

# Re: User Locout Issue

---

*Source:*

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2006-09/msg01676.html>

---

- *From:* v-chacez@xxxxxxxxxxxxxxx (chace zhang)
  - *Date:* Thu, 14 Sep 2006 02:48:28 GMT
- 

Hi,

Thank you for posting here.

Based on my experience, troubleshooting account lockout issue is complicated. We need to confirm which client computer is causing the account lockout issue first. After that, we need to check which process/application on that computer keeps causing the problem.

Also please let me know the following questions:

Can these users login OWA?

Are these users really lock out in ADUC?

Currently, I would like to suggest that we check the following:

Suggestions:

=====

1. Please enable the user logon audit in your domain.

To do so, you can configure both the Default Domain Policy and the Default Domain Controller Policy and enable the following settings:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\  
"Audit account logon events"

Please enable both Success and Failure logon audit.

Then, check the audit event logs on the domain controllers to see on which computer the original bad domain logon attempt occur.

For example, on Windows Server 2003 DCs, we may see event 681 when the user is locked out. Please check the 681 events for that problematic user account, and check what the exact "From Workstation" is. It is a DC, please

## Re: User Locout Issue

go to that DC and check the 681 event's "From Workstation" string.

273499 Description of Security Event 681

<http://support.microsoft.com/?id=273499>

This will tell us whether the original bad domain logon attempt occurs on the problematic user account's own computer.

2. I am not sure how the account lockout policy is set there. Generally, it is a best practices suggestion to set the Threshold value to 10 or higher. This is high enough to rule out user error and low enough to deter hackers, especially when the password complexity policy is enabled.

Technical speaking, As you know, account lockout policy is a Microsoft Windows security feature that locks a user account if a designated number (Account lockout threshold) of failed logon attempts occur within a specified time frame. These variables are based on security policy lockout settings. You cannot log on to the network through a locked account until the lockout period (Account lockout duration) has expired. To completely lock out an account, you may set the Account lockout duration to 0, so the account will be locked out until an administrator explicitly unlocks it. If you need to learn more about Account Lockout Policy, you may refer to the following information:

### Account lockout duration

=====

This security setting determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from 0 minutes through 99,999 minutes. If you set the account lockout duration to 0, the account will be locked out until an administrator explicitly unlocks it.

If an account lockout threshold is defined, the account lockout duration must be greater than or equal to the reset time.

Default: None, because this policy setting only has meaning when an Account lockout threshold is specified.

### Account lockout threshold

=====

This security setting determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the account will never be locked out.

Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE or password-protected screen savers count as failed logon attempts.

## Re: User Locout Issue

Default: 0.

Reset account lockout counter after

=====

This security setting determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts. The available range is 1 minute to 99,999 minutes.

If an account lockout threshold is defined, this reset time must be less than or equal to the Account lockout duration.

Default: None, because this policy setting only has meaning when an Account lockout threshold is specified.

Explanation of the policies and an example

=====

The Account lockout threshold tracks the bad password count variable. If the bad password counter meets or exceeds the threshold number, the account is locked out for the domain.

Account lockout duration is set from the time of the last bad password count that leads to it being locked out. From that system time, the additional time is added and the user cannot log into the domain. The default value if this is Not Defined is infinite – in other words, the account is locked out until someone with authority to unlock the account does so.

The Reset account lockout counter after variable again impacts the bad password account. It is the amount of time that, if the user enters no more bad passwords, the bad password count remains until it is reset to zero. It cannot be greater than the Account Lockout duration.

Generally, for medium security requirement, the recommended configurations are:

Reset account lockout counter after: 30

Account lockout duration: 30

Account Lockout Threshold: 10

For high security requirement, the recommendations are:

Reset account lockout counter after: 30

Account lockout duration: 0

Account Lockout Threshold: 10

3. If the client computer of that user is running Windows XP. We need to remove the previous password cache, which may be used by some applications

Re: User Locout Issue

and therefore cause the account lockout problem.

To do so:

- 1) Click Start, click Run, type "control userpasswords2" (without the quotation marks), and then click OK.
- 2) Click the Advanced tab.
- 3) Click the "Manage Password" button.
- 4) Check to see if these domain account's passwords are cached. If so, remove them.
- 5) Check if the problem has been resolved now.

For more information, you may refer to the following article:

Q281660:Behavior of Stored User Names and Passwords  
<http://support.microsoft.com/?id=281660>

Hope the info above is helpful. If you have any other concern, please let me know.

Have a nice day!

Best Regards,

Chace Zhang (MSFT)

Microsoft CSS Online Newsgroup Support

Get Secure! – [www.microsoft.com/security](http://www.microsoft.com/security)

=====  
This newsgroup only focuses on Exchange technical issues. If you have issues regarding other Microsoft products, you'd better post in the corresponding newsgroups so that they can be resolved in an efficient and timely manner. You can locate the newsgroup here:  
<http://www.microsoft.com/communities/newsgroups/en-us/default.aspx>

When opening a new thread via the web interface, we recommend you check the "Notify me of replies" box to receive e-mail notifications when there are any updates in your thread. When responding to posts via your newsreader, please "Reply to Group" so that others may learn and benefit from your issue.

Microsoft engineers can only focus on one issue per thread. Although we provide other information for your reference, we recommend you post different incidents in different threads to keep the thread clean. In doing so, it will ensure your issues are resolved in a timely manner.

Re: User Locout Issue

For urgent issues, you may want to contact Microsoft CSS directly. Please check <http://support.microsoft.com> for regional support phone numbers.

Any input or comments in this thread are highly appreciated.

-----  
This posting is provided "AS IS" with no warranties, and confers no rights.

-----  
| From: "Ed Crowley [MVP]" <curspice@xxxxxxxxxxxxxxxx>  
| References: <A4F3171B-24B5-4389-BCB1-7EEB5669E3F0@xxxxxxxxxxxxxxxx>  
| <#A8Gle31GHA.1288@xxxxxxxxxxxxxxxxxxxxxxxx>  
| <DF7F65FD-34C5-42C8-8A10-492C40589588@xxxxxxxxxxxxxxxx>  
| Subject: Re: User Locout Issue  
| Date: Wed, 13 Sep 2006 17:52:32 -0700  
| Lines: 51  
| X-Priority: 3  
| X-MSMail-Priority: Normal  
| X-Newsreader: Microsoft Outlook Express 6.00.2900.2869  
| X-RFC2646: Format=Flowed; Original  
| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2962  
| Message-ID: <OBlmQg51GHA.2516@xxxxxxxxxxxxxxxxxxxxxxxx>  
| Newsgroups: microsoft.public.exchange.admin  
| NNTP-Posting-Host: adsl-216-103-85-85.dsl.snfc21.pacbell.net 216.103.85.85  
| Path: TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTNGP06.phx.gbl  
| Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.exchange.admin:568709  
| X-Tomcat-NG: microsoft.public.exchange.admin

|  
| Is your lockout policy too fussy? Personally, I have strong doubts as to  
| how a lockout policy improves security. If you're going to use lockout,  
| you  
| should have a healthy retry limit (3 is way too small) and it should  
| expire  
| after a few minutes. The only reason to lock out accounts is to thwart  
| hacking passwords, not inconvenience users or increase the issuance of  
| trouble tickets.

| --  
| Ed Crowley  
| MVP - Exchange  
| "Protecting the world from PSTs and brick backups!"

| "George Schneider" <georgedschneider@xxxxxxxxxxxxxxxx> wrote in message  
| [news:DF7F65FD-34C5-42C8-8A10-492C40589588@xxxxxxxxxxxxxxxx](mailto:news:DF7F65FD-34C5-42C8-8A10-492C40589588@xxxxxxxxxxxxxxxx)  
| > That was my first assumption as well. But over the moths as we would  
| get  
| > something like 30 lockouts issues a month i got suspicious. we only  
| have  
| > probaly 60 full time users. I then begain observing people login into  
| the  
| > network without an issue. When they would attempt to login into

Re: User Locout Issue

outlook

|> they

|> type the same password and they would be instantly locked out. We have

a

|> threshold of 3 invalid attempts before being locked out. we have some

|> cases

|> if you are logging into outllok using one profile and when you attempt

to

|> login later using a different profile you'll be locked out instantly as

|> well.

|>

|> "Ed Crowley [MVP]" wrote:

|>

|>> Are they entering the wrong password?

|>> --

|>> Ed Crowley

|>> MVP – Exchange

|>> "Protecting the world from PSTs and brick backups!"

|>>

|>> "George Schneider" <georgedschneider@xxxxxxxxxxxxxxxx> wrote in message

|>> [news:A4F3171B-24B5-4389-BCB1-7EEB5669E3F0@xxxxxxxxxxxxxxxx](mailto:news:A4F3171B-24B5-4389-BCB1-7EEB5669E3F0@xxxxxxxxxxxxxxxx)

|>> >I have a really strang occurance that has been happening ever since

we

|>> > migrated from Exchange 5.5 to Exchange 2003. Users will log onto the

|>> > network

|>> > without an issue. When they attempt to log onto outlook they will

get

|>> > locked

|>> > out even wghen they are putting the proper password. Any idea what

|>> > could

|>> > cause this unusal behavior and what I can do to get to the bottom of

|>> > it.

|>> >

|>> >

|>>

|>>

|>>

|

|

|

|

|

|

|

|

|

|

|

|

|

|

|

|

|

|

|