

# Re: Account Operators accessing other account operators

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-02/msg00910](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-02/msg00910)

---

- *From:* "Joe Richards [MVP]" <[humorexpress@xxxxxxxxxxxx](mailto:humorexpress@xxxxxxxxxxxx)>
  - *Date:* Fri, 10 Feb 2006 00:42:35 -0500
- 

Bingo.

and I agree, don't use acc ops. It is there for legacy NT4 migrations. Once you are done with that you should move to fully delegated accounts where the exact permissions needed are delegated.

In the meanwhile, in one of those articles it will tell you how to disable the protection of adminsldholder over acc ops.

BTW, if the acc ops are bright enough, they can give themselves Domain and Enterprise Admin rights anyway. That is why you want to use delegated accounts for AD data admins.

joe

--

Joe Richards Microsoft MVP Windows Server Directory Services  
Author of O'Reilly Active Directory Third Edition  
[www.joeware.net](http://www.joeware.net)

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

Jorge de Almeida Pinto [MVP] wrote:

it is better not to use the account operators group, but to use your own group and delegate the correct permissions on an OU that applies to the correct objects in that OU. If you go that way, make sure to remove the account from the account operators group as that is a protected group by AD (to be more precise adminsldholder). after that reset the admincount attribute to NOT SET and enable permissions inheritance on the objects.

for more info see:

<http://blogs.dirteam.com/blogs/jorge/archive/2005/11/16/86.aspx>

ADMINSHOLDER:

## Re: Account Operators accessing other account operators

Every hour, the Microsoft Windows domain controller that has the primary domain controller (PDC) emulator operations master role verifies the ACLs on members of these administrative groups and compares them to the ACL on the AdminSDHolder object. If the ACL that is on the AdminSDHolder object is different, the ACLs on the members of the administrative group are reset to match the ACL on the AdminSDHolder object.

For more info on the ADMINSDHOLDER object see the following related KB articles (not all may apply to your situation!)

Description and Update of the Active Directory AdminSDHolder Object

--> MS-KBQ232199 (<http://support.microsoft.com/?id=232199>)

AdminSDHolder Thread Affects Transitive Members of Distribution Groups

--> MS-KBQ318180 (<http://support.microsoft.com/?id=318180>)

Delegated permissions are not available and inheritance is automatically disabled

--> MS-KBQ817433 (<http://support.microsoft.com/?id=817433>)

AdminSDHolder Object Affects Delegation of Control for Past Administrator Accounts

--> MS-KBQ306398 (<http://support.microsoft.com/?id=306398>)

Security tab of the adminSDHolder object does not display all properties

--> MS-KBQ301188 (<http://support.microsoft.com/?id=301188>)

"You do not have sufficient permissions in the Domain" error message occurs and Exchange Setup does not respond

--> MS-KBQ319966 (<http://support.microsoft.com/?id=319966>)

Certification Authority configuration to publish certificates in Active Directory of trusted domain

--> MS-KBQ281271 (<http://support.microsoft.com/?id=281271>)