

## Re: Automatically making AD users local administrators on computers in SBS 2003

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-04/msg04920.html>

---

- *From:* "Rick F" <[rick.REMOVE@xxxxxxxxxxxxxxxxxxxx](mailto:rick.REMOVE@xxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sun, 17 Apr 2005 20:56:52 -0500
- 

You have to remember that even though you give the user a different account to install software and then they logoff and back in as themselves, it still might not work if the software does not have the "Designed for XP/2000" logo certification. If it isn't, you are going to have to touch the workstation to figure out what file or registry permissions need to be changed to allow it to work.

—

Rick Faria – MCSE / A+  
RDF Technical Services – [www.rdfts.com](http://www.rdfts.com)  
Email: support at rdfts dot com

"Bob Genestet" <[bob\\_genestet@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:bob_genestet@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:%23oPC005QFHA.2996@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%23oPC005QFHA.2996@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

- > Thanks everyone, for the excellent discussion.
- > I am in total agreement that it is best practice to adhere to a "least is best" when assigning user rights. It used to be that a company policy was enough to prevent misuse, but not anymore given the increasing presence of malicious software installing itself by impersonating the currently logged on user.
- > My goal is to give some control back to those clients requesting it and at the same time protect them from unwanted malicious software. I believe that implementing firewalls, antivirus, antispyware, patching, and company usage policy are fundamental to good security. These are relatively automatic and do not require an administrator's ongoing presence.
- >
- > I think I will set up an account as Chad suggested using option 2 and provide the client this account and password. When an employee needs to install some new software that requires local administrative rights, they can use this special local administrator account. I suppose you could set up everyone with a second account having local administrative rights to use for software installation. The incentive to not use their local administrative account except for software installation would be their email not available under that account.
- >
- > I would like to find a simpler, more transparent method that would allow

Re: Automatically making AD users local administrators on computers in SBS 2003

- > programs that require local administrative rights to install correctly
- > from a logon script. Is anyone familiar with EPAL (Elevated Privileges
- > Application Launcher)?

>  
> <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=CF3CC921-9B8E-4266-A905-2E2A>

> I also ran across this product which might provide a solution.

> [http://www.emco.is/tutorials/runasprofessional/how\\_to\\_create\\_runas\\_action/how\\_to\\_create\\_runas\\_action.html](http://www.emco.is/tutorials/runasprofessional/how_to_create_runas_action/how_to_create_runas_action.html)

> I suppose Microsoft SMS offers a solution to this problem although a  
> little pricey for my clientele.

> Thanks to all,  
> Bob

> "Chad A. Gross [SBS MVP]" <chad.gross@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in  
> message [news:uqNcNt3QFHA.244@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uqNcNt3QFHA.244@xxxxxxxxxxxxxxxxxxxxxxxx)

>> But that gets cumbersome . . . e.g. you've already deployed your SBS &  
>> workstations (via ConnectComputer) – and three months later you have a  
>> new user that you want to be a local Admin on all workstations (which  
>> I'll point out up front isn't a great idea anyway . . . stupid insecure  
>> apps . . . but I digress . . . ) There's no additional benefit to  
>> re-running the ConnectComuter wizard on each machine – because if you  
>> have to touch each workstation, why not just add the user as an Admin  
>> versus running the ConnectComputer wizard?

>> In this scenario, you have three options – and they'll all involve  
>> touching each workstation – but you'll be good to go moving forward.

>> 1) On each PC, add the INTERACTIVE group to the Administrators group.  
>> This will automatically give each user that logs in local Admin rights.  
>> Downside is that if you ever want a user to not have local admin rights,  
>> you won't be able to restrict them as long as you have this  
>> configuration.

>> 2) Create a Security Group within AD (e.g. Local Admins). On each  
>> workstation, add the domain Local Admins group you created to the local  
>> Administrators group. Then on your SBS, add your existing users to the  
>> Local Admins group, and create a new user template that includes Local  
>> Admins group membership. When you create a new user, use the custom  
>> template and they'll be included in the Local Admins security group,  
>> which will give them local admin rights on the machines where you added  
>> the Local Admins group to the local Administrators group.

>> 3) Preferred solution: Don't give users local admin rights. Find  
>> your problem apps that don't run as a restricted user and start nagging  
>> the vendor. Ask why they find exposing your business to undue risk as a  
>> justified business practice on their part. Find what directories / reg  
>> keys those apps want access to and tweak the permissions accordingly to  
>> allow restricted users to be able to access those locations (and thus run

Re: Automatically making AD users local administrators on computers in SBS 2003

>> the problem apps).  
>>  
>> --  
>>  
>> Chad A. Gross – SBS MVP  
>> SBS ROCKS!  
>>  
>> www.msmvps.com/cgross  
>> www.gosbs.org  
>>  
>>  
>> Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP] wrote:  
>>> Run the connect computer wizard and that's exactly what is done.  
>>>  
>>> Bob Genestet wrote:  
>>>> Is there any way to automatically add new AD users as local  
>>>> administrators to each client computer. I tried to rerun the  
>>>> "Network Configuration Wizard" to add newly added multiple AD users  
>>>> to client computers except that the wizard will not run again if it  
>>>> detects the computer is already a member of the domain. It would be  
>>>> nice to have the server to automatically assign local rights when a  
>>>> new user logs on at a computer. Is this possible? Thanks,  
>>>> Bob  
>>  
>>  
>  
>

---

• **References:**

- ◆ **[Automatically making AD users local administrators on computers in SBS 2003](#)**  
    ◇ From: Bob Genestet
  - ◆ **[Re: Automatically making AD users local administrators on computers in SBS 2003](#)**  
    ◇ From: Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]
  - ◆ **[Re: Automatically making AD users local administrators on computers in SBS 2003](#)**  
    ◇ From: Chad A. Gross [SBS MVP]
  - ◆ **[Re: Automatically making AD users local administrators on computers in SBS 2003](#)**  
    ◇ From: Bob Genestet
- 
- Prev by Date: **[Re: It pays to read the help once in a while...](#)**
  - Next by Date: **[Re: Internet Connection](#)**
  - Previous by thread: **[Re: Automatically making AD users local administrators on computers in SBS 2003](#)**
  - Next by thread: **[SBS2003 Exchange Sent Mail is being Rejected](#)**
  - Index(es):
    - ◆ **[Date](#)**
    - ◆ **[Thread](#)**