

## Re: Protect user accounts

**Source:**

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2004-05/1713.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2004-05/1713.html)

---

**From:** Chriss3 (noSpamHere\_at\_chrisse.se)

**Date:** 05/30/04

Date: Sun, 30 May 2004 02:49:29 +0200

Enable strong passwords in the password policy, set minimum password age this helps to protect in that way if some one take over an account the 'hacker' can't change the password. Use GPOs and Deny Logon Locally for users in OU1 to computers in OU2 and the other way around. Enable Audit and tack all logon/logoff events. Do not cache credentials. If you want to become really secure use smart cards!

--

Regards

Christoffer Andersson

No email replies please - reply in the newsgroup

-----  
<http://www.chrisse.se> - Active Directory Tips

"timpuri" <anonymous@discussions.microsoft.com> skrev i meddelandet  
news:14dc501c445a8\$ea069a20\$a301280a@phx.gbl...

> Hi

>

> In a sinqe-domain, single - forest impementation. How am I

> able to protect useraccounts from hacking. For example: I

> have a ou1 with users. I have another ou2 with users. I

> have a security policy that locks user account after 5

> failed logon attempns. Now if users in ou2 somehow would

> get to know (or guess) another username from ou1 and they

> wanted to do harm, they intentionally make five failed

> logons as a user in ou1 and the account is locked.

> I know

> - we can define the computers netbios name, where user

> only can logon

> - we can make gpos "log on locally"

> - we can make restricted group policy

>

> But still. If you are in the same domain and you know the

> username, you can try to logon and DCs' do as if defined

> in the domain policy.

>

> Thanks

>

> Timo