

Re: SfcIsKeyProtected (Windows Resource Protection)

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2006-08/msg00083.html>

- *From:* "Idan" <rubin.idan@xxxxxxxxxx>
 - *Date:* 3 Aug 2006 14:32:54 -0700
-

First let's review SfcIsKeyProtected a bit. This function returns a boolean value which indicate whether the registry key is WRP protected or not. (if you want more info about the WRP feature let me know). All base keys such as HKLM, HKCR are not WRP protected, therefore the value 0 (FALSE) is actually the right value.

the parameters of the functions are:

HKEY – a handle to a registry key. This is a required parameters, and cannot be NULL. When you passed NULL you got error 6 which is ERROR_INVALID_HANDLE and this is also by design.

LPCWSTR – a string containing a sub key of the opened registry key.

This parameter is optional and can be NULL.

REGSAM – this parameter is used to check 32bit registry keys on 64bit machine. I'd pass KEY_READ.

To check if a registry key is WRP, you can do the following:

1. open regedit.
2. right click on a registry key and choose 'Permissions...'
3. A key is WRP if TrustedInstaller service has full access to it and all other users/groups have only read access. TI is the owner of the key in most cases.

(check out HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Speech\UX for example)

so if you want to the API to return true you have to do the following:

HKEY key;

LONG status = RegOpenKeyExW(HKEY_LOCAL_MACHINE,
L"SOFTWARE\Microsoft\Speech\UX",

NULL,

READ_ACCESS,

&key);

BOOL isProtected = SfcIsKeyProtected(key,NULL,KEY_READ);

Let me know if you have other questions/problems.

Rubin.

Jim wrote:

Re: SfcIsKeyProtected (Windows Resource Protection)

Hi Rubin,

Thanks for responding – I can't find anything other than the MS doc on SfcIsKeyProtected.

I was using Beta 2 Build 53?? and installed the most recent build the other day. Neither of them worked and both behaved the same way. I'm away from my office so I can't get access to see what the latest build number is.

SfcIsKeyProtected returns 0 with GetLastError returning 0 when I provide one of the root keys (HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, HKEY_USER) and anything for the SubKey. I tried "SOFTWARE", "SOFTWARE\Microsoft\Windows\CurrentVersion", keys that don't exist, other keys that do but shouldn't be protected. I tried passing NULL for the subkey to check the root key and it returned the same codes. I tried calling RegOpenKeyEx on a subkey and passing the returned HKEY as the root and it still behaved the same. The only test I made that returned something different was when I passed NULL for the root key, in which case the function returned 0 and GetLastError returned 6.

Thanks,
Jim

"rubin.idan@xxxxxxxx" wrote:

Hi Jim,

1. What build of Vista are you using?
2. How were you using SfcIsKeyProtected? (what were the parameters you passed?)
3. What was the failure? (Did it return FALSE on a WRP protected key? did it return an error message?)

Thanks,
Idan Rubin

Jim wrote:

Has anyone been able to get SfcIsKeyProtected or SfcGetNextProtectedFile to work on Vista? I have been able to use SfcIsFileProtected but the other two don't seem to work at all?

Are there any tricks to using them? Is the documentation wrong?

Thanks for any information.

Re: SfclsKeyProtected (Windows Resource Protection)