

# Re: Question on software install and event log security

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group\\_policy/2005-06/msg00053.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2005-06/msg00053.html)

---

- *From:* "Tommy Nguyen" <[tommyboy\\_nguyen@xxxxxxxxxxxxx](mailto:tommyboy_nguyen@xxxxxxxxxxxxx)>
  - *Date:* Fri, 3 Jun 2005 13:30:35 -0700
- 

Steve,

Thanks for the quick response. I don't think that publishing or assigning the software is a good solution due to the fact that all users must be able to install software continuously throughout the day. Your suggestion on modifying the user right for "manage auditing and security log" sounded like a good idea until I noticed that the policy does not have the option to deny a group. The policy only allows. (Hope that made sense).

Does anyone know what the policy on Windows Installer where it states "always install with elevated privileges" mean?

Tommy

"Steven L Umbach" <[n9rou@xxxxxxxxxxxxxxxxxxxxx](mailto:n9rou@xxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:eXW1OTGaFHA.2900@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:eXW1OTGaFHA.2900@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

> When you add a user to the local administrators group then yes they are all

> powerful on the computer. You might be able to avoid such by publishing or > assigning .msi software packages to the users or computers which will allow

> those packages to be installed without the user being local administrator.

> If that is not an option for some reason one thing I think you could try is

> to modify the user right for "manage auditing and security log" by removing

> administrators group and possibly adding specific domain global group or

> domain admins. You would want to do such at the domain/OU level so that the

> local administrator could not change that user right via Local Security

> Policy. Note that local administrators can unjoin a computer from the

> domain and possibly rejoin it up to ten times. --- Steve

>

>

>

> "Tommy Nguyen" <[tommyboy\\_nguyen@xxxxxxxxxxxxx](mailto:tommyboy_nguyen@xxxxxxxxxxxxx)> wrote in message

> [news:%23qCkclFaFHA.2520@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%23qCkclFaFHA.2520@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Re: Question on software install and event log security

>> Hello all,  
>>  
>> I must meet two requirements:  
>>  
>> 1. Files and folders are audited so therefore the audit trails  
(event  
>> logs) must be available to administrators only.  
>> 2. All users must be able to install software on all computers,  
>> including servers.  
>>  
>> Goal #2, can be easily implemented by adding the Domain User group to  
the  
>> local administrator group, therefore allowing all users to install  
>> software.  
>> However by adding them to the local administrator group they are allowed  
>> to  
>> view the security event log.  
>>  
>> I have looked into group policy but have not found the appropriate  
>> policies  
>> that will allow me to meet these requirements.  
>>  
>> I am at a road block as to how to implement both of these requirements.  
I  
>> have searched and have not found the answer. Can someone please point  
me  
>> in  
>> the right direction. Thanks.  
>>  
>> Tommy  
>>  
>>  
>  
>

---

• *Follow-Ups:*

- ◆ *Re: Question on software install and event log security*  
◇ From: Steven L Umbach

• *References:*

- ◆ *Question on software install and event log security*  
◇ From: Tommy Nguyen
- ◆ *Re: Question on software install and event log security*  
◇ From: Steven L Umbach

- Prev by Date: *Re: How to publish printers*

Re: Question on software install and event log security

- Next by Date: ***Re: Local Security Policy – Win2K3 SE***
- Previous by thread: ***Re: Question on software install and event log security***
- Next by thread: ***Re: Question on software install and event log security***
- Index(es):
  - ◆ ***Date***
  - ◆ ***Thread***