

## Re: Where is Local Group Assignment Stored?

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-03/msg00033.html>

---

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
  - *Date:* Tue, 6 Mar 2007 13:45:19 -0700
- 

"Will" <westes-usc@xxxxxxxxxxxxxxxx> wrote in message  
[news:rbadneANGavSXHDYnZ2dnUVZ\\_tmknZ2d@xxxxxxxxxxxxxxxx](news:rbadneANGavSXHDYnZ2dnUVZ_tmknZ2d@xxxxxxxxxxxxxxxx)

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message  
<news:%23dKDvYAYHHA.3848@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Right. However, simply giving it a long password (I use a tool the genreates, given n a pseudo-random phrase n char long). It is more simple to monitor for password change, logon/use than for change to memberships of a number of groups used to guard the user rights.

Is there a simple tool available that will monitor logins, and that would –  
for example – send you an e-mail every time an attempt to login with the builtin administrator account takes place?

I'm all for leaving the account intact as long as I can get immediate notification when someone starts to try to break in. In fact, it might serve as a kind of honeypot as long as the notifications are immediate and reliable.

You might want to look into what MS is doing with System Center (and its heritage in MOM). There are third-party also, but what MS is doing with security event log centralization does an end run around admins (or those with admin) attempting to disrupt what is in the per machine locally stored security log.

On a tangent, you might want to consider getting your powers that be to up the schedule for W2k to W2k3 upgrade. A number of issues in W2k were addressed with W2k3. For example, one can disable the built-in Administrator in W2k3, making it of use only for a safe mode boot local console login, and one can restrict use of the domain built-in in ways not designed into W2k.

Re the builtin as you have it, if it is set to require smartcard even if you do not have smartcards, what happens ?

Re: Where is Local Group Assignment Stored?

Roger