

## Re: Password questions/problems

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-09/7750.html>

---

*From:* aladin ([aladin168@hotmail.com](mailto:aladin168@hotmail.com))

*Date:* 09/20/02

From: [aladin168@hotmail.com](mailto:aladin168@hotmail.com) (aladin)

Date: 20 Sep 2002 12:33:34 -0700

Hi Dr. LL,

You probably want to first to recall if anyone else has logged into your server as the administrator to do something on the server. If not, then I suggest you run an anti-virus and Anti-Trojan program with the latest and most up-to-date virus definition.

It seems to be a trend for virus/Trojan to spread itself to vulnerable systems and change the security template. On my last virus/Trojan analysis

(<http://groups.google.com/groups?hl=en&lr=&ie=UTF-8&oe=UTF-8&threadm=bf0f8e77.0209080706.7f395b0c%40http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/deploy/confeat/08>

that mIRC virus actually modified the security template on the Windows 2000 servers (using secedit.exe) and locked out all domain users from connecting to it. Your situation is a bit different, but seems like a Denial of Service (DoS).

Here are some recommendations on your user account and passwords management:

1. Change the default administrator account "Administrator" to something else that's hard to guess. This will prevent people from guessing your administrator account. Now, create a regular user account called "Administrator", and **DO NOT MAKE IT A MEMBER OF ANY GROUPS**. This way you can see if anyone is trying out "Administrator" user account. This will give you warnings of hacking activities too.
2. Make sure Administrator account is changed every 30 – 90 days to increase server security.
3. Password policies on the Windows 2000 should be changed from the default settings.

Here are default password policy settings:

Enforce password history 1 passwords remembered

Maximum password age =42 days

Minimum password age =0 days  
Minimum password length =0 characters  
Passwords must meet complexity requirements =Disabled  
Store password using reversible encryption for all users in the domain  
=Disabled

Here are the default Account Lockout policy settings:

Account lockout duration =Not defined  
Account lockout threshold =0 invalid logon attempts  
Reset account lockout counter after =Not defined

Here are some suggested settings for the password policy:

- Enforce password history =12 passwords remembered  
Reason: Users cannot re-use passwords from the past 3 years
- Maximum password age =90 days  
Reason: User MUST change passwords within 90 days. Usually between 30 – 90 days. Sys Admin can decide a reasonable value.
- Minimum password age =7 days  
Reason: User can't reset password within 7 days. This will prevent intruders from trying different passwords.
- Minimum password length =8 characters  
Reason: Usually between 6 – 12 characters. 6–8 characters is a more common length.
- Passwords must meet complexity requirements = Disabled (You decide)  
Reason: If set with default passfilt.dll:
  1. Passwords must be at least six characters long.
  2. Passwords can't contain the user name, such as bobm, or parts of the user's full name, such as Bob.
  3. Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols (+,=,\_,\*,&,...).
- Store password using reversible encryption for all users in the domain = Disabled (You decide)  
Reason: Usually not set. Learn more from the Microsoft link below.

Here are some suggested settings for the password policy:

- Account lockout duration =99999 minutes  
Reason: Maximum number allowed for this policy. This will ensure users report to system administrator to reset account. System Administrators will have more control on the account management. You can set to 30 minutes to automatically remove the lockout for accounts, however, most legitimate users will call you anyway when they get locked out. Note: value "0" is good too because it means to lockout indefinitely.
- Account lockout threshold =3 invalid logon attempts  
Reason: Legitimate users should not have to type in more than 3 bad passwords. If they do, the account will get lockout, and you can find out the reason for the lockout and justify this value. 3 attempts is a common value for this policy.
- Reset account lockout counter after =120 minutes

## microsoft.public.win2000.security: Re: Password questions/problems

Reason: The time requires before resetting the counter for bad password attempts. 1 or 2 hours is usually good. After this time, the counter for bad password attempts reset to 0. So, for example, if a person tried 2 bad passwords to logon to his account, Windows 2000 has a counter to remember that he has 2 bad password attempts. Only after 120 minutes, this counter will reset to 0.

For more information on the settings, you can find the detail on Microsoft website:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/deploy/confeat/08>

4. Make sure users do NOT write down their passwords and posted it on the computer monitor or keyboard. You probably will laugh now, but check out those users, and you probably can spot couple of them, or more, doing exactly that. If they do need to write down for whatever reason, make sure the passwords are stored in a secure location, i.e. locked drawer.
5. Make sure users do NOT share passwords with other people.
6. Make sure users do NOT reveal passwords to anyone other than the system administrators and people delegated by the system administrators.
7. Enable logging for successful and failed logon/logoff events. This shows you the activities on your system.
8. Make sure the desktop users with Windows 2000 workstations have good password for their "Administrator" accounts. Make sure "Administrator" accounts on their desktops have NO BLANK PASSWORDS, and NO EASY TO GUESS PASSWORDS. Recent discovered Trojan tries to get into systems with Blank passwords, "Administrator" account with "Administrator" as the password, "admin" account with "admin" as password, "root" with "root" as password... Be careful. Many people overlooked the desktops.

This should be a good start for a good password management and password policy. Microsoft does provide some security guidelines on Windows 2000, and you should definitely check it out and look over the Microsoft recommendations. Again, you can find more Account and Group account management from Microsoft at

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/deploy/confeat/08>

Good luck!

Kyle Lai, CISSP, CISA, MCSE  
Kyle Lai Consulting  
508-380-2022  
<http://www.kylelai.com>  
[kyle@kylelai.com](mailto:kyle@kylelai.com)