

## Re: Problems creating keys under the HKEY\_LOCAL\_MACHINE in Windows XP

*Source:* <http://www.tech-archive.net/Archive/VB/microsoft.public.vb.winapi/2004-11/0320.html>

---

*From:* Jim Carlock (*anonymous\_at\_127.0.0.1*)

*Date:* 11/18/04

Date: Wed, 17 Nov 2004 21:27:21 -0500

Well, to help you along with some of the concepts that are involved, the best way I know how to do this comes into effect when describing NTFS file permissions...

It used to be that on Windows NT (Version 4, maybe 3.5 too) when one did a fresh install of the Server product, there was a group called Everyone. Everyone was given access to the hard disk drive. :-) I don't know if that applied to the registry as well so someone else will have to comment on that. Note, the Nimbda Virus infects computers and opens a system up for others to gain access to, by putting the Everyone group Full Control and propagating that over all folders on all drives.

Very bad bad thing. A default installation of Windows 2000 server with no service packs does the same thing I believe. It is left up to the administrators to remove the Everyone group and tighten up security.

I believe the Everyone Group is given Read-Only access to things... it's been a long time since I've done such an install. One of Win2Ks service packs might have fixed the Everyone problem. If not, the Microsoft Baseline Security Analyzer will take care of such things (I hope). I've always removed the Everyone Group from the root drive (right click on a drive in Explorer, click Properties, Security tab) before running the Baseline Analyzer.

The registry operates in much the same way that NTFS permissions operate. Things are usually configured at the root, with a few exceptions, and then everything is inherited from those root keys.

There are some special groups that get special permissions, in XP, and I think they might be inside NT as well but I don't know right off the top of my own head, such as CREATOR,

RESTRICTED, USERS, POWER USERS,  
ADMINISTRATORS and AUTHENTICATED USERS.

If there is only one person on the machine, you can pretty much remove all the groups and leave only the Administrators and System as having FULL CONTROL. I would suggest leaving things intact (and get rid of the Everybody account from having any permissions anywhere). Create a non-administrative account, and a power user account to test things.

I'm just babbling about things and don't have all the answers, so if anyone sees anything that is should be expounded upon, please expound!

--

Jim Carlock

Post replies to newsgroup.

"mayayana" <mayaXXyanala@mindYYspring.com> wrote in message news:D9Smd.3506\$pk6.3495@newsread2.news.atl.earthlink.net...

Actually, I was asking because I use Win98 (no one has to be a lackey there!) and have little experience with XP directly. I've never quite figured out exactly what options non-administrators have. On one occasion I was helping a friend with his XP computer and found that as the non-original administrator I had to go through the bizarre step of giving myself permission to access all keys! So apparently an administrator is not always an administrator on XP.

My impression was that non-admins can read but not write to HKLM, but I don't understand the overall design of Registry permissions in NT, so I was hoping that someone might explain it clearly.

---

mayayXXanala@mindYYspring.com

For return email remove XX and YY.

---

Jim Carlock <anonymous@localhost.com> wrote in message news:OmFT0yOzEHA.2568@TK2MSFTNGP10.phx.gbl...

> We are lackeys at all times... :-)

>

> For instance, try to take ownership of every key in the registry and let me know if you get it done successfully.

>

> Also, try to access every key in the registry by adding a dummy group or a dummy account that will never be used, by assigning that dummy group or individual as having access to the root of HKLM and forcing inheritance upon it.

>

> Make sure you mess with such things on a machine that you know can be lost. ;-)

>

> Let me know if there are keys you cannot take ownership of, or keys that cannot be assigned new permissions.

>

> I haven't tried it in safe mode. So maybe safe-mode will get it to work.

>

microsoft.public.vb.winapi: Re: Problems creating keys under the HKEY\_LOCAL\_MACHINE in Windows XP

> Also, things get real complicated as far as permissions  
> and such when network engineers put denials into  
> effect.  
>  
> --  
> Jim Carlock  
> Post replies to newsgroup.  
>  
> "mayayana" <mayayana@mindyyspring.com> wrote in message  
> news:8Unmd.1580\$pk6.22@newsread2.news.atl.earthlink.net...  
> He's talking about creating keys. Doesn't that require  
> full access? Are you saying that there's a more limited  
> permission available that still has the ability to create  
> keys?  
> ( As I think about that, though, I suppose there wouldn't  
> be much point in logging on as a lackey if one still had  
> full power in HKLM.)  
> \_\_\_\_\_  
>  
> mayayana@mindyyspring.com  
> For return email remove XX and YY.  
> \_\_\_\_\_  
>  
>  
>