

## Re: UNLOCKING ADMINISTRATOR PASSWORD

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-11/0524.html>

---

**From:** Vanguard (*no-email\_at\_post-reply-in-newsgroup.nix*)

**Date:** 11/06/03

Date: Thu, 06 Nov 2003 05:54:33 GMT

Karl Levinson [x y] mvp wrote:

- > *It's still not a bad idea. Every little bit helps. But you won't*
- > *necessarily die if you don't do it. Lots of people do this without*
- > *problems. It should not cause problems with running Runas. IIRC you*
- > *get a chance to enter which login ID you want to Run As.*
- >
- > *Because the SID stays the same, some people use special tools as*
- > *mentioned before to disable the default Admin account and create new*
- > *ones, and also use RestrictAnonymous where possible to try to reduce*
- > *account enumeration [difficult to do very effectively on domain*
- > *controllers]. If you do this, then the real admin account can't be*
- > *guessed by SID [although someone doing this could easily just try*
- > *every possible SID to find your login IDs].*
- >
- > *Really, no one should be using the "Administrator" account, assuming*
- > *it is a shared account. Ideally, each person, admin or otherwise,*
- > *gets one or more login IDs that uniquely identify them and only them*
- > *[and what has been done to a system by them].*
- >
- >
- > *"Vanguard" <no-email@post-reply-in-newsgroup.nix> wrote in message*
- > *news:PU%pb.81873\$ao4.249228@attbi\_s51...*
- >
- >> *Other than using a complex password, is it still advisable to rename*
- >> *the "Administrator" account to something else (since it should still*
- >> *retain the same SID) to also thwart hacking? Does renaming the*
- >> *Administrator account result in other problems, like when using*
- >> *RunAs?*

I don't use the Administrator account. Instead I use my own userid that is in the Administrators group. I do copy my profile atop the Administrator's profile (right-click My Computer, User Profiles, Copy To, set permissions to Administrator for the profile, and do the copy) so if I do need to use the Administrator userid then I get a familiar desktop and Start menu (I had to relocate the My Documents folder to eliminate copying it all into the Administrator's profile using this method). I figure you always need a backup admin account, so I leave the Administrator account alone (mostly). Actually, at one time, I had

both accounts using the same profile path through a registry edit (i.e., change their profile paths to point to the same one) but I figured that if the profile got screwed up in one account then it was screwed in the other and I preferred having separate but duplicated profiles as a backup. I never encountered an error with sharing a profile across multiple userids but I just didn't feel comfortable with it, always expecting that something could happen to really fark me up.

If I rename the Administrator account to a different name (but with same SID), will the Recovery Console still work (when it has you log under "Administrator" which would now have a different name)? According to KB # 243330, a SID of S-1-5-domain-500 is for the Administrator account, so hopefully the Recovery Console uses that one, too, regardless of whatever it got renamed to.

Renaming Administrator to a different name is probably as far as I'd go to provide some protection. I'd feel uncomfortable disabling the SID for the standard Administrator account (whatever it was named) and using alternate SIDs as administrator accounts (seems that I could do that just by creating userids in the Administrators group and disabling the Administrator account, however that's done). If, and I only say if because I doubt that I would ever go that far, but because it's one of those topics that pique interest (mostly in how to fathom how to fix stuff), is there an official Microsoft info on how to do this. I don't want to reveal anything that fledgeling hackers might find as a juicy target for attack that Microsoft itself doesn't reveal.

--

---

\*\*\* Post replies to newsgroup. E-mail is not accepted. \*\*\*

---