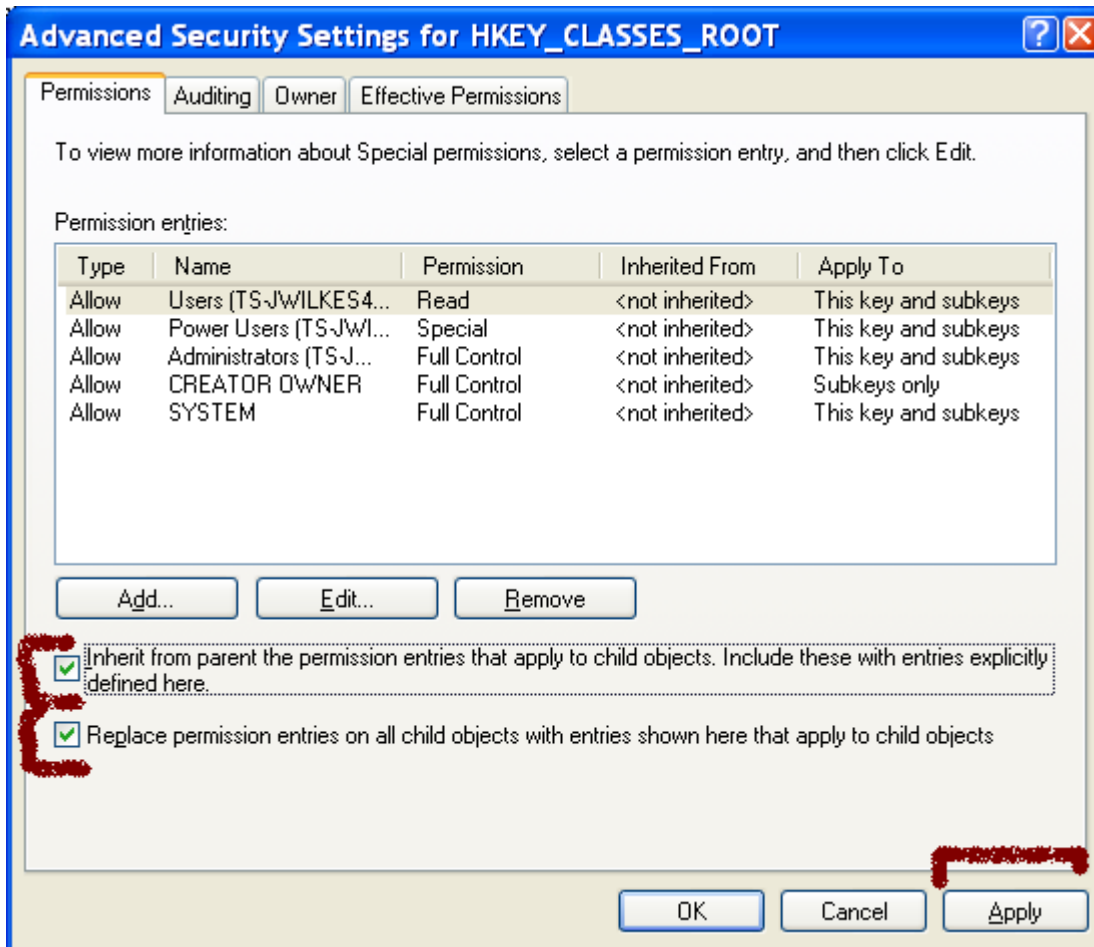
Run Regedit - <Start><Run>{Regedit}

Select the registry {HKEY_CLASSES_ROOT}
From the right mouse button (RMB) menu select <Permissions>
Select the "Advanced" button on the first screen
Select the Owners tab

To reset the ownership of keys elect to change owner to the Administrators group, choose to "Replace owner on subcontainers and objects" and then apply the changes.

In some instances this action may need to be undertaken by a member of the Domain Administrators group and possibly the Domain Administrator account. If the user owning the key is an enterprise rather than domain account the Enterprise administrator may need to make this change.

Advanced Security Settings for HKEY_CLASSES_ROOT

Permissions | Auditing | Owner | Effective Permissions

You can take ownership of an object if you have the appropriate permissions.

Current owner of this item:

Administrators (TS-JWILKES4-SWK\Administrators)

Change owner to:

Name

Administrators (TS-JWILKES4-SWK\Administrators)
Jeremy Wilkes (jwilkes@solidworks.swk)

☑ Replace owner on subcontainers and objects

OK   Cancel   Apply

After changing the ownership of keys the permissions should be changed by selecting the Permissions tab. Apply the default permissions selecting the inheritance option and the option to "Replace permissions on child objects…" and then apply the changes.

Advanced Security Settings for HKEY_CLASSES_ROOT

Tabs: Permissions | Auditing | Owner | Effective Permissions

To view more information about Special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Users (TS-JWILKES4...	Read	<not inherited>	This key and subkeys
Allow	Power Users (TS-JWI...	Special	<not inherited>	This key and subkeys
Allow	Administrators (TS-J...	Full Control	<not inherited>	This key and subkeys
Allow	CREATOR OWNER	Full Control	<not inherited>	Subkeys only
Allow	SYSTEM	Full Control	<not inherited>	This key and subkeys

[Add...] [Edit...] [Remove]

☑ Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.

☑ Replace permission entries on all child objects with entries shown here that apply to child objects

[OK] [Cancel] [Apply]

This advice would reset permissions and is believed to address several installation and operational issues.