

Re: What program is used to write events to the event log??????

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-02/3984.html

From: Roger Abell (*mvpNOSpam_at_asu.edu*)

Date: 02/25/04

Date: Wed, 25 Feb 2004 04:09:45 -0700

I have in the past tried reading through the MSDN library info for the SAFER technology to find where/how it is persisting its mastering info, but never followed it to a final, definitive answer. I was left with the impression that it, similar to the COM+ technology has its own catalog with currently ill-documented info on way to access in ways outside of the pre-planned interfaces.

The intent of Safer is for it to be applied from AD in GPOs. Using it with transportable definitions on stand-alone machines seems to have been outside of the design scope.

The registry key trees with \Policy\ in them are volatile, meaning that they are refetched by the sce policy engine. Changes that you manually make in these are subject to overwriting based on what the group policy engine sees as appropriate. The exact tie-in of the Safer extension to the policy system is also not clearly doc'd in today's admin-level writeups.

It sounds like you have progressed down this road to about the same roadblocks where I have stalled out.

--

Roger Abell
Microsoft MVP (Windows Server System: Security)
MCSE (W2k3,W2k,NT4) MCDBA
<BillMadison@nosspam.com> wrote in message
news:6e3n30951gn6n83v49v4rnqvnvlhg9tium@4ax.com...
> Roger,
>
> I have done some further testing and have come up empty. The result when
importing the exported
> registry files is that while apparently the restrictions are applied...you
can't see them in the mmc
> editor.
> That to me is not acceptable since I have to be able to see the settings
in future when I have to
> make adjustments.
>
> The thing is...when making new path rules these settings get written to a

microsoft.public.windowsxp.security_admin: Re: What program is used to write events to the event log??????

```
temporary branch in the
> registry in two locations ( the "GROUP POLICY OBJECTS")
>
> [HKEY_USERS\***insert ADMIN SID
here***\Software\Microsoft\Windows\CurrentVersion\Group Policy
>
Objects\LocalMachine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifie
rs]
>
> [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy
>
Objects\LocalMachine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifie
rs]
>
> These directories disappear when you do a logoff and log back on. The only
reference to these
> settings that remains are the ones in the HKEY local Machine.
>
> I have also tried exporting the entire group policy objects directory from
both these registry
> locations without duplicate entries and importing them in a new install,
logging of and logging back
> on and still I dont see these entries.
>
> If MS didn't include or can provide some way in which admins can exported
"path rules" then that
> means that which each new install you have to manually add them and that
is ...YAWN...a very
> tedious affair.
> So if you or anyone else knows some MS programmers or such and contact
them about this issue I will
> have to let this slip for a while.
>
> They can hardly expect me to install file/registry watchers and such to
monitor dll access, file
> creation, file deletion, registry key creation, accessing stamps and GOD
knows whatever action is
> taken from the moment you click apply when creating a new path rule.
>
> Kind Regards,
> J
>
>
>
> On Tue, 24 Feb 2004 01:26:06 -0700, "Roger Abell [MVP]"
<mvpNoSpam@asu.edu> wrote:
>
> >Hi J,
> >
> >I believe that the event logging functionality is implemented as
> >a part of services.exe
> >It may be that part of one of the mechanisms that may be used
> >to get an event message into the logs is what is actually blocked.
> >
> >You have gone about as far in trying to decipher how Safer is
> >persisting its settings as have I to date. I have seen as of yet
> >no references that detail how to export Safer settings so that
> >they are transportable, but I have searched, and have seen this
> >asked a few times (in NGs frequented by MS staff) with no answer.
> >I would be interested in your further experiments, as it has been
> >on my to-do (but not of urgent need) list.
> >
```

Re: What program is used to write events to the event log??????

microsoft.public.windowsxp.security_admin: Re: What program is used to write events to the event log??????

```
> >Regards,
> >Roger
> >
> >
> ><BillMadison@nospam.com> wrote in message
> >news:bagl30hqcsuvhu73n0s7qd2gimjp3ttqtq@4ax.com...
> >> Hi All,
> >>
> >> Been testing software restriction policies on virtual PC for the last
> >>couple a days and have
> >> encountered a minor problem.
> >>
> >> I have now created a deny all exe policy with certain "allow only
> >>exe's"
> >>that windows needs in
> >> normal operation.
> >> The problem however is that in a normal user account everything works
> >>ok
> >>but for one
> >> issue....whenever there is an exe being started it normally writes this
> >>event to the event log so as
> >> admin you can see what program or exe it was that was about to get
> >>started.
> >> After applying my restrictions I now don't see these events in my log
> >>anymore so that means that one
> >> exe is being denied from writing to the log.
> >>
> >> Now my question ofcourse,...what exe or program is used to write these
> >>events to the event log?
> >>
> >> Also, a few days ago I posted a question about wether these policies
> >>could
> >>be exported...the
> >> question remained unanswered then but I have now found a way to do it
> >>(maybe....)
> >>
> >> The thing is, these policies get written to three different parts of
> >>the
> >>registry
> >>
> >> [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group
> >>Policy
> >>
> >>
> >>Objects\LocalMachine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifi
> >>e
> >>rs]
> >>
> >>
> >>
> >>[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifie
> >>r
> >>s]
> >>
> >> [HKEY_USERS\***insert ADMIN SID
> >>here***\Software\Microsoft\Windows\CurrentVersion\Group Policy
> >>
> >>
> >>Objects\LocalMachine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifi
> >>e
> >>rs]
> >>
```

Re: What program is used to write events to the event log??????

microsoft.public.windowsxp.security_admin: Re: What program is used to write events to the event log??????

```
> >> So, normally you would think that by exporting these and reimporting
them
> >> in a default install would
> >> be sufficient for these policies to be applied on a new installation.
> >> Would I be correct in that
> >> assumption????
> >>
> >> I noticed that each path rule I created has an unique GUID associated
with
> >> it but when using the
> >> search function it can only be found in the registry at the three above
> >> mentioned registry branches.
> >> Does this then mean that they will work on a new machine when importing
> >> them since no other
> >> reference of these GUIDs can be found on the system.
> >> I even searched my harddrive to all files with a text containing one of
> >> these gui's to see if there
> >> would be a place where windows stores these GUID's as a reference and
also
> >> came up empty. Maybe they
> >> are just created as GUIDS for the sole purpose of creating a unique
string
> >> each time under these
> >> registry keys but thats only my logical conclusion to this and I could
> >> ofcourse be wrong.
> >>
> >> Anyway, thats about all I wanted to ask for now,...and as always I hope
> >> someone who has read this
> >> till the end and can provide some more details then I would be much
> >> obliged.
> >>
> >> Kind Regards,
> >> J
> >>
> >
>
```

Re: What program is used to write events to the event log??????