

Re: Changing Registry ACL (need some more help)

Source: <http://www.tech-archive.net/Archive/Scripting/microsoft.public.scripting.wsh/2005-01/0169.html>

From: Gerry Hickman (gerry666uk_at_yahoo.co.uk)

Date: 01/12/05

Date: Wed, 12 Jan 2005 20:39:18 +0000

Hi,

The user should not have admin rights as this is a major security risk. First you need to decide who is in charge of this computer – the user or you? If it's the user, then you need to leave it alone. If it's you then you should have local admin password, in which case go and add yourself to the local admins group, reset all permissions on the whole machine and take the user out of the admins group. Send an email to the user and CC the manager asking the user not to change any permissions in future and how much time and expense it's wasted.

If you allow the user to continue to be an admin they could just remove all the permissions all over again and then you're wasting even more time.

mostro wrote:

> Well, I tried SetACL.exe and I can't get in to the users registry. This is
> the issue. The user has admin rights to his/her computer and has removed the
> domain admin and administrators groups from the registry (HKLM, HKU). Yes, I
> can go logonto the computer and remove the ACL on the registry key. Yes, I
> have full power to even scold the user and issue a formal warning to make
> them set the perms back. But, this isn't any fun. It's like playing chess
> and it's my move. I want to do it using the resources available and behind
> the scenes. Anyway, I have tried using Setacl using the following command.
>
> I tried this first using a login script. Testing it on my machine (login
> script from the domain) and it works. The same login script from then pushed
> out to the user doesn't work. Probably because of the rights.
>
> \\server\openshare\SetACL.exe -on "hklm" -ot reg -actn ace -ace
> "n:domain\myuser;p:full"
> \\server\openshare\SetACL.exe -on "hku" -ot reg -actn ace -ace
> "n:domain\myuser;p:full"
>
>
> I then threw the executable in the users local windows directory and put a
> batch file containing the below information in the start up folder (hidden).
> Still no go. Again, because I don't have rights to the reg key.

microsoft.public.scripting.wsh: Re: Changing Registry ACL (need some more help)

>
> c:\windows\SetACL.exe -on "hklm" -ot reg -actn ace -ace
> "n:domain\myuser;p:full"
> c:\windows\SetACL.exe -on "hku" -ot reg -actn ace -ace
> "n:domain\myuser;p:full"
>
> Any ideas?
>
> Thanks
>
>
>
> "Mostro" <mostro@adelphia.netnospam> wrote in message
> news:u2OaN0E1EHA.1968@tk2msftngp13.phx.gbl...
>
>>Thanks I will give it a read....
>>
>>
>>"Torgeir Bakken (MVP)" <Torgeir.Bakken-spam@hydro.com> wrote in message
>>news:%23\$tJF8x0EHA.1028@TK2MSFTNGP10.phx.gbl...
>>
>>>Mostro wrote:
>>>
>>>
>>>>Is there a way to change the the ACL on a registry key using WSH?
>>>>
>>>>Thanks
>>>>
>>>>Hi
>>>>
>>>>If WinXP or Win2k3, using the IADsSecurityUtility object
>>>>is an option.
>>>>
>>>>IADsSecurityUtility
>>>><http://msdn.microsoft.com/library/en-us/adsis/adsis/iadssecurityutility.asp>
>>>>
>>>>
>>>>Command line (Win2k and up):
>>>>
>>>>Regini.exe or SetACL.exe is an option:
>>>>
>>>><http://groups.google.com/groups?selm=400CA361.8E02C9C2%40hydro.com>
>>>>
>>>>SubInACL.exe can also be used for this, a new, bug-fixed version of
>>>>SubInACL.exe is available for download here (Win2k/WinXP/Win2k3):
>>>>
>>>><http://www.microsoft.com/downloads/details.aspx?FamilyID=e8ba3e56-d8fe-4a91-93cf-ed6985e3927b>
>>>>
>>>>
>>>>
>>>>

Re: Changing Registry ACL (need some more help)

microsoft.public.scripting.wsh: Re: Changing Registry ACL (need some more help)

>>>

>>>

>>>

>>>--

>>>*torgeir, Microsoft MVP Scripting and WMI, Porsgrunn Norway*

>>>*Administration scripting examples and an ONLINE version of*

>>>*the 1328 page Scripting Guide:*

>>><http://www.microsoft.com/technet/scriptcenter/default.mspx>

>>

>>

>

>

--

Gerry Hickman (London UK)