

## Re: How can I prevent an account from being locked out?

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2007-02/msg01324](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-02/msg01324)

---

- *From:* "Rich Raffenetti" <[rich@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:rich@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 14 Feb 2007 21:28:02 -0600
- 

Joe,

The root of the problem is that persons with no mathematics education are writing security guidelines. They write recommendations that, like you say, are totally unrealistic and without mathematical justification. Someone recommends a threshold of 10 and someone else comes along and thinks his guideline will be better if s/he halves the threshold. Pretty soon there's no room for fat fingers! The security folks pick up on a published guideline and are afraid that an auditor will question why their policy deviates from that which was recommended.

Our domain ran quite well for years with a lockout threshold of 20 with a minimum password length of 8. I was forced to change the threshold to 5 and now we have 700 lockouts per quarter with only about 3000 accounts. That's not bad enough but now they want to build or buy automated processes to notify people about the unnecessary lockouts. I suspect we have never seen an attempt at brute-force breakin. The lockout threshold is a good deterrent at any reasonable value (except for the collateral effects).

Thanks for writing your opinion on lockouts. It's good to know that there are thinking beings out there. I needed to write this. :-)

"Joe Richards [MVP]" <[humorexpress@xxxxxxxxxxxx](mailto:humorexpress@xxxxxxxxxxxx)> wrote in message [news:%23tgNA7HUHHA.1208@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%23tgNA7HUHHA.1208@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

There is no way to sidestep the lockout policy in a single domain. If you configure it, accounts will lock out. If you absolutely need this functionality for the domain ID you need a new domain with that policy.

I have to say though, 3 is ridiculously low and is totally not following the intent of lockout capability in the first place. The idea of lockouts is to prevent automated systems from guessing passwords. These systems submit tens, hundreds, or possibly thousands of requests every minute. Setting a policy that says 3 bad attempts is just punishing users who are making small mistakes versus adding any additional security to the environment. You should be able to easily set 25-40 bad attempts and reset after 5-10 minutes and your password length/aging policy should be easily

Re: How can I prevent an account from being locked out?

enough to handle the numbers to still give low possibility of cracking.

Additionally, depending on the security providers being used, I have seen a single bad logon attempt generate 3–5 bad attempts against a DC even though the user only entered the password once. The lowest I would consider for a lockout policy is about 15.

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>

Winston Smith wrote:

Before you answer – please read this. I have implemented a web-based tool which allows users to reset their password or unlock their account (Win2K Active Directory, XP Clients). I've got an AD account I'm using as a service account – users can log on anywhere, including their own machine, using this account. I've applied a User-Oriented Group Policy to this account which, upon logon, launches the Password Reset Page in Kiosk mode, prevents users from closing IE, and only allows Log Off when they CTRL+ALT+DEL. I've applied several other sundry security measures to this account which are not directly relevant to this problem I'm presenting. Suffice it to say – if you worked here and locked your account or forgot your network password, you'd be able to log on to your own machine using this account and unlock or reset your password – but other than that you wouldn't be able to do anything but log out again (to subsequently log on using your own credentials). The credentials/instructions to do this are displayed on the security screen after the CTRL+ALT+DEL, so if you've locked yourself out the solution will be right there for you. (Cool, eh?).

Anyways, the logon, the page, the process works a treat, but I have one minor problem. If a user passes a bad password with this account 3 times, the account gets locked out – that's the default domain policy and with all other accounts it's a good thing. However, I want this account, and only this account, to never lock. Unfortunately, this particular bit of policy is a Computer-Oriented Group Policy in AD, and since I want users to be able to log on anywhere using this account I can't override the lock out policy on every machine (Catch-22). I was hoping I'd find a solution within the net user command (I used net user to allow a blank

Re: How can I prevent an account from being locked out?

password on this account contrary to domain policy), or in ADSI Edit, but I haven't found a solution. I thought perhaps this could be done through LDAP, but my searches have revealed nothing. The best solution I can come up with, lacking a conventional solution, is to implement a script that runs constantly setting the badPwdCount value (via ADSI Edit) back to ZERO. This is sloppy, though – I consider this only a bridge to a better solution.

So. Thoughts? Questions? Solution?

Mods: I apologize if this isn't in the right forum. Please (of course) feel free to move it if necessary.

Thanks,

Winston