

# Re: remove local admin rights

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group\\_policy/2008-03/msg00150.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2008-03/msg00150.html)

---

- *From:* Cindy B <benedett@xxxxxxxxxxxx>
  - *Date:* Thu, 6 Mar 2008 12:03:01 -0800
- 

thanks for your info – I finally did get the Restricted group to work –  
I kind of struggle with the scripts.... :-)

—

Cindy B

"Lanwench [MVP – Exchange]" wrote:

Cindy B <benedett@xxxxxxxxxxxx> wrote:

Hi–

I have set up a policy to make all domain users Local Admins – I apply this policy when we need to push out updates to the workstations, so the users can install with their profile. It's been great – saves us a lot of Hands on time.

Well – sure, but if you use WSUS and GP to distribute updates & software, this shouldn't be something you need to do regularly. Users shouldn't require admin rights.

Here's the problem... even though I remove the policy after a day or 2, I just realized that the setting stayed in place. All domain users have remained in the local Admin group... THAT'S NOT what I wanted. I thought when I removed the policy – it would remove them from the Admin group.

Is there is way with a new GP to remove them from that Admin group?  
HELP! Thanks for your time or sharing your knowledge!

I'm not sure of the exact answers to your questions, but thought I'd post anyway, because instead of using restricted groups, here's what I do –

Set up AD groups called LocalAdmin, LocalPowerUser, to make this easier. You

## Re: remove local admin rights

can also create one for Remote Desktop access, too – in this case, RDaccess

The batch file would have this:

```
.....  
net localgroup administrators DOMAIN\localadmin /add  
net localgroup power users DOMAIN\localpoweruser /add  
net localgroup remote desktop users DOMAIN\RDaccess /add
```

.....

You can create/link a new GPO at the appropriate OU where your computers live (if you haven't created custom ones, you'll need to – unless you're using SBS, which creates its own hierarchy).

Edit the GPO – go to Computer Configuration \ Windows Settings \ Scripts (startup/shutdown)

Double-click Startup, click Add

Copy the batch file you created to the clipboard, then paste it in the window here

Exit/apply/ok/finish whatever

All the computers in this OU should have the startup script applied when they restart, and you can now control all this at the server. Add users or groups to the AD "LocalAdmin" group and remove them when you wish.

Restricted groups are useful sometimes but I'm old fashioned and prefer the granular control I get with this technique.