

Re: Local policy, IE and SP2...

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.embedded/2005-02/1284.html>

From: KM (*konstmor_at_nospam_yahoo.com*)

Date: 02/21/05

Date: Mon, 21 Feb 2005 12:21:04 -0800

YaronM,

I must mention here that I rarely use GPEdit and almost always I change the Explorer or System policies through registry.

The same I did for those tests I mentioned for SP2. As I said earlier, the NoViewOnDrive worked just fine for me.

Could you write for us the steps you did exactly (including logoff's and reboot's)?

However, this is true – those policies will not allow you to lock user accounts from launching applications from hidden drives.

That is where the DisallowRun can help you. I checked – it worked fine for me on XP Pro SP2. Therefore it will work on XPe SP2 too.

Although I must admit, locking some applications through NTFS permissions may be a better idea.

If you really want to lock down the OS you may want to take a look at some 3rd party solutions. E.g., Sygate agent will allow you to

lock down user account(s) to allow the launch of only particular applications. There is an XPe version of Sygate client available.

--

Regards,

KM, BSquare Corp.

> Hi,

>

> I am using different shells for each user. I use the Explorer.exe for the
> administrator and my custom shell for the user.

> I have two problems:

> 1. the policy NoViewOnDrive only works if I use it through gpedit.msc and
> not if I set it manually in the user's hive (NTuser.dat in his profile).

> by locking through gpedit.msc I am limited because it can affect the
> admin account also and I need to use workarounds such as NTFS deny on the
> GroupPolicy folder or the

> registry.pol and it is very inconvenient to administer and maintain.

> in SP1 the manual setting in the user's registry hive worked fine and
> now in SP2, Windows is ignoring the registry settings and just let the user
> access the drive's content.

> 2. even when using the above policy, the user can still write a full path to
> a file in the IE address-bar and launch it. for example,
> C:\WINDOWS\NOTEPAD.EXE. only if I prevented running the specific file or
> locked it using NTFS CALS then the file will be locked. but this means

microsoft.public.windowsxp.embedded: Re: Local policy, IE and SP2...

```
> changing all the system's default permissions on all files and I can't even
> imagine what problems could come from such an approach.
>
> I basically need to turn IE into an "Internet Browser Only Mode" without any
> local access to files and folders (if such a thing even exist...).
>
> Thanks,
>
> YaronM
>
>
> "KM" <konstmor@nospam_yahoo.com> wrote in message
> news:uqlIFx%23FFHA.1456@TK2MSFTNGP09.phx.gbl...
> > YaronM,
> >
> > I haven't tried the DisallowRun policy on SP2 but NoViewOnDrive and
> > NoDrives worked for me just fine.
> >
> > As you know the NoDrives key would only "hide" the specified drives in My
> > Computer folder (user can still type a hidden drive name or a folder on
> > that drive and can navigate there). However, if the NoViewOnDrive would
> > disallow the user to go into any folder of the restricted drive and on
> > typing in the Explorer address bar user would see an error message saying
> > something about the policies set up.
> >
> > That worked for me on XP Pro SP2 and XPe SP2.
> >
> > KM
> >
> >> Hi,
> >>
> >> I've been working with local security policies since SP1 and used many
> >> registry tweaks to lock-down the user's desktop.
> >> now, after I upgraded my builds to SP2 level, I'm getting some strange
> >> behaviour from Windows.
> >>
> >> My purpose is to lock the user's access to the local drive (i.e. C: Flash
> >> and Z: Ram-disk). that way, the user can only browse the internet using
> >> IE and launching application using my custom-shell.
> >> I've used the following reg-policies on the HKCU to prevent access for
> >> the user only (not the admin account):
> >>
> >> [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
> >> "DisallowRun"=dword:00000001
> >> "NoViewOnDrive"=dword:67108863
> >> "NoDrives"=dword:67108863
> >>
> >> [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun]
> >> "1"="ewfmgr.exe"
> >> "2"="mmc.exe"
> >> "3"="musrmgr.exe"
> >> "4"="tweakui.exe"
> >> "5"="explorer.exe"
> >>
> >>
> >> the number 67108863 represent "all drives". the problem is that on SP1,
> >> when a user launched IE and on the address-bar entered C:\ or some sort
> >> of a local path- it gave him "access denied" errors. now, in SP2 if I
> >> type C:\ it doesn't allow but if I launch c:\windows it does... :((
> >> (P.S. I tried setting the number that represent C+Z only.. same
> >> behaviour).
```

microsoft.public.windowsxp.embedded: Re: Local policy, IE and SP2...

```
> >>
> >> maybe I am looking in the wrong direction.. is there a way to turn IE to
> >> be an Internet-Browser only, without having this irritating synergy with
> >> the Explorer shell ?
> >>
> >> just a thought: maybe I could rename explorer.exe to MSshell.exe and set
> >> it to be the admin's defeault shell, that way in the user's session the
> >> IE will not find it...
> >>
> >> anyways, if anyone could share it's expirience I will be most thankful !
> >>
> >> Cheers,
> >>
> >> YaronM
> >>
> >
> >
>
>
```