Implementing and Troubleshooting Account Lockout

Date Launched: Aug 31, 2004
Last Updated: Aug 31, 2004
Section: Articles :: Authentication, Access Control & Encryption
Author: Mitch Tulloch
Printable Version
Rating: 3.5 / 5 - 11 Votes

1 2 3 4 5

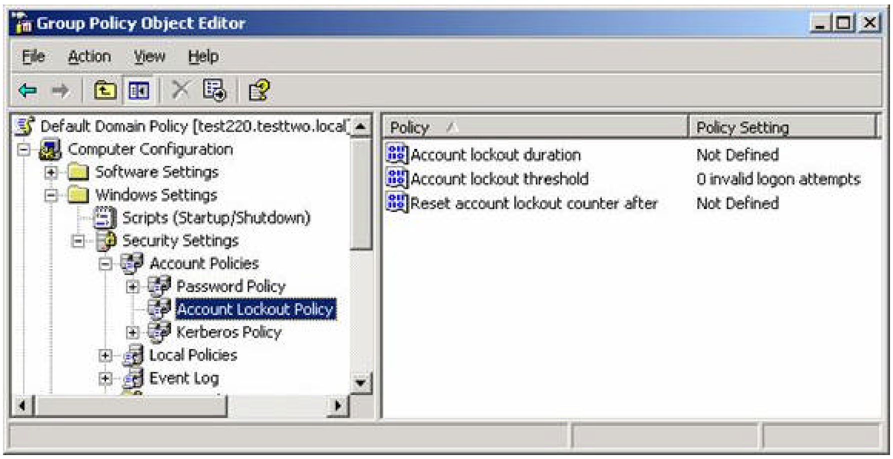
This article examines the advantages and disadvantages from a security standpoint of implementing account lockout on a network running Active Directory. The article also describes some account lockout and management tools you can obtain from the Microsoft Download Center and how to use these tools to troubleshoot account lockout problems.

Account lockout is a feature of password security in Windows 2000 and later that disables a user account when a certain number of failed logons occur due to wrong passwords within a certain interval of time. The purpose behind account lockout is to prevent attackers from brute-force attempts to guess a user's password--too many bad guess and you're locked out.

To configure account lockout in a domain environment you typically use the Default Domain Policy, a Group Policy Object (GPO) linked to the domain. The relevant Group Policy settings are found under:

Computer Configuration
    Windows Settings
        Security Settings
            Account Policies
                Account Lockout Policy

The default settings for account lockout are shown in Figure 1:



Policy	Policy Setting
Account lockout duration	Not Defined
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Defined

Figure 1: Default account lockout policy for a domain

The three policy settings are:

- Account lockout duration - How long (in minutes) a locked-out account remains locked-out (range is 1 to 99,999 minutes).
- Account lockout threshold - How many failed logons it will take until the account becomes locked-out (range is 1 to 999 logon attempts).
- Reset account lockout counter after - How long (in minutes) it takes after a failed logon attempt before the counter tracking failed logons is reset to zero (range is 1 to 99,999 minutes).

A few special cases are:

- Account lockout duration = 0 means once locked-out the account stays locked-out until an administrator unlocks it.
- Account lockout threshold = 0 means the account will never be locked out no matter how many failed logons occur.

As you can see from Figure 1 above, the default account lockout policy is that accounts are never locked out. Is that a good or bad idea?

Pros and Cons of Account Lockout

On the face of it, account lockout seems like a good thing to implement as it makes it difficult for attackers to launch brute force attacks against passwords for user accounts. For example, if Account lockout threshold = 5 then after five guesses of the user's password the user's account could be automatically locked out for Account lockout duration = 30 minutes. Then after 30 minutes elapses the attacker gets another 5 attempts at cracking the password, after which he is locked out again. Obviously it will take some time this way to crack a password.

On the other hand, if Account lockout threshold = 5 and the user hasn't had her coffee yet, she might easily mistype her password 5 times in a row and lock herself out. Then comes the proverbial call to Help Desk saying "I can't log on to my computer" and precious business resources are consumed, both in terms of the time spent resolving the problem and the loss of productivity for the user.

There's more to it though. What if the attacker doesn't care if he guesses the user's password? Perhaps all he's interested in is preventing the user from logging on to the network. In this case the attacker can simply enter any random string for the user's password 5 times in a row and suddenly the user is unable to log on to her computer. Again an annoying call to Help Desk and lost productivity on the user's part. This demonstrates how an attacker can utilize account lockout to create a denial of service (DoS) condition.

While these examples seem somewhat contrived since they assume an attacker has physical access to the network, it turns out account lockout is much more than just typing wrong passwords into the Log On to Windows dialog box. Other ways accounts can get locked out include:

- Applications using cached credentials that are stale.
- Stale service account passwords cached by the Service Control Manager (SCM).
- Stale logon credentials cached by Stored User Names and Passwords in Control Panel.
- Scheduled tasks and persistent drive mappings that have stale credentials.
- Disconnected Terminal Service sessions that use stale credentials.
- Failure of Active Directory replication between domain controllers.
- Users logging into two or more computers at once and changing their password on one of them.

Any one of the above situations can trigger an account lockout condition, and the results can include applications behaving unpredictably and services inexplicably failing.

What should you do? Even Microsoft seems to be of two minds concerning whether to implement account lockout. On the one hand, on page 3 of their white paper called Account Lockout Best Practices, they recommend the following:

"Microsoft recommends that you use the account lockout feature to help deter malicious users and some types of automated attacks from discovering user passwords."

They then go on to recommend the following account lockout policies for low, medium and high security environments:

Low Security

- Account lockout duration = Not Defined
- Account lockout threshold = 0 (no lockout)
- Reset account lockout counter after = Not Defined

Medium Security

- Account lockout duration = 30 minutes
- Account lockout threshold = 10 invalid logon attempts
- Reset account lockout counter after = 30 minutes

High Security

- Account lockout duration = 0 (an administrator must unlock the account)
- Account lockout threshold = 10 invalid logon attempts
- Reset account lockout counter after = 30 minutes

On the other hand, Ben Smith and Brian Komar on page 48 of the Microsoft Windows Security Resource Kit suggest something different:

"Although account lockout settings are common, often they are the cause of numerous support calls to the help desk. If passwords are appropriate in length and complexity, this setting provides little additional security."

Troubleshooting Account Lockout

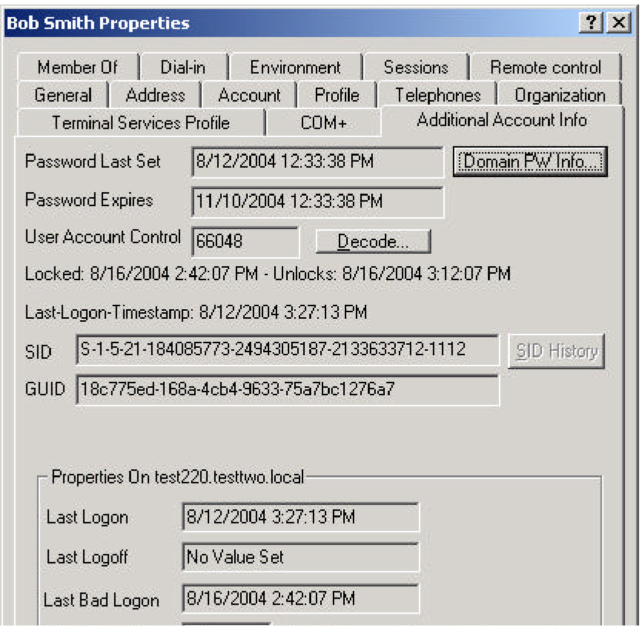
Assuming you've come down on the side of implementing an account lockout policy, are there any tools that can help you troubleshoot problems arising from locked-out accounts? The answer is yes: Microsoft provides a free set of tools called Account Lockout and Management Tools which you can download as the self-extracting file ALTools.exe from the Microsoft Download Center. The remainder of this article examines several of these tools (more detail on them can be found in the Account Lockout Best Practices white paper mentioned previously).

Installing ALTools.exe

After you've downloaded ALTools.exe from the Download Center, double-click on the file to extract the tools to a directory of your choosing. Then install the tools as needed on domain controllers, member servers, or workstations as described under each tool discussed below.

AcctInfo.dll

This DLL adds a new tab called Additional Account Info to user account properties sheets in the Active Directory Users and Computers (ADUC). Copy the file to the System32 folder of the computer on which you run ADUC (typically an administrator workstation with adminpak.msi installed) and then open a command prompt and type regsrv32 acctinfo.dll to register the DLL. Now open ADUC and view the properties of a locked-out user like Bob Smith in Figure 2 below:



Password Last Set 8/12/2004 12:33:38 PM

Password Expires 11/10/2004 12:33:38 PM

User Account Control 66048

Locked: 8/16/2004 2:42:07 PM - Unlocks: 8/16/2004 3:12:07 PM

Last-Logon-Timestamp: 8/12/2004 3:27:13 PM

SID S-1-5-21-184085773-2494305187-2133633712-1112

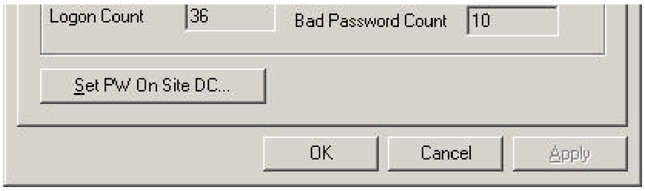
GUID 18c775ed-168a-4cb4-9633-75a7bc1276a7

Properties On test220.testtwo.local

Last Logon 8/12/2004 3:27:13 PM

Last Logoff No Value Set

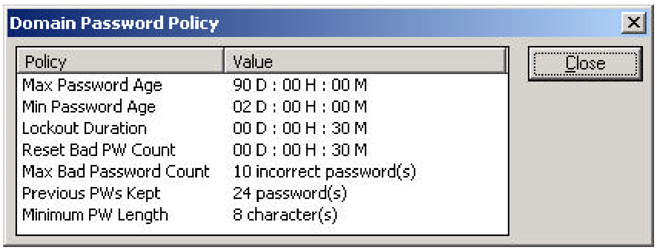
Last Bad Logon 8/16/2004 2:42:07 PM



Logon Count: 36
Bad Password Count: 10

Figure 2: AcctInfo.dll adds the Additional Account Info tab to the properties sheet for a user account

There's lots of information here, but in particular line four indicates the date and time when Bob's account became locked and when it will automatically unlock. Clicking the Domain PW Info button displays the password policy for the domain:

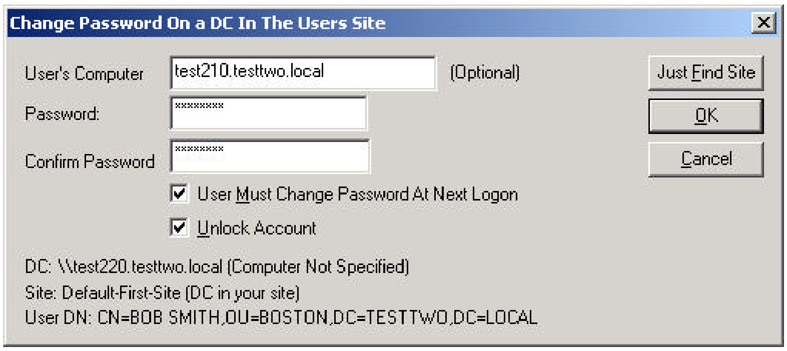


Domain Password Policy

Policy	Value
Max Password Age	90 D : 00 H : 00 M
Min Password Age	02 D : 00 H : 00 M
Lockout Duration	00 D : 00 H : 30 M
Reset Bad PW Count	00 D : 00 H : 30 M
Max Bad Password Count	10 incorrect password(s)
Previous PWs Kept	24 password(s)
Minimum PW Length	8 character(s)

Figure 3: Result of clicking the Domain PW Info button

Clicking the Set PW On Site DC button lets you reset the password for the user and unlock the account (see Figure 3). This is useful because if you want to reset a user's password you should do it using a domain controller in the AD site where the user's computer resides, otherwise replication latency may cause a delay before the user can log on again. This is a better approach to resetting an account by right-clicking on it and selecting Reset Password.



Change Password On a DC In The Users Site

User's Computer: test210.testtwo.local (Optional)
Password: ********
Confirm Password: ********
☑ User Must Change Password At Next Logon
☑ Unlock Account

DC: \\test220.testtwo.local (Computer Not Specified)
Site: Default-First-Site (DC in your site)
User DN: CN=BOB SMITH,OU=BOSTON,DC=TESTTWO,DC=LOCAL

Figure 4: Resetting a user's password on a DC in a remote site

ALockout.dll

This tool creates a log file that can help you diagnose the cause of account lockout problems. Extract the files from ALockout.zip (for Windows 2000) or AlockoutXP.zip (for Windows XP) and copy them the computer experiencing the lockout problems (usually a user's workstation). Copy ALockout.dll to the System32 directory and double-click on Appinit.reg to register the DLL. Then restart the machine and when the lockout problem happens again you can view the log file %WinDir%\debug\ALockout.txt to troubleshoot. Note that interpreting this log requires you understanding Netlogon logging, which is discussed in detail in the previously mentioned whitepaper.

AloInfo.exe

This tool displays the password age for user accounts so you can determine which accounts are about to expire and anticipate problems before they occur. To use this tool copy it to a folder in the system path on a domain controller and run it from a command prompt. Here's an example:

```
C:\>aloinfo /expires /server:test220

Getting Users (This may take a while)...

Retrieved 28 users
Printing Users in descending PW age...

Administrator,28
krbtgt,28
asmith,4
bsmith,4
csmith,3
dsmith,3
esmith,3
...
```

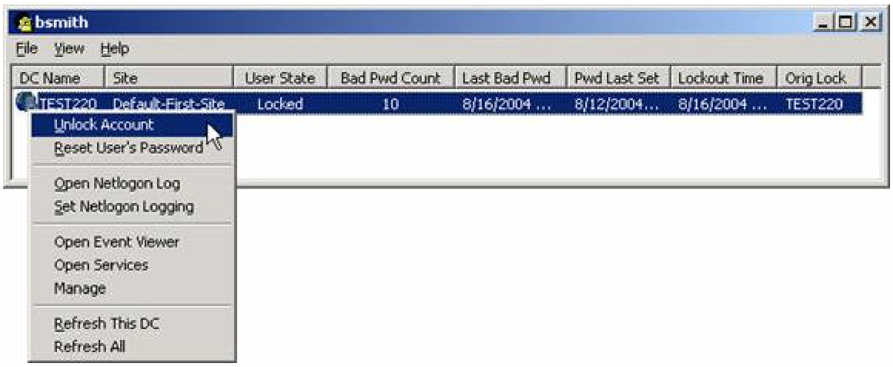
You can also use this tool to display the credentials for all mapped drives for the currently logged-on user, which can help when troubleshooting account lockout problems caused by cached credentials for persistent connections:

```
C:\>aloinfo /stored /server:test220

Getting Service Names and the account they start with...

Checking Mapped Drives for usernames...
Drive Y: is mapped to \\test220\docs with username DEFAULT_USERNAME
```

LockoutStatus.exe

This tool displays various information about locked out accounts that can help you troubleshoot the cause of the lockout. Copy the file to a domain controller and double-click on it to run it, then choose File-->Select Target and specify the name of the user whose account lockout status you want to display. Right-click on a displayed entry to unlock the account, reset its password, or perform other actions (Figure 5):

unlock the account, reset its password, or perform other actions (Figure 5).



DC Name	Site	User State	Bad Pwd Count	Last Bad Pwd	Pwd Last Set	Lockout Time	Orig Lock
TEST220	Default-First-Site	Locked	10	8/16/2004 ...	8/12/2004...	8/16/2004 ...	TEST220

Figure 5: Unlocking an account using LockoutStatus.exe

This tool is particularly useful if lockout problems are arising from AD replication problems, as typically this means you'll see two or more entries for different domain controllers. Note that Microsoft has released an updated version of this tool which can be downloaded here.

Other Tools

Other tools included in ALTools.exe are:

- EventCombMT.exe - Used to consolidate event logs from multiple computers into a single location for analysis.
- NLParse.exe - Used to parse Netlogon files, for example to find status codes relating to account lockout.
- EnableKerbLog.vbs - Used to enable Kerberos logging on multiple computers.

Summary

In this article we've examined the pros and cons of implementing an account lockout policy and how such a policy should be configured in differing security environments. We've also looked at how to use several of the free account lockout tools to display information about locked accounts, reset or unlock accounts, and perform other troubleshooting steps.

About Mitch Tulloch

Mitch Tulloch is a writer, trainer and consultant specializing in Windows server operating systems, IIS administration, network troubleshooting, and security. He is the author of 15 books including the Microsoft Encyclopedia of Networking (Microsoft Press), the Microsoft Encyclopedia of Security (Microsoft Press), Windows Server Hacks (O'Reilly), Windows Server 2003 in a Nutshell (O'Reilly), Windows 2000 Administration in a Nutshell (O'Reilly), and IIS 6 Administration (Osborne/McGraw-Hill). Mitch is based in Winnipeg, Canada, and you can find more information about his books at his website www.mtit.com.