

Group Policy Case Solved

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-03/1248.html>

From: Jon (nospamj@i0ta.com)

Date: 03/10/03

From: nospamj@i0ta.com (Jon)
Date: 10 Mar 2003 09:11:03 -0800

#####

The Environment

#####

I decided to implement group policy in our Windows 2000 corporate network. So, I began with the "Security Options" under the Computer Configuration\Windows Settings\Security Settings\Local Policies section, modeling it specifically after the security guidelines found at the NSA's site (<http://nsa2.www.conxion.com/>).

I modified the group policy from my Windows XP Pro workstation using the Active Directory Users and Computers tool. Microsoft claims there isn't any problem editing a policy from an XP workstation. XP has many more settings than Windows 2000 does; it will ignore the settings that it doesn't understand. I looked in the knowledgebase just to make sure before proceeding and found article 307900 (<http://support.microsoft.com/default.aspx?scid=kb:en-us:307900>) which explains this.

I had no problem modifying the policy with XP, nor applying the policy. I applied it to two Windows XP Pro workstations and two Windows 2000 workstations. The both received the settings without any trouble.

#####

The Problem

#####

After I removed the computers from the policy, I checked to see whether the workstations actually removed the policy by going into gpedit.msc or secpol.msc. The XP machines were back to the defaults again. However, I received the message: "Windows cannot open the local policy database. An unknown error occurred when attempting to open the database." on our Windows 2000 workstation machines. There were also problems getting into Outlook.

I struggled with this for quite some time, trying to figure out what had happened. Eventually one of the users in my test rebuilt their

workstation. I placed the remaining Windows 2000 workstation back into the policy and magically, the machine worked fine again. I could open secpol.msc and gpedit.msc without any trouble. They would reflect the settings that the policy had given. So, I left my troubled user's machine in the policy until I could find a fix.

#####

The Solution

#####

After working with the problem for a while, trying different solutions found in the knowledgebase and the newsgroups by searching for the error, I decided to call Microsoft Support and see if they could help.

The tech was VERY helpful, but he had trouble duplicating it in his environment. So, it was naturally difficult for him to troubleshoot the problem. I was pretty much on my own: using the tech as my reference and brain-storming partner.

I did eventually come up with what I think was the solution. Below is a copy of the e-mail that I mailed to the tech explaining what I think was going on. The last thing the tech asked me to try was to restore the security database using the default template with the secedit tool.

Message to Microsoft Tech Support

I was not able to restore the settings using the secedit tool. I tried multiple variations of the command with no success. I pasted the results of one of my tries below:

```
-----  
C:\>secdit /configure /cfg %windir%\security\templates\basicwk.inf  
/db %windir%\security\database\basicwk.sdb /verbose /overwrite /log  
%windir%\security\logs\scesrv.log
```

```
To configure the current system with this template in the /overwrite  
mode will result in losing the existing security records in the  
database specified.Do you want to continue this operation ? [y/n] y
```

An extended error has occurred.

Task is completed with error.

See log C:\WINNT\security\logs\scesrv.log for detail info.

Unfortunately, there was no scesrv.log to look at. No file by that name was on the computer at all. It didn't write it. So, that left me going nowhere.

The exciting news is that I discovered the settings that cause the error. It wasn't just the LAN Manager authentication level setting that we were playing with earlier. It turned out to be a combination of the "Minimum session security for NTLM SSP based (including secure RPC) clients" and the "LAN Manager authentication level".

Here's what I believe is going on. In my group policy, I had these settings under Security Options:

Network security: LAN Manager authentication level = Send NTLMv2 response only\refuse LM & NTLM
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients = Require NTLMv2 session security,Require 128-bit encryption

That worked fine. But when I disabled the policy or set the LAN Manager authentication level in the policy to "Send LM & NTLM responses", I received the "Windows cannot open the local policy database. An unknown error occurred when attempting to open the database." in Secpol.msc or GPEdit.msc.

I think what is happening is that the two settings are colliding. When I lower the LAN Manager authentication level to "Send LM & NTLM responses", it collides with the rule in the Minimum session security setting that says "Require NTLMv2 session security". How can it require NTLMv2 when the previous setting doesn't have an option to use it? That makes sense. And that's why any other LAN Manager authentication level setting worked, although I haven't checked the "Send NTLM response only" setting. If my theory is right, that setting shouldn't work either.

So, why did I still receive the error after disabling the policy? Because the Minimum session security setting isn't being removed from the registry. So, the LAN Manager authentication level goes back to its default of "Send LM & NTLM responses" while the "Require NTLMv2 session security" setting is still in the registry. It produces the same error again in Secpol.msc and GPEdit.msc because the settings collide again.

To fix the situation, the key needs to be manually removed from the registry. Here's a copy of the exported key:

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0]
"ntlmminclientsec"=dword:20080000
```

When I delete that key and then reboot, everything works fine. I was able to fix our broken user that way.

Anyway, I hope that you can pass this on to the developers or somehow put out a knowledgebase article that warns people about using those two settings with Windows 2000 computers. Hopefully things will be fixed in SP4 or Windows Server 2003.

End of Message to Tech Support

I hope this helps someone with a similar problem. :-)

```
#####  
# THE END #  
#####
```