

## Re: Question on Account Lockout – Urgent

---

*Source:*

[http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active\\_directory/2007-08/msg00024.html](http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2007-08/msg00024.html)

---

- *From:* Brandon McCombs <[none@xxxxxxx](mailto:none@xxxxxxx)>
  - *Date:* Sun, 05 Aug 2007 16:39:29 -0400
- 

Abhi wrote:

Hi All,

We are in Windows 2000 mixed mode. User accounts are on Child domain. Now a days there is a huge increase in the number of account lockout calls that the helpdesk is receiving. The settings are like this,

Account lockout duration = 0 (an administrator must unlock the account) Account lockout threshold = 5 invalid logon attempts Reset account lockout counter after = 15minutes

I have tried to use account lockout tools to find out the root cause. I found that subsequent wrong credentials are being passed by the end users but according to them they have typed the password only once, it is also noted that while they are working all of a sudden their accounts are getting lockedout!

I have enabled netlong logging on PDC Emulator but it did not give any hint. I was also referring to the technet article,

<http://technet2.microsoft.com/windowsserver/en/library/f3abc878-3eab-4eaf-9bff-9f0d058d4fc31033.mspx?>

there are a few things I want to clarify,

Article says Many programs cache credentials or keep active threads that retain the credentials after a user changes their password.

1)How do I find out the applications which are creating problems? May be IE I if the user selects the option save password), can anyone help me in this?

2)Bad Password Threshold is set too low: This is one of the most common misconfiguration issues. Many companies set the Bad Password Threshold registry value to a value lower than the default value of 10. If you set this value too low, false lockouts occur when programs automatically retry invalid passwords. Microsoft recommends that you leave this value at its default value of 10. For more information, see "Choosing Account Lockout Settings for Your Deployment" in this document.

In our environment Bad Password Threshold is set to 5. But my question is regarding the value 10 which is given in the article. Is there any specific reason why a value of 10 is recommended? and what does it mean by false lockout?

For a secure environment, 3 is the usual standard. The higher the value the easier it is for an unauthorized person to continue guessing an account's password for unauthorized access. It's up to you what you set the

## Re: Question on Account Lockout – Urgent

value to given the level of security you need.

I'm guessing False lockout is probably when a user has changed their password but some drive mappings (such as discussed in item 3 below) use the older password and when the credentials are reverified the older password obviously won't match the new password and eventually the account can be locked out.

3)Persistent drive mappings: Persistent drives may have been established with credentials that subsequently expired. If the user types explicit credentials when they try to connect to a share, the credential is not persistent unless it is explicitly saved by Stored User Names and Passwords. Every time that the user logs off the network, logs on to the network, or restarts the computer, the authentication attempt fails when Windows attempts to restore the connection because there are no stored credentials.

Who does net use differ by map network drive from GUI? Is persistent drive mappings are not recommended?

One more thing I have noticed is that these issues are coming from Windows 2000 professional with SP4, not from XP professional and our DCs are Windows 2000 with SP4. Any help and pointers are highly appreciated.

You may want to make sure you have enough licenses for all users. We had this problem a couple years ago at work where users were randomly being locked out multiple times and it turned out there wasn't enough licenses to go around.

.