

Re: Firewall Client Question

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa.clients/2004-06/0014.html>

From: Mike (michael.s.sprauer_at_doc.state.or.us)

Date: 06/03/04

Date: Thu, 3 Jun 2004 08:36:18 -0700

I have to disagree. The software install is turning off inheritance.
"Jim Harrison [MSFT]" <jmharr@online.microsoft.com> wrote in message
news:OYNBOBPSEHA.1340@TK2MSFTNGP12.phx.gbl...
> *The default registry and file permissions are outside the scope of a
single product.*
> *If you find that "Everyone" has R/W access to the registry, then you have
larger issues, because this isn't the default.*
> *The "All Users" location is intended to be exactly that; a place where all
users can store and modify common data,such as firewall
> client configuration.*
>
> --
> *Jim Harrison [ISASE]*
> *Read the help, books and articles!*
>
> *This posting is provided "AS IS" with no warranties, and confers no
rights.*
>
>
> *"Mike" <michael.s.sprauer@doc.state.or.us> wrote in message
news:eY5kzzNSEHA.1396@TK2MSFTNGP12.phx.gbl...
> Not correct are users are not Local Admins or even Power Users and they
have
> full control.*
> *Inheritance is turned off by default on the file location (All Users) and
> the Registry Key and Everyone Full Control.*
> *Maybe you could address the above. Which has been the question from the
> beginning as well as my prior post.*
> *I must admit I'm only using the Technet version to test with which doesn't
> take service packs, so unless Microsoft has addressed these permissions
and
> the program requiring them it is a big hole.*
> *Thanks for your help Jim.*
> *"Jim Harrison [MSFT]" <jmharr@online.microsoft.com> wrote in message
> news:%23fzNiIASEHA.2552@TK2MSFTNGP11.phx.gbl...
> > Hi all,
> >
> > Wspecfg.ini is application-specific and does not apply to the FWC itself.*

> > *Additionally, locking down that folder will, as you pointed out, cause the*
> *FWC to fail in the 6-hour updates, eventually causing*
> > *complete disconnection from the ISA.*
> >
> > *The problem here is that his users are local admins on the client machines*
> *and regardless of the controls you place on the folders,*
> > *etc., they can take ownership and change them back.*
> >
> > *Since you don't have full control over user actions (again; the "local admin issue), the better place to address the issue of users*
> > *and "illegal" applications is via company policy.*
> > *The ISA logs will clearly show what users are changing their "local" FWC policies and provide a valid reference for "official action".*
> >
> > --
> > *Jim Harrison [ISASE]*
> > *Read the help, books and articles!*
> >
> > *This posting is provided "AS IS" with no warranties, and confers no rights.*
> >
> >
> > *"Mike" <michael.s.sprauer@doc.state.or.us> wrote in message*
> > *news:ODjHOVaQEHA.2100@TK2MSFTNGP11.phx.gbl...*
> > *Permissions is the only way I see to lock FWC down on W2k and above.*
> > *Q Article 328256 talks about XP requiring Administrative rights to do the*
> > *Update. As close to any thing I could find concerning rights.*
> > *A thought, or maybe hope, SP2 will update the client to install where*
> > *restricted users cannot modify the config of the client.*
> >
> > *What we're doing is this to permissions:*
> > *ALLUSERSPROFILE\Application Data\Microsoft\Firewall Client*
> > *Turn Inheritance on at the Folder and change Everyone to Read*
> > *HKLM\Software\Microsoft\Firewall Client*
> > *Turn Inheritance on at the Key and change Everyone to Read.*
> >
> > *They won't be able to update which could cause issues such as slowness to*
> > *be*
> > *denied access to a read icon on the taskbar, if visible, due to not being*
> > *able to update.*
> >
> > *A trick would be to clone your mspclnt.ini to the wspcfg.ini and place it*
> > *in*
> > *the ALLUSER location. With this file there FWC should not try to update*

> *and*
>> *use the wspcfg.ini configuration. This will require manually placing*
and
>> *updating (if needed) this file.*
>>
>> *Please let me know if this is of any help or if you uncover anything.*
>> *"Tony" <anonymous@discussions.microsoft.com> wrote in message*
>> *news:56E26B60-4FF5-4474-8A05-A24437E56B28@microsoft.com...*
>>> *To add to my question;*
>>>
>>> *I have configured the firewall client to block IM type applications.*
It
>> *occured to me that if the user simply looks in his control panel he can*
>> *disable the client hence bypassing any ruleset which I've set in the*
> *client*
>> *ini.*
>>>
>>> *Is there some way without using a group policy to limit access to the*
>> *control panel, for me to stop these kinds of users from changing or*
>> *disabling the client? I have been researching through most of the day,*
if
> *an*
>> *answer is out there I haven't found it yet.*
>>>
>>> *Can anyone help?*
>>
>>
>>
>
>
>