

# Re: Help with configuration

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.terminal\\_services/2007-04/msg00251.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.terminal_services/2007-04/msg00251.html)

---

- *From:* "Vera Noest [MVP]" <[vera.noest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:vera.noest@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 11 Apr 2007 15:15:57 -0700
- 

Managing GPOs is an art in itself...

Have to run, will be away for a week, but check the links on my Group Policy page, especially:

816662 – Recommendations for Managing Group Policy Administrative Template (.adm) files

<http://support.microsoft.com/?kbid=816662>

307900 – Upgrading Windows 2000 Group Policy for Windows XP

<http://support.microsoft.com/?kbid=307900>

896669 – When use the Group Policy Object Editor on a computer that is running Windows Server 2003 or Windows XP to change GPOs on a remote domain controller, the changes do not take affect for a long time

<http://support.microsoft.com/?kbid=896669>

---

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?bGF2YWdpcmw=?= <[lavagirl@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:lavagirl@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>

wrote on 11 apr 2007 in

microsoft.public.windows.terminal\_services:

Oh dear, my GPO is not working again. It seems like it works sometimes, and does not work other times. Is that possible? I do have the processing mode set to "Replace", and I may have been wrong about it redirecting the home folder. It had applied all the other settings, so I think I may have made an assumption on that one. I will specify it on the folder redirect in the GPO.

But now, aside from that, it is not applying any of the settings

## Re: Help with configuration

again!

In our network, we have a W2000 server and a W2003 server running, both as domain controllers, replicating each other. I created the GPO on the 2000 server originally. I noticed that if I try to edit it on the 2003 server, I get error messages when I go back and edit it on the 2000 server because of the added policies added on the 2003 server. Should I create it on the 2000 server, and just make sure I always go there to edit it? I did not actually make any changes to it on the 2003 server, I just went in there and looked at it (I guess it automatically saves). After that, I had to delete it and recreate it on the 2000 server because of the error messages. Typically, I do all the active directory changing on the 2000 server anyway. But even after recreating it, it worked for a while, and then didn't. It seems that whenever I make changes to it, it stops working.

Other than that, I have checked the following:

1. I have the Terminal Server computer object in the security list of the GPO with "Read" and "Apply Group Policy" checked.
2. I have my test user included in the Remote Desktop Users group local to the Terminal Server. Remote Desktop users group has "User Access" security in the RDP-tcp connection permissions.
3. In the profile on the server for the test user, I have "Allow login to terminal services" checked.
4. Where i have loopback processing enabled, I have "replace" as the mode.

Is there anything that I've missed? On the GPO properties page, should I have "Block Policy inheritance" checked or unchecked? Also, when I invoke the Remote Desktop connection software on the user workstation, on the screen to enter the user credentials, it defaults to "\\terminalserver\tuser". Do I need to manually change that to "\\ourdomain\tuser"? Same thing when it logs into the terminal server...I have to choose the domain (we already talked about that one) over the local machine.

Sorry for more questions. I had it there for a moment, but then I guess I did something and lost it! :-)

"Vera Noest [MVP]" wrote:

Mmm, that's a bit unexpected.

The only explanation that "My Documents" is redirected on the TS as well is that you have configured the "User Group Policy loopback processing mode" with the "Merge" option, is that correct? meaning that settings which are undefined in the TS GPO are taken from the User GPO.

Re: Help with configuration

If so, then you don't have to redirect it again in the TS GPO.

But I always use the "Replace" option for the loopback setting in the TS GPO, simply because it is easier to manage if all settings are taken from the same GPO, and you don't have to check both.

But both scenarios will work, so it's mostly a matter of taste how you set it up.

No need for a consultancy fee, Lavagirl, newsgroup help is free. I'm glad I've been able to help you getting started. Maybe you'd like to come back here after a while and help other people out!

---

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?bGF2YWdpcmw=?=  
<lavagirl@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote on 11 apr 2007 in  
microsoft.public.windows.terminal\_services:

Oops, let me clarify. Right now, I have a group policy for the regular users to redirect their My Documents folder to a share on the fileserver. The TS profile path and regular profile paths are blank. I do not have the folder redirection configured in the GPO on the TS, but it still defaults the My Documents folder on both accounts to the share on the fileserver (ie: they both show the same redirected folder). Is there any reason why I need to go ahead and configure folder redirection for the My Documents folder in the GPO, if it is already redirecting by default? Should I redirect there also for the other 3 folders shown to the local account?

Thank you so much, you have pretty much walked me through setting up my TS! I should pay you a consulting fee!

"Vera Noest [MVP]" wrote:

OK, so your GPO is working now, good!

About your other questions:

Re: Help with configuration

1. If you leave both profile paths blank, then users will have a local profile, both on their clients and on the TS. Nothing wrong with that, but it will also mean that they have different "My Documents" folders. Users will find it very frustrating that they can't access documents which they created in a TS session from their clients and vice versa. That's why I suggested to redirect at least the "My Documents" folder on the TS to the file server which already holds their "My Documents" folder from the clients.

2. the keyword here is "almost"! I would *\*strongly\** suggest to create 2 separate GPOs and leave the user accounts in their current "Users" OU. The settings in the TS GPO and the normal users GPO might be very similar right now, but they can easily divert later on, when new demands come up. Separating them later on will be much more disruptive than starting with 2 separate GPOs right from the beginning.

---

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?bGF2YWdpcmw=?=  
<lavagirl@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote on 10 apr 2007 in  
microsoft.public.windows.terminal\_services:

OK, my group policy is  
being applied now. I  
realized that

## Re: Help with configuration

I did not have the option cleared on the RDP-tcp connection Client properties tab for "Use connection settings from user settings". Once I cleared that, the GPO settings were applied.

Can I ask two more questions? (I thought about starting a new post, but there was so much history here!)

1. If I do NOT specify a roaming profile path, do I still need to enable folder redirection? (The profile path on the domain account profile is blank, also). If so, do I need it on the My Documents folder, since I am redirecting that to another server with another group policy?
2. I want the students to have almost the same restrictions on their local workstations as on the TS. Should I do this by putting their user object into the TS OU along with the TS computer, or should I create a new group policy on a new OU?

Again, Vera, thanks so much for your help!

"Vera Noest [MVP]" wrote:

OK, it seems that you have come a long way in such

## Re: Help with configuration

a  
short time,  
good work!

About your  
questions:

1.  
Pass-through  
authentication  
is not a  
feature of  
Windows  
Terminal  
Services.  
You would  
need Citrix  
for  
that. But  
you can  
minimize  
the logins to  
2, and users  
can  
save their  
credentials.  
Users  
should  
logon to the  
workstation  
using their  
domain  
account and  
password.  
And  
they should  
use the  
same  
domain  
account and  
password  
logging in  
to the TS.  
Do \*not\*  
create local  
user  
accounts  
for them on  
the TS,  
that's a  
waste of

## Re: Help with configuration

your time as well as a nuisance for your users. It seems to me that you are using the new (Vista, version 6.0) rdp client, is that correct? It has some peculiarities in the way it handles and stores usernames and passowrds. But once users logon with the correct username and passowrd, they can select "Remember my password", which effectively takes away one logon. Be sure to read the information for the rdp 6.0 client here:

Vista  
Remote  
Desktop  
Connection  
Authentication

Re: Help with configuration

FAQ

<http://blogs.msdn.com/ts/archive/2007/01/22/vista-remote-desktop-top-connection-authentication-faq.aspx>

and here:

TS

connection  
experience  
improvements  
based on  
RDP 6.0  
client  
customer  
feedback

<http://blogs.msdn.com/ts/archive/2007/03/28/ts-connection-experience-improvements-based-on-rdp-6-0-client-customer-feedback.aspx>

2. Your

GPO

settings do  
not apply to  
your  
Terminal  
Server.

Have you  
checked in  
the security  
settings of  
the  
GPO that  
the  
Terminal  
Server  
object is in  
the security  
list? As you  
have  
noticed, you  
should  
\*not\* put  
the user  
accounts in  
the  
Terminal  
Servers OU,  
because  
then user  
accounts

## Re: Help with configuration

will always  
be locked  
down, also  
when they  
logon  
to the  
workstations.

3. See  
answer 1.  
Use domain  
accounts.

4. This is a  
bit  
puzzling. It  
should be  
enough to  
add the  
TSUSER  
account as a  
member of  
the Remote  
Desktop  
Users  
group. Note  
that this is  
the \*local\*  
RDU group  
on the  
Terminal  
Server, not  
the Remote  
Desktop  
Users group  
which  
you can see  
in AD.

---

Vera Noest  
MCSE,  
CCEA,  
Microsoft  
MVP –  
Terminal  
Server  
TS  
troubleshooting:  
<http://ts.veranoest.net>  
— please

Re: Help with configuration

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

=?Utf-8?B?bGF2YWdpcmw=?=  
<lavagirl@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote on 05  
apr 2007  
in  
microsoft.public.windows.terminal\_services:

Vera,  
you  
have  
been  
so  
helpful,  
I  
hope  
you  
don't  
mind  
me  
asking  
a  
few  
more  
questions.  
I  
spent  
the  
day  
configuring  
the  
terminal  
server,  
and  
it  
actually  
went  
pretty  
well!  
In  
Active  
Directory,  
I  
created  
an

Re: Help with configuration

OU  
called  
"Terminal  
Services"  
and  
then  
created  
a  
GPO  
for  
it,  
with  
all  
of  
the  
recommended  
lockdown  
settings  
(based  
on  
the  
articles  
you  
mentioned).  
I  
moved  
the  
Terminal  
Server  
object  
into  
the  
new  
OU.  
I  
created  
a  
testuser  
called  
"TSUSER"  
and  
made  
sure  
he  
had  
"Allow  
login  
to  
Terminal  
Services"  
checked

Re: Help with configuration

in  
his  
profile.  
I  
also  
made  
him  
a  
member  
of  
the  
Remote  
Desktop  
Users  
group,  
and  
made  
sure  
that  
this  
group  
had  
access  
to  
use  
the  
TS.  
I  
only  
have  
the  
Office  
apps  
installed  
on  
the  
server,  
so  
I  
put  
the  
icons  
for  
Word,  
Excel  
and  
Powerpoint  
into  
the  
Desktop  
Folder

Re: Help with configuration

under  
"All  
Users"  
on  
the  
TS.  
Then,  
I  
logged  
into  
the  
TS  
as  
TSUSER,  
and  
VOILA!  
There  
was  
my  
desktop  
with  
the  
3  
apps.

Here's  
the  
issues,  
though:

1.  
The  
student  
has  
3  
logons  
that  
he  
has  
to  
go  
through:  
1)  
to  
login  
to  
the  
domain/local  
workstation,  
2)  
to

Re: Help with configuration

give  
credentials  
for  
RDP,  
and  
then  
3)  
to  
logon  
to  
the  
TS!  
Is  
there  
any  
way  
to  
do  
all  
these  
in  
one  
step  
(ie:  
pass  
userid/password  
through)?  
The  
students  
have  
enough  
trouble  
remembering  
their  
regular  
account  
password.

2.  
I  
set  
the  
Computer  
Configuration  
restrictions  
AND  
the  
User  
Configuration  
restrictions  
in

Re: Help with configuration

the  
GPO,  
and  
enabled  
loopback  
processing,  
but  
when  
TSUSER  
logs  
in,  
the  
User  
restrictions  
do  
not  
seem  
to  
be  
in  
effect  
(ie:  
SHUTDOWN  
still  
appears  
on  
the  
start  
menu).  
If  
I  
put  
TSUSER  
into  
the  
lockdown  
OU  
also,  
those  
user  
restrictions  
take  
effect  
on  
the  
local  
machine  
(domain  
account).  
(ie:  
if

Re: Help with configuration

I  
minimize  
the  
remote  
desktop  
session,  
the  
SHUTDOWN  
does  
not  
appear  
on  
the  
Start  
menu,  
but  
it  
still  
appears  
on  
the  
TS  
session).  
How  
do  
I  
apply  
them  
to  
the  
TS  
logon  
session?

3.  
When  
I  
log  
onto  
the  
TS,  
do  
I  
need  
log  
onto  
the  
local  
machine,  
or  
to

Re: Help with configuration

the  
domain?  
Do  
I  
need  
to  
create  
local  
accounts  
for  
all  
of  
my  
domain  
users?

4.  
It  
did  
not  
work  
to  
just  
put  
TSUSER  
into  
the  
Remote  
Desktop  
Users  
group.  
I  
had  
to  
give  
group  
EVERYONE  
user  
rights  
on  
the  
TS.

I  
think  
I'm  
almost  
there!  
Any  
help  
you

Re: Help with configuration

can  
give  
on  
these  
items  
would  
be  
so  
appreciated!  
Thank  
you...

"Vera  
Noest  
[MVP]"  
wrote:

OK,  
good  
luck,  
and  
feel  
free  
to  
post  
back  
here  
if  
you  
have  
more  
questions!

---

—  
Vera  
Noest  
MCSE,  
CCEA,  
Microsoft  
MVP

—  
Terminal  
Server  
TS  
troubleshooting:  
<http://ts.veranoest.net>

—  
please  
respond  
in

Re: Help with configuration

newsgroup,  
NOT  
by  
private  
email

—  
  
=?Utf-8?B?bGF2YWdpcmw=?=  
<lavagirl@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote  
on  
04  
apr  
2007  
in  
microsoft.public.windows.terminal\_services:

Thank  
you  
so  
much  
for  
all  
the  
info.  
I  
am  
going  
to  
configure/test  
starting  
tomorrow.  
I  
wanted  
to  
get  
a  
good  
plan  
and  
make  
sure  
I  
understood  
before  
I  
even  
touched  
the  
server.

Re: Help with configuration

I  
will  
not  
be  
putting  
anything  
into  
production  
for  
the  
students  
until

I  
know  
it  
works.

I  
wish  
we  
could  
hire  
someone  
to  
help,  
but  
we  
are  
a  
small  
school  
with  
little  
money,

so  
I'm  
it!  
:-)  
Thank  
you  
so  
much  
for  
all  
your  
help.

"Vera  
Noest  
[MVP]"  
wrote:

Re: Help with configuration

Yes,  
they  
logon  
to  
the  
workstation  
first.  
From  
there,  
they  
start  
the  
Terminal  
Server  
session  
with  
a  
small  
program  
called  
"Remote  
Desktop"  
(this  
is  
also  
referred  
to  
as  
the  
rdp  
client).  
You  
can  
find  
that  
on  
any  
XP  
workstation,  
under  
Start  
Menu  
–  
Applications  
–  
Accessories  
–  
Communication  
(I  
think,  
I'm

Re: Help with configuration

translating  
from  
Swedish).  
But  
you  
wrote  
in  
your  
first  
post  
that  
you  
had  
"installed  
RDP  
on  
the  
client  
computers"?  
Assuming  
that  
you  
meant  
the  
rdp  
client,  
that's  
the  
program  
you  
use  
to  
connect  
to  
the  
Terminal  
Server.

And  
no,  
you  
cannot  
logon  
directly  
to  
the  
TS  
without  
logging  
in  
to

Re: Help with configuration

the  
workstation  
first.  
There  
is  
3rd  
party  
software  
(Citrix)  
which  
you  
install  
on  
top  
of  
Terminal  
Services  
to  
enable  
you  
to  
use  
your  
cached  
domain  
account  
credentials  
to  
automatically  
logon  
to  
the  
TS  
once  
you  
have  
logged  
on  
to  
the  
workstation,  
but  
it's  
quite  
expensive  
if  
this  
is  
the  
only  
feature

Re: Help with configuration

you  
need.

When  
you  
create  
a  
GPO,  
you  
link  
it  
to  
a  
OU.  
The  
computer  
settings  
in  
the  
GPO  
are  
applied  
to  
the  
objects  
in  
the  
OU.  
So  
if  
you  
link  
your  
lock-down  
GPO  
to  
the  
OU  
which  
contains  
the  
Terminal  
Server,  
it  
applies  
to  
the  
Terminal  
Server.  
If  
you

Re: Help with configuration

link  
the  
same  
GPO  
to  
the  
OU  
which  
contains  
your  
workstations,  
it  
applies  
to  
your  
workstation.  
Note  
that  
by  
default,  
the  
user  
settings  
are  
always  
taking  
from  
the  
GPO  
(if  
any)  
which  
is  
linked  
to  
the  
OU  
which  
contains  
your  
user  
accounts.  
That's  
why  
you  
have  
to  
use  
the  
"loopback  
processing"

Re: Help with configuration

options  
in  
your  
TS  
GPO.

Setting  
up  
a  
Terminal  
Server  
and  
locking  
it  
down  
properly  
with  
GPOs  
is  
not  
a  
trivial  
task.  
I  
would  
advise  
you  
to  
\*not\*  
take  
it  
into  
production  
before  
you  
have  
tested  
everything  
thoroughly,  
not  
only  
with  
your  
own  
Administrator  
account,  
but  
also  
with  
a  
test

Re: Help with configuration

Re: Help with configuration

user  
account.  
It  
could  
be  
a  
wise  
decision  
to  
hire  
some  
external  
company  
to  
assist  
you  
in  
setting  
this  
up  
properly.

---

—  
—  
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?bGF2YWdpcmw=?=  
<lavagirl@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
wrote  
on

Re: Help with configuration

03

apr

2007

in

microsoft.public.windows.terminal\_s

Okay,  
please  
forgive  
my  
ignorance...you  
have  
been  
very  
helpful.  
So,  
they  
log  
onto  
the  
local  
domain  
account  
first,  
then  
logon  
again  
to  
the  
TS?  
How  
do  
they  
do  
that?  
Is  
there  
a  
desktop  
shortcut  
or  
start  
menu  
icon  
to  
the  
session?  
Is  
there  
a

Re: Help with configuration

28

Re: Help with configuration

way  
to  
have  
ONE  
login  
and  
log  
just  
into  
the  
TS?  
I  
noticed  
in  
the  
configuration  
of  
the  
TS  
OU,  
you  
can  
configure  
it  
to  
disable  
the  
Control  
panel,  
network  
neighborhood,  
manage  
dialogue,  
search,  
internet  
address,  
etc...  
If  
you  
configure  
these  
things  
in  
the  
lockdown  
OU  
this  
disabling  
it  
locally  
or

Re: Help with configuration

on  
the  
TS  
session?  
This  
is  
very  
confusing.  
Thanks!