

# Re: Delegation dilemma

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-01/msg01352](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-01/msg01352)

---

- *From:* "Paul Williams [MVP]" <ptw2001@xxxxxxxxxxxx>
  - *Date:* Mon, 23 Jan 2006 06:13:42 -0000
- 

- > In one or another way the administrators of all these components have
- > access to domain controller data and can escalate their privileges up to
- > Domain Admins or affect security of the controllers in another manner.

This is often the case. The difficult part is getting everyone out of this way of thinking and into the newer model as recommended in the k3 deployment guide.

- > 1. Give all the administrative tasks (SMS+MOM+SAN+ ...) to Domain Admins.
- > That will keep all the security control in one hands but will end up with
- > overloaded broad-profile AD admins.

Don't go down this route if you can avoid it. I've got many customers in this position, and it's very difficult (costly) to get them out again.

- > 2. Delegate the tasks, like SMS or MOM management, to highly trusted individuals. That will spread the security control over a group of people but diminish the load on AD admins

This is the recommended way. This is usually relatively easy to a point. Branch office deployments start to mess this up.

Realistically, your SMS and MOM servers are going to be member servers. SMS is easy to delegate, you create a bunch of groups, e.g. SMSAdmins, SMSQueries, etc. and grant the necessary rights. I would also place SMSAdmins in the local administrators group of the SMS Primary and Secondary servers.

The complexities arise when you start installing software on DCs. If you are lucky enough to have dedicated DCs, you are much more likely to succeed in this model.

One thing I will say is plan this thoroughly, and don't rush it. Document your decisions and especially any changes and deviations away from the original design. Grant additional rights sparingly, and face all opposition strongly, with the unbudging opinion that the person in question DOES NOT

## Re: Delegation dilemma

need to be an administrator in the traditional sense.

You will probably end up with a mixture of both your points. If so, keep the administrative members to a minimum, and try and only grant trusted users membership to these groups. Forget about legacy groups like account operators, server operators, etc. and create your own and delegate only the necessary permissions. Think about Quest or NetIQs products for managing permissions in the AD if you can. Otherwise, get a web-based front end for the people who create users and mailboxes, etc. and do it all through scripts/ code as opposed to the admin tools which often require more rights than necessary.

Persevere!

—

Paul Williams

Microsoft MVP – Windows Server – Directory Services

<http://www.msresource.net> | <http://forums.msresource.net>

---

### • *References:*

#### ◆ *Delegation dilemma*

◇ *From:* boomboom999

- Prev by Date: *Re: NETLOGON.DNS*
- Next by Date: *Re: Roaming Profile question*
- Previous by thread: *Delegation dilemma*
- Next by thread: *Re: Computers with same SID in Win 2003 AD*
- Index(es):
  - ◆ *Date*
  - ◆ *Thread*