

Re: How to prevent some specific Domain Admin Accounts from creating USERS, Groups, OUs

## Re: How to prevent some specific Domain Admin Accounts from creating USERS, Groups, OUs

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2008-01/msg00168.html>

---

- *From:* Meinolf Weber <meiweb(nospam)@gmx.de>
  - *Date:* Fri, 4 Jan 2008 17:50:23 +0000 (UTC)
- 

Hello coco07@xxxxxxxxxx,

See your other posting and please do not multipost. If you need more NG's you can crosspost so all replies will go to all NG's.

Best regards

Meinolf Weber

Disclaimer: This posting is provided "AS IS" with no warranties, and confers no rights.

\*\* Please do NOT email, only reply to Newsgroups

\*\* HELP us help YOU!!! <http://www.dts-l.org/goodpost.htm>

How Can I PREVENT some specific Domain Admin Accounts from creating User Account, Security Groups, OUs and modifying those object properties??

These Domain Admin Account handle administrative tasks over Domain Controllers Servers such as: Install/Uninstall Software, Add Server Roles, Promote New Domain Controller, Configure AD Replication, DNS Configuration, DHCP Configuration, Manage Event Viewer, Troubleshooting related Tasks, Restart Services, etc... As far as I know the only way they can do all those things in a domain Controller Server is making those Users Account Domain Admins....

Im almost sure that the "Delegate Control" Concept doesnt work in this case, please correct me if Im wrong....

I Tried Restrict loading of Active Directory Users & Computers snap-in into MMC.... but the users already know how to manage Users or Groups using Command - Line Tools or Scripts....

I Tried removing those Account from Domain Admins Group.... I created a group where I place all of those user accounts, then I placed these group as member of other Built In Security Group Such as: DHCP Administrators, DNS Administrators, Server Operators, Network Configuration Operators, etc.... I Also gave most of the Privileges

Re: How to prevent some specific Domain Admin Accounts from creating USERS, Groups, OUs

that Domain Admin Group Has... and yes.. I prevented these users from managing Users, Groups or OUs.. but that also I prevented these users from Installing/Uninstalling software, Restarting Services, Adding Roles, they couldnt handle AD Replication, etc.... So at the end it didnt work the way I wanted....

And finally I tried to place these accounts in two Security Groups: Domain Admins and a group called "LEVEL1". Using ADUC Permissions TAB, I configure "LEVEL1" group with DENY permisiions over USER, GROUP an OUs Objects... hoping that "the most restrictive permission would apply"... but sadly... it didnt work neither....

So I really hope you can guide how to achieve this goal.