

# Re: lockdown desktop without Group Policy

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.terminal\\_services/2007-10/msg00572.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.terminal_services/2007-10/msg00572.html)

---

- *From:* Tonky <[Tony@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Tony@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 26 Oct 2007 09:51:00 -0700
- 

Dear Vera

I have a similar issue, but on a Server 2003 R2 SP1 box which is a DC and so I followed the instructions for GP Editor as suggested by TP. All seemed to go well until accessing the desktop shortcut created in the last step. A Command prompt appears requesting the gpedit password. When I attempt to type it in, nothing appears but the Command Line disappears launching Group Policy Editor saying access denied.

Something obviously went wrong, which could stem back to editing the security settings for gpt.ini, which suggested changes couldn't be made as it was read only, but it appeared to make changes all the same as all existing security groups were removed from the list.

I can now no longer edit group policy.

Any help?

Many thanks.

Tony

--

Always hands on and keen to learn.

"Vera Noest [MVP]" wrote:

That's one of the disadvantages of local policies, they don't allow security filtering.

TP posted a way around this a while ago:

From: "TP" <[tperson.knowspamn@xxxxxxxxxxxxxxxxxxxxx](mailto:tperson.knowspamn@xxxxxxxxxxxxxxxxxxxxx)>

Subject: Re: local policy and terminal server

Date: Wed, 8 Nov 2006 16:59:42 -0500

Newsgroups: microsoft.public.windows.terminal\_services

Here are the instructions for a standalone 2003 server, which can

## Re: lockdown desktop without Group Policy

be summarised with:

1. create a group and user (steps 1 – 4)
2. set permissions and ownership on three folders and a file (steps 5 – 23)
3. create a shortcut (steps 24 – 27)

### INITIAL SETUP

This should be done before attempting any changes to Group Policy settings.

1. Logon as an administrator
2. Open up Computer Management from Administrative Tools
3. Create a new local group named "GP Editors"
4. Create a new local user named "gpedit". Assign this user a password, and check "password never expires". Make this user a member of the GP Editors group.
5. Open up windows explorer and browse to the following folder (make sure that view hidden files is enabled):  
C:\WINDOWS\system32\GroupPolicy
6. Right-click on the GroupPolicy folder and Properties – Security – Advanced
7. Click the Add button, enter GP Editors in the Select User or Group dialog, and click OK
8. Check Full Control under the Allow column, and click OK
9. Check "Replace permission entries on all child objects with entries shown here that apply to child objects"
10. Click the Apply button and confirm Yes twice.
11. On the Owner tab, click the Other Users and Groups button, enter GP Editors, and click OK.
12. Check "Replace owner on subcontainers and objects"
13. Make sure GP Editors is selected in the Change Owner to list.
14. Click the OK button to change the owner, click OK to close the GroupPolicy Properties
15. Within the GroupPolicy folder, right-click on the Machine folder, and choose Properties – Security
16. On the Security tab, select Administrators on the top, and check Full Control under the Deny column
17. Click OK to save the Deny permission you just made, confirm by answering Yes twice
18. Within the GroupPolicy folder, right-click on the User folder, and choose Properties
19. On the Security tab, select Administrators on the top, and check Full Control under the Deny column
20. Click OK to save the Deny permission you just made, confirm by answering Yes twice
21. Within the GroupPolicy folder, right-click on the gpt.ini file, and choose Properties
22. On the Security tab, select Administrators on the top, and check Full Control under the Deny column
23. Click OK to save the Deny permission you just made, confirm

Re: lockdown desktop without Group Policy

by answering Yes twice

24. Right-click on the desktop and choose New-->Shortcut

25. Enter the following in the location box:

runas /user:gpedit "%windir%\system32\mmc gpedit.msc"

26. Click Next, and enter "Edit Group Policy" for the name

27. Click Finish

MODIFYING GROUP POLICY SETTINGS

1. Logon using the account you used for the initial setup

2. Double-click on the Edit Group Policy shortcut

3. Enter the password for the gpedit account

4. Edit the policies as needed

---

Vera Noest

MCSE, CCEA, Microsoft MVP – Terminal Server

TS troubleshooting: <http://ts.veranoest.net>

\_\_\_ please respond in newsgroup, NOT by private email \_\_\_

=?Utf-8?B?UGVhcmw=?= <Pearl@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote on 07 sep 2007 in microsoft.public.windows.terminal\_services:

Vera

That seems to work fine but it also restricted the administrator. How can I get back into the server as the administrator and apply the policy to all users EXCEPT the administrator? I now don't have run nor any of the items I activated...which is good for the users but not for the administrator.

"Vera Noest [MVP]" wrote:

Use gpedit.msc

---

Vera Noest

MCSE, CCEA, Microsoft MVP – Terminal Server

TS troubleshooting: <http://ts.veranoest.net>

\_\_\_ please respond in newsgroup, NOT by private email \_\_\_

=?Utf-8?B?UGVhcmw=?=

<Pearl@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote on

07 sep 2007 in microsoft.public.windows.terminal\_services:

thanks for replying. What we'd like to do is setup only Local Users (no AD users) to access this TServer and still

Re: lockdown desktop without Group Policy

apply desktop restrictions like: 1. limit only a specific application to launch 2. remove and disable key desktop icons like Network Places, My Computer, Internet Explorer  
3. Disable the RUN command  
4. Disable the wallpaper and Desktop properties from being customized 5. Not making security tab available to the users  
6. Only showing and allowing Logoff....no shutdown  
7. Prevent access to the command prompt  
8. Prevent users from accessing Registry tools to edit the Registry

I have GPMC and the server is Windows 2003 standard. I am advised that GPMC will not allow us to configure these restrictions for the User so what other options do I have?

Thanks in advance

"Lanwench [MVP – Exchange]" wrote:

Pearl

<Pearl@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote:

is there a way to lockdown a Terminal Server session desktop without using Group Policy?

Sure, many ways. For example, if you're using a standalone or member server you can

Re: lockdown desktop without Group Policy

do a lot of things with  
\*local\*  
policies. But you may wish  
to be more specific about  
what  
exactly you're trying to do,  
and why you're trying to do  
it  
without group policy if you  
have it as an option....