

# Re: Secure an Administrative Group

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2008-02/msg01025](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-02/msg01025)

---

- *From:* "Richard Mueller [MVP]" <[rlmueller-nospam@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:rlmueller-nospam@xxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sat, 23 Feb 2008 18:57:53 -0600
- 

When a computer is joined to the domain, the group "Domain Admins" is added to the local Administrators group. This allows members of this group to add/remove users to the local Administrators group. You could add another domain group to the local Administrators group to give users that do not have "Domain Admin" privileges admin privileges on the local machines. This can be done with Restricted Groups or a VBScript program that adds the domain group to each computers local Administrators group.

A group can be given permission to add computers to the domain by granting the following privileges:

Reset Password

Validated write to DNS host name

Validated write to service principal name

Write Account Restrictions

To grant permission to create, edit, unlock, disable, and change passwords, but not delete users, you may need to deny the delete privilege. Deny overrides grant. Someone else may have more detail.

—  
Richard Mueller  
Microsoft MVP Scripting and ADSI  
Hilltop Lab – <http://www.rlmuellet.net>  
—

"a\_user" <[auser@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:auser@xxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
<news:3F227F5C-A4E4-4AC5-8AD8-373A99AA5A95@xxxxxxxxxxxxxxxx>

I meant to also add to this we need to ability to have our helpdesk staff be able to add a user to the local administrator group on desktops and laptops

## Re: Secure an Administrative Group

without them having domain admin rights.

"a\_user" wrote:

Similar to a previous post I am looking for a guide to create a limited locked down group for AD administration for our HelpDesk group.

I want to allow very limited functionality. Namely the following:

- Allow joining of computers to domain (unlimited, more than 10 limit)
- Create users
- Edit users
- Unlock users
- Change user passwords
- Disable Users
- Create groups
- Edit group memberships

I do NOT want helpdesk group to have the ability to delete objects like users, groups or computers.

I tried using the delegation wizard but there are far too many options when trying to get granular and not using just the default option of adding a computer to a domain.

I tried adding the helpdesk group to the domain security settings and enabling write permission and disabling delete options. Users in this group can still delete user accounts, groups and computers from different OU's.

Is there a guide somewhere that steps through this process? I can't believe it should be this hard or that nobody else has done this before but the documentation I have been able to find has been very limited without supplying irrelevant or overwhelming and confusing information.

Please help.

Thanks!!