

Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2004-11/0315.html

From: Bruce Sanderson (*Bruce.Sanderson_at_junk.junk*)

Date: 11/17/04

Date: Wed, 17 Nov 2004 14:25:03 -0800

Here's a diagram that might help. For this to work, don't use any GPO filtering (except as explained at the end of this note) and don't change the GPO security settings from the defaults. This is essentially what we have in our situation with about 650 workstations, 600 users and 7 Terminal Servers and it works exactly as advertised (Windows 2000 Domain Controllers, Windows 2003 Terminal Servers, Windows XP SP1 and SP2 workstations).

TopLevel OU

|_ TerminalServerOU – contains only the computer account for the Terminal Server – no user accounts – no workstation computer accounts

| GPOs linked at TerminalServerOU

|_ TerminalServerLoopback – GPO with Computer Configuration, Administrative Templates,

| System, Group Policy,

| "User Group Policy loopback processing mode" set to

Enabled

|_ TerminalServerNoShutdown – GPO with User Configuration, Administrative Templates,

| Start Menu and Taskbar,

| "Remove and prevent access to the Shutdown command" set

to Enabled

|

|_ UsersOU – contains only user accounts – no computer accounts

| GPOs linked at UsersOU

|_ UsersNoScreenSaver – GPO with User Configuration, Administrative Templates, Control Panel,

| "Display Hide Screen Saver tab" set to Enabled

|

|_ WorkstationComputersOU – contains workstation computer accounts
No GPOs linked here

Wait long enough for the replication to all domain controllers after making any changes (usually, not more than a few minutes at most).

Restart the workstation computer and the Terminal server, or run the command

microsoft.public.windows.group_policy: Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

gpupdate /force on the computers.

Logon at the workstation with a user account that is in the UsersOU.
Observe that the Screen Saver tab in the Display Properties is missing per the GPO linked to the Users OU, but that the Shutdown button appears in the Start Panel and the user can shutdown the workstation.

>From the workstation, use the Remote Desktop Connection (or whatever client you use) to establish a Terminal Services Server and logon with the same user account as was used to logon to the workstation. Observe that not only is the Screen Saver tab missing from the Display Properties, but the Shutdown button is missing from the Start Menu.

I've chosen these settings only because the affect is easy to observe. You could of course use whatever settings are appropriate in your situation.

If you are using Roaming Profiles, I suggest using a seperate set of Roaming Profiles for Terminal Services. You can configure this by adding the following setting in a GPO applied to the TerminalServerOU – Computer Configuration, Administrative Templates\Windows Explorer\Set path for TS Roaming Profiles:.

The GPO Loopback setting in the TerminalServerLoopback GPO tells the Group Policy processing system to apply the User Configuration settings in any GPOs linked to the TerminalServerOU to users when they logon to a computer whose computer account is in that OU.

Once you have the OUs and GPO set up and working as described above, you can change the permissions on the TerminalServerNoShutdown GPO so that it does not apply to Administrators.

1. Open Group Policy Management
2. navigate to where the TerminalServerNoShutdown GPO is linked and select it
3. select the Delegation tab
4. click Add
5. key the name of a Domain Group that contains user accounts you want to be able to shutdown the terminal server (e.g. Domain Admins)
6. click Advanced...
7. select the Group you added in step 5
8. remove all check marks
9. add check mark in the Deny column for Apply Group Policy
10. click OK

As usual, it is a good idea to not have both User Configuration settings and Computer Configuration settings in the same GPO.

--

Bruce Sanderson MVP

It's perfectly useless to know the right answer to the wrong question.
"Gregg Hill" <bogus@nowhere.com> wrote in message
news:%23%23C1zGIzEHA.336@TK2MSFTNGP10.phx.gbl...

Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

microsoft.public.windows.group_policy: Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

```
> Roger,
>
> I just checked my client today. Their server does NOT have the extra link
> in the picture that I have on my server, yet SOME of the GPO gets applied
> to the desktops.
>
> I logged into my laptop as Administrator, and as Test (a user in the
> Terminal Server Users group). I ran gpresults.exe from each login.
>
> According to my current gpresult.exe output, it looks as though the GPO is
> not getting applied when the regular user logs into a workstation ("Test"
> logging into my laptop), yet SOME of the restrictions in the GPO are
> indeed applied.
>
> I am building fresh domains at home to test all this stuff out. I need to
> start from scratch and see where it is going wrong. I will have a 2003
> server with AD, a 2000 member server Terminal Server, and XP Pro
> workstation. I also will have a 2000 server with AD, a 2000 member server
> Terminal Server, and XP Pro workstation.
>
> In case you get real bored, here are the results of today's gpresults.exe
> runs. I am going to bed 12 seconds after I hit Send. If I cannot figure it
> out with fresh test domains, I will call Microsoft next week.
>
> Thanks for all your help.
>
> Gregg Hill
>
> gpresults output: I changed the actual domain name, but nothing else.
> *****
> 1) Logged into laptop as Domain Admin: there were no restrictions. I have
> admins excluded by using article
> http://support.microsoft.com/?kbid=816100. There were no restrictions when
> logging into the TS, which is how I want it.
>
> Microsoft Windows XP [Version 5.1.2600]
> (C) Copyright 1985-2001 Microsoft Corp.
>
> c:\>gpresult
>
> Microsoft (R) Windows (R) XP Operating System Group Policy Result tool
> v2.0
> Copyright (C) Microsoft Corp. 1981-2001
>
> Created On 11/16/2004 at 11:13:53 AM
>
>
> RSOP results for MYDOMAIN\administrator on LAPTOP-GH1 : Logging Mode
> -----
>
> OS Type: Microsoft Windows XP Professional
> OS Configuration: Member Workstation
> OS Version: 5.1.2600
> Domain Name: MYDOMAIN
> Domain Type: Windows 2000
> Site Name: Default-First-Site-Name
> Roaming Profile:
> Local Profile: E:\Documents and
> Settings\administrator.MYDOMAIN
> Connected over a slow link?: No
>
>
```

microsoft.public.windows.group_policy: Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

```
> COMPUTER SETTINGS
> -----
> CN=LAPTOP-GH1,CN=Computers,DC=mydomain,DC=local
> Last time Group Policy was applied: 11/16/2004 at 10:54:21 AM
> Group Policy was applied from: dc01.mydomain.local
> Group Policy slow link threshold: 500 kbps
>
> Applied Group Policy Objects
> -----
> Default Domain Policy
> Local Group Policy
>
> The following GPOs were not applied because they were filtered out
> -----
> Terminal Services Policy
> Filtering: Not Applied (Unknown Reason)
>
> The computer is a part of the following security groups:
> -----
> BUILTIN\Administrators
> Everyone
> Debugger Users
> BUILTIN\Users
> NT AUTHORITY\NETWORK
> NT AUTHORITY\Authenticated Users
> LAPTOP-GH1$
> Domain Computers
>
>
> USER SETTINGS
> -----
> CN=Administrator,CN=Users,DC=mydomain,DC=local
> Last time Group Policy was applied: 11/16/2004 at 11:12:30 AM
> Group Policy was applied from: dc01.mydomain.local
> Group Policy slow link threshold: 500 kbps
>
> Applied Group Policy Objects
> -----
> Default Domain Policy
>
> The following GPOs were not applied because they were filtered out
> -----
> Local Group Policy
> Filtering: Not Applied (Empty)
>
> The user is a part of the following security groups:
> -----
> Domain Users
> Everyone
> BUILTIN\Users
> BUILTIN\Administrators
> NT AUTHORITY\INTERACTIVE
> NT AUTHORITY\Authenticated Users
> LOCAL
> Enterprise Admins
> Group Policy Creator Owners
> Schema Admins
> Domain Admins
>
> c:\>
> *****
>
```

Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

microsoft.public.windows.group_policy: Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

```
> 2) Logged into laptop as Test, a Domain User. I believe I have Domain
> Users unchecked for Apply GP in the Terminal Server Policy GPO's security
> settings (because I cannot get loopback to work right).
>
> E:\Documents and Settings\test>gpresult
>
> Microsoft (R) Windows (R) XP Operating System Group Policy Result tool
> v2.0
> Copyright (C) Microsoft Corp. 1981-2001
>
> Created On 11/16/2004 at 10:59:06 AM
>
>
> RSOP results for MYDOMAIN\test on LAPTOP-GH1 : Logging Mode
> -----
>
> OS Type:                Microsoft Windows XP Professional
> OS Configuration:      Member Workstation
> OS Version:            5.1.2600
> Domain Name:           MYDOMAIN
> Domain Type:           Windows 2000
> Site Name:             Default-First-Site-Name
> Roaming Profile:
> Local Profile:         E:\Documents and Settings\test
> Connected over a slow link?: No
>
>
> COMPUTER SETTINGS
> -----
>   CN=LAPTOP-GH1,CN=Computers,DC=mydomain,DC=local
>   Last time Group Policy was applied: 11/16/2004 at 10:54:21 AM
>   Group Policy was applied from:      dc01.mydomain.local
>   Group Policy slow link threshold:   500 kbps
>
>   Applied Group Policy Objects
>   -----
>     Default Domain Policy
>     Local Group Policy
>
>   The following GPOs were not applied because they were filtered out
>   -----
>     Terminal Services Policy
>       Filtering:  Not Applied (Unknown Reason)
>
>   The computer is a part of the following security groups:
>   -----
>     BUILTIN\Administrators
>     Everyone
>     Debugger Users
>     BUILTIN\Users
>     NT AUTHORITY\NETWORK
>     NT AUTHORITY\Authenticated Users
>     LAPTOP-GH1$
>     Domain Computers
>
>
> USER SETTINGS
> -----
>   CN=test,CN=Users,DC=mydomain,DC=local
>   Last time Group Policy was applied: 11/16/2004 at 10:57:12 AM
>   Group Policy was applied from:      dc01.mydomain.local
>   Group Policy slow link threshold:   500 kbps
```

microsoft.public.windows.group_policy: Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

```
>
> Applied Group Policy Objects
> -----
> Default Domain Policy
>
> The following GPOs were not applied because they were filtered out
> -----
> Local Group Policy
> Filtering: Not Applied (Empty)
>
> The user is a part of the following security groups:
> -----
> Domain Users
> Everyone
> BUILTIN\Users
> NT AUTHORITY\INTERACTIVE
> NT AUTHORITY\Authenticated Users
> LOCAL
>
> E:\Documents and Settings\test>
>
> *****
>
> 3) Logged into laptop as Test, now temporarily added to the Terminal
> Server Users group inside the Users container. The Terminal Server OU
> itself is empty except for the TS machine account moved from the default
> Computers container. When I log into my laptop as this user, there should
> be NO restrictions from the GPO applied (if I understand the purpose of
> the loopback processing). If I use this user to log into the TS, the TS
> session desktop should, and does, get tightly locked down.
>
> This login to my laptop resulted in a restricted desktop, but NOT as
> tightly restricted as when I access the TS via Remote Desktop Connection.
> It looks as though the Computer Settings portion of the GPO gets skipped,
> but the User Settings portion of the GPO gets applied. I thought loopback
> made it skip this GPO completely.
>
>
> E:\Documents and Settings\test>gpresult
>
> Microsoft (R) Windows (R) XP Operating System Group Policy Result tool
> v2.0
> Copyright (C) Microsoft Corp. 1981-2001
>
> Created On 11/16/2004 at 10:49:33 AM
>
>
> RSOP results for MYDOMAIN\test on LAPTOP-GH1 : Logging Mode
> -----
>
> OS Type: Microsoft Windows XP Professional
> OS Configuration: Member Workstation
> OS Version: 5.1.2600
> Domain Name: MYDOMAIN
> Domain Type: Windows 2000
> Site Name: Default-First-Site-Name
> Roaming Profile:
> Local Profile: E:\Documents and Settings\test
> Connected over a slow link?: No
>
>
> COMPUTER SETTINGS
```

Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

microsoft.public.windows.group_policy: Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

```
> -----
> CN=LAPTOP-GH1,CN=Computers,DC=mydomain,DC=local
> Last time Group Policy was applied: 11/16/2004 at 9:41:02 AM
> Group Policy was applied from:      dc01.mydomain.local
> Group Policy slow link threshold:   500 kbps
>
> Applied Group Policy Objects
> -----
>     Default Domain Policy
>     Local Group Policy
>
> The following GPOs were not applied because they were filtered out
> -----
>     Terminal Services Policy
>     Filtering:  Not Applied (Unknown Reason)
>
> The computer is a part of the following security groups:
> -----
>     BUILTIN\Administrators
>     Everyone
>     Debugger Users
>     BUILTIN\Users
>     NT AUTHORITY\NETWORK
>     NT AUTHORITY\Authenticated Users
>     LAPTOP-GH1$
>     Domain Computers
>
>
> USER SETTINGS
> -----
> CN=test,CN=Users,DC=mydomain,DC=local
> Last time Group Policy was applied: 11/16/2004 at 10:48:11 AM
> Group Policy was applied from:      dc01.mydomain.local
> Group Policy slow link threshold:   500 kbps
>
> Applied Group Policy Objects
> -----
>     Default Domain Policy
>     Terminal Services Policy
>
> The following GPOs were not applied because they were filtered out
> -----
>     Local Group Policy
>     Filtering:  Not Applied (Empty)
>
> The user is a part of the following security groups:
> -----
>     Domain Users
>     Everyone
>     BUILTIN\Users
>     NT AUTHORITY\INTERACTIVE
>     NT AUTHORITY\Authenticated Users
>     LOCAL
>     Terminal Server Users
>
> E:\Documents and Settings\test>
>
> *****
>
> Well, there you have it. The story of my life for the last two weeks!
>
> Gregg Hill
```

Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

microsoft.public.windows.group_policy: Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

```
>
>
>
>
> "Roger Abell" <mvpNOSpam@asu.edu> wrote in message
> news:e4DMd%23GzEHA.3408@tk2msftngp13.phx.gbl...
>>
>>> Should I take it that the link to "mydomainname.local" is the cause of
>>> the
>>> problem?
>>
>> That it would be. You thus apply it to all accounts no matter to
>> what machine they log in.
>>
>> --
>> Roger
>> "Gregg Hill" <bogus@nowhere.com> wrote in message
>> news:OK6rcH0yEHA.3844@TK2MSFTNGP12.phx.gbl...
>>> Roger,
>>>
>>> Thanks for the help. By "restricted GPO" I meant that it is the one that
>> has
>>> all the settings for lockdown in it. It is not restricted in that user
>>> permissions have been changed: they are still the default permissions,
>> with
>>> the exception of placing the TS machine account into the security
>>> settings
>>> per 260370.
>>>
>>> I think you are on to something with the linking of the GPO. I just set
>>> everything up per the articles mentioned and it has the GPO linked to
>>> the
>>> "Terminal Servers" OU and to "mydomainname.local" when viewed in the
>>> Group
>>> Policy Management Console. I am using SBS 2003 at home with a test
>>> 2000TS,
>>> but the other sites I was trying to set up are plain 2003 DC with
>>> 2000TS.
>>> I'll check them later today.
>>>
>>> Should I take it that the link to "mydomainname.local" is the cause of
>>> the
>>> problem?
>>>
>>> Gregg Hill
>>>
>>>
>>> "Roger Abell" <mvpNOSpam@asu.edu> wrote in message
>>> news:uLQohDuyEHA.804@TK2MSFTNGP12.phx.gbl...
>>> > Hi Gregg,
>>> >
>>> > No, I do not have a GP book I most value to recommend.
>>> > At any rate, I am not likely familiar with all of them (few
>>> > as they are).
>>> >
>>> > You bring up many things.
>>> > When it say loopback is only for a purely W2k environment
>>> > what it means is that the machines involved cannot be pre-W2k
>>> > and that the user accounts cannot be coming from a trusted NT4
>>> > domain.
>>> > When it cautioned you that the machine objects must be in the
>>> > OU to which the loopback GPO is linked, it was not referring
```

microsoft.public.windows.group_policy: Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

```
>>> > to the workstations used when connecting to the TS server, but
>>> > it was meaning all machine logging into which should cause the
>>> > user settings to be dominated by the loopback processing need
>>> > to be in the OU.
>>> > So, you have a new OU and a new GPO linked to it, and in this
>>> > OU you placed the TS server, and you set loopback on in replace
>>> > mode in the linked GPO. Good. I noticed that you referred to
>>> > this GPO as a "restricted GPO" and I am not certain what you
>>> > intended by that "restricted". By default, a GPO will be set to
>>> > apply to all accounts via the Authenticated Users group, which
>>> > will include the TS server itself and all domain users that might
>>> > log into it. Notice that the setting to turn on loopback processing
>>> > is in the computer tree of policy settings. So, in normal course of
>>> > events, computer policies are applied to computers objects contained
>>> > in the OU where a GPO is linked. When this happens on your new
>>> > OU the loopback setting is seen. This in turn causes it to enable use
>>> > of the users tree of policy settings (in merge or replace mode as has
>>> > been selected) whenever there is a user account login session with
>>> > the machine. If you have altered the security filtering of the GPO,
>>> > so that it no longer has read and apply for Authenticated Users, then
>>> > you need to grant read and apply for the TS machine and for all user
>>> > accounts that should have the loopback settings applied to them.
>>> >
>>> > If you are finding that the settings you make in the user policy tree
>>> > of the loopback GPO are being applied to users no matter where
>>> > they log in, then check and make sure that the loopback GPO is
>>> > linked only to your new TS containing OU. For example, if it is
>>> > also linked to the domain object then one will see the settings
>>> > always being applied for all logins at any machine.
>>> >
>>> > --
>>> > Roger Abell
>>> > Microsoft MVP (Windows Server System: Security)
>>> > MCSE (W2k3,W2k,Nt4) MCDBA
>>> > "Gregg Hill" <bogus@nowhere.com> wrote in message
>>> > news:%23RX5nWsyEHA.3844@TK2MSFTNGP12.phx.gbl...
>>> >> Thank you for helping a desperate soul!
>>> >>
>>> >> If I understand your suggestions, that is what I have set up already.
>>> >> Let
>>> >> me
>>> >> try to clarify if what you are suggesting is the same as what I have,
>>> >> or
>>> >> if
>>> >> I misunderstand something here (the more likely scenario!). I am
>>> >> barely
>>> >> familiar with group policies, so please bear with me.
>>> >>
>>> >> First of all, my assumption is that all of the OU and GPO setup is
>>> >> done
>>> >> on
>>> >> the 2003 domain controller and not on the TS itself, including any
>>> >> loopback
>>> >> settings. Also, roaming profiles are not being used.
>>> >>
>>> >> Container 1:
>>> >> When you say Container 1, would that be equal to the new OU that I
>>> >> created
>>> >> and named "Terminal Server OU"? I think we are talking about the same
>>> >> thing.
>>> >> If so, then I think I have the first half of your step 1 done, since
>>> >> I
```

microsoft.public.windows.group_policy: Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

```
>>> > used
>>> >> ethod 1 from "How to Apply Group Policy Objects to Terminal Services
>>> >> Servers" http://support.microsoft.com/?kbid=260370 to set up the new
>>> >> OU
>>> > with
>>> >> the terminal server as the only thing in it, then set up a new
>> restricted
>>> >> GPO, named "Terminal Server Policy", under that new OU.
>>> >>
>>> >> For the second half of your step 1, I used 260370's Method 2 link to
>>> >> http://support.microsoft.com/?id=231287 to set up loopback processing
>> on
>>> > the
>>> >> "Terminal Server Policy" GPO that is linked to the "Terminal Server
>>> >> OU"
>> I
>>> >> had created. I used Replace mode. The way that article 260370 is
>> written,
>>> > it
>>> >> almost sounds if I am supposed to use one or the other method, but
>>> >> not
>>> > both
>>> >> at the same time, although I did use both methods, since everyone
>>> >> else
>>> >> recommended it.
>>> >>
>>> >> I don't think I understand exactly where the loopback is supposed to
>>> >> be
>>> >> applied. When I first read the article, I thought I should apply the
>>> >> loopback to the "Terminal Server Policy" GPO that I created under my
>> new
>>> >> "Terminal Server OU." Now I am not sure if that is correct.
>>> >>
>>> >> What does article 231287 mean by "Loopback is supported only in a
>> purely
>>> >> Windows 2000 based environment"? Does that mean it cannot have NT in
>> the
>>> >> picture as it seems to say, or that this method will not work with a
>> mix
>>> > of
>>> >> 2003DC, 2000TS, and XP workstations, either?
>>> >>
>>> >> Article 231287 says that "If this policy is enabled, the location of
>>> >> a
>>> >> users's computer object is the main factor in determining which set
>>> >> of
>>> > Group
>>> >> Policy objects are to be applied." The only GPO to which loopback is
>>> > applied
>>> >> is the Terminal Server Policy inside the Terminal Server OU.
>>> >> Something
>> is
>>> >> overriding this setting and applying it to all users who log into any
>>> >> machine.
>>> >>
>>> >> When you say "Container 1 - this OU contains the Terminal Server
>> computer
>>> >> account, and the Group policy for the Terminal Server with local
>> loopback
>>> >> turned on", it sounds as though you used both Method 1 and Method 2
>>> >> in
>>> >> article 260370 noted above. Is that correct?
```

```
>>> >>
>>> >> Container 2:
>>> >> All the workstations are under the Computers container. The terminal
>>> > server
>>> >> was under there when it joined the domain, but has been moved per
>> 260370
>>> > to
>>> >> the newly created "Terminal Server OU" item. I think that takes care
>>> >> of
>>> > step
>>> >> two. The machine account of the terminal server has been added to the
>>> >> security properties of the GPO that I created with Apply Group Policy
>> and
>>> >> Read permissions set.
>>> >>
>>> >> Container 3:
>>> >> I have not changed anything, so I assume this container is the
>>> >> default
>>> > Users
>>> >> container.
>>> >>
>>> >> Final analysis: you said that "So, when a user account in container3
>> logs
>>> >> into workstation that's in container2, there would be no way the
>>> >> Group
>>> >> Policy for term server would be applied", yet that is precisely what
>>> >> is
>>> >> happening. I have done this in three different test domains and it
>> always
>>> >> happens the same way.
>>> >>
>>> >> I have to be missing something!
>>> >>
>>> >> Gregg Hill
>>> >>
>>> >>
>>> >>
>>> >> <harrykrishna.nospam@online.ie> wrote in message
>>> >> news:2f6fp0178s8gtqbe0o936t9klssmfnfbk6g@4ax.com...
>>> >> > Please excuse me if I missed something, but here's essentially what
>>> >> > you should have:
>>> >> >
>>> >> > Container1 - this OU contains the Terminal Server computer account,
>>> >> > and the Group policy for the Terminal Server with local loopback
>>> >> > turned on.
>>> >> >
>>> >> > Container2 - this would contain the various workstation accounts,
>>> >> > including the workstation account for the machine that will be
>>> >> > connecting to the term server
>>> >> >
>>> >> > Container3 - user accounts, including the user account used to
>> connect
>>> >> > to the term server.
>>> >> >
>>> >> > Note that only container1 need be the way I described it. Just make
>>> >> > sure that any workstations you do NOT want to have the Group Policy
>>> >> > apply to are NOT in this container. )Also don't have user accounts
>>> >> > explicitly live there either).
>>> >> >
>>> >> > So, when a user account in container3 logs into workstation that's
>>> >> > in
>>> >> > container2, there would be no way the Group Policy for term server
```

microsoft.public.windows.group_policy: Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

```
>>> >> > would be applied. However, once logged in, the same user,
>>> >> > connecting
>>> >> > from the same workstation, would have the term serv Group Policy
>>> >> > applied to them when logging on the term server.
>>> >> >
>>> >> > Hope this helps, but if it just muddies the waters, please forgive!
>>> >> >
>>> >> >
>>> >> >
>>> >> > "Gregg Hill" <bogus@nowhere.com> wrote:
>>> >> >
>>> >> >>Roger,
>>> >> >>
>>> >> >>Can you recommend a book that goes into depth about securing
>>> >> >>Terminal
>>> >> >>Server? What about a good book for AD and GPO stuff?
>>> >> >>
>>> >> >>Thanks again!
>>> >> >>
>>> >> >>Gregg Hill
>>> >> >>
>>> >> >>
>>> >> >>"Roger Abell [MVP]" <mvpNoSpam@asu.edu> wrote in message
>>> >> >>news:%2311efThyEHA.3624@TK2MSFTNGP09.phx.gbl...
>>> >> >>> Hi Gregg
>>> >> >>>
>>> >> >>> To get different user policies applied to an account when
>>> >> >>> it logs into a TS session as compared to when the account
>>> >> >>> is used for a direct workstation login, you need to have the
>>> >> >>> TS server(s) in an OU to which you have linked a GPO that
>>> >> >>> is set to do loopback processings and that carries the user
>>> >> >>> policies to be used for a TS login session.
>>> >> >>> http://support.microsoft.com/?id=231287
>>> >> >>>
>>> >> >>> --
>>> >> >>> Roger Abell
>>> >> >>> Microsoft MVP (Windows Server System: Security)
>>> >> >>> MCDBA, MCSE W2k3+W2k+Nt4
>>> >> >>> "Gregg Hill" <bogus@nowhere.com> wrote in message
>>> >> >>> news:uLP5N1JyEHA.3416@TK2MSFTNGP09.phx.gbl...
>>> >> >>>> OK, I have Googled for HOURS over a period of about a week and
>>> >> >>>> read
>>> >> >>>> every
>>> >> >>>> article I can find on getting a GPO to apply ONLY to a Terminal
>>> >> >>>> > Server
>>> >> >>>> login and not any other computer on this planet. Basically, my
>>> >> >>>> > problem
>>> >> >>>> > is
>>> >> >>>> > that the GPO gets applied to a user logging into the local
>>> >> >>>> > workstation
>>> >> >>>> > as
>>> >> >>>> > well as when the user logs into the Terminal Server.
>>> >> >>>>
>>> >> >>>> Here are the details. Sorry it is so long, but I wanted to make
>>> >> >>>> > my
>>> >> >>>> > dilemma as clear as possible.
>>> >> >>>>
>>> >> >>>> If I cannot get this fixed by Saturday morning, I will have to
>>> >> >>>> > call
>>> >> >>>> > Microsoft.
>>> >> >>>> >>>>
```

microsoft.public.windows.group_policy: Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

```
>>> >> >>>> *****Start of previous message to other
>>> >> >>>> newsgroups*****
>>> >> >>>> I originally posted this problem in the
>>> >> >>>> microsoft.public.windowsnt.terminalserver.setup group. Vera
>>> >> >>>> Noest
>>> >> >>>> has
>>> >> >>>> been a TREMENDOUS help with other TS problems and pointed out
>>> >> >>>> some
>>> >> >>>> of
>>> >> >>>> the
>>> >> >>>> articles noted here, but I have one major problem that I cannot
>> get
>>> >> >>>> past.
>>> >> >>>>
>>> >> >>>> I have a test setup running (Windows Server 2003 Standard as a
>>> >> >>>> domain
>>> >> >>>> controller and licensing server, 2000 TS member server, and two
>>> >> >>>> XP
>>> > Pro
>>> >> >>>> SP2 clients) to test group policies to secure a Windows 2000
>>> >> >>>> Terminal
>>> >> >>>> Server in a Windows Server 2003 domain. I have tried this setup
>> with
>>> >> >>>> two
>>> >> >>>> different sets of servers (two complete test domains at
>>> >> >>>> different
>>
>>> >> >>>> locations).
>>> >> >>>>
>>> >> >>>> I used "How to Apply Group Policy Objects to Terminal Services
>>> > Servers"
>>> >> >>>> http://support.microsoft.com/?kbid=260370 and set up the new OU
>> with
>>> >> >>>> the
>>> >> >>>> terminal server as the only thing in it, then set up the
>> restricted
>>> > GPO
>>> >> >>>> under that new OU. That secured the TS, but every article I find
>>> >> >>>> says
>>> >> >>>> in
>>> >> >>>> order to limit the restrictions to only the terminal server
>>> >> >>>> itself
>>> > and
>>> >> >>>> not to workstation logons, you must use loopback processing per
>>> >> >>>> http://support.microsoft.com/default.aspx?scid=kb;en-us;231287.
>>> >> >>>> Well,
>>> > I
>>> >> >>>> enabled loopback, put the machine account into the GPO as
>> suggested
>>> > by
>>> >> >>>> Vera Noest and the last part of article 260370, but the policy
>> still
>>> >> >>>> gets
>>> >> >>>> applied no matter where the test user logs in. In article
>>> >> >>>> 260370,
>>> >> >>>> are
>>> >> >>>> Method 1 and Method 2 exclusive of each other, or should I still
>> use
>>> >> >>>> loopback if I have Method 1 in place?
>>> >> >>>>
>>> >> >>>> Apparently, GPOs are getting applied differently than the MS
>>> >> >>>> documentation suggests. I have read and applied the following
```

microsoft.public.windows.group_policy: Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

```
>>> >> >>>> documents:
>>> >> >>>>
>>> >> >>>> 260370 - How to Apply Group Policy Objects to Terminal Services
>>> > Servers
>>> >> >>>> http://support.microsoft.com/?kbid=260370
>>> >> >>>>
>>> >> >>>> Loopback Processing of Group Policy
>>> >> >>>> http://support.microsoft.com/default.aspx?scid=kb:en-us;231287
>>> >> >>>>
>>> >> >>>> 816100 - How To Prevent Domain Group Policies from Applying to
>>> >> >>>> Administrator
>>> >> >>>> Accounts and Selected Users in Windows Server 2003
>>> >> >>>> http://support.microsoft.com/?kbid=816100
>>> >> >>>> I applied this one to Domain Administrators and Enterprise
>>> >> >>>> Administrators.
>>> >> >>>>
>>> >> >>>> 278295 - How to Lock Down a Windows 2000 Terminal Services
>>> >> >>>> Session
>>> >> >>>> http://support.microsoft.com/?kbid=278295
>>> >> >>>>
>>> >> >>>> Locking Down Windows Server 2003 Terminal Server Sessions
>>> >> >>>>
>>> >
>> http://www.microsoft.com/windowsserver2003/techinfo/overview/lockdown.msp
>>> >> >>>>
>>> >> >>>> After setting up the new OU for the terminal server and setting
>>> >> >>>> up
>>> > the
>>> >> >>>> GPO, when I log onto either of my XP Pro workstations as the
>>> >> >>>> test
>>> >> >>>> domain
>>> >> >>>> user, the restricted GPO for the terminal server gets applied to
>> my
>>> >> >>>> local
>>> >> >>>> workstation. It gets applied to the TS session as expected, but
>> why
>>> >> >>>> does
>>> >> >>>> this policy get applied on my workstation when the ONLY thing in
>> the
>>> >> >>>> Terminal Server OU is the actual terminal server? I did not move
>>> > users
>>> >> >>>> into any new groups; they are still in the default locations.
>>> >> >>>>
>>> >> >>>> I started all over again by deleting the GPOs and OUs I had
>> created.
>>> > I
>>> >> >>>> opened AD Users and Computers, created a new OU in the domain
>>> >> >>>> and
>>> > named
>>> >> >>>> it "Terminal Server." I moved the actual terminal server from
>>> >> >>>> the
>>> >> >>>> Computers group to the new Terminal Server OU. I added a GPO
>>> >> >>>> under
>>> > the
>>> >> >>>> Terminal Server OU and named it Terminal Server Policy. In that
>>> >> >>>> Terminal
>>> >> >>>> Server Policy, I made only three changes to the policy so I
>>> >> >>>> could
>>> > test
>>> >> >>>> its application: 1) I enabled loopback processing, 2) I enabled
>>> >> >>>> "Interactive logon: Do not display last user name" and 3) I
>> disabled
```

Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

microsoft.public.windows.group_policy: Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!

```
>>> >> >>>> the
>>> >> >>>> Windows Installer under Computer Configuration, Admin Templates,
>>> >> >>>> Windows
>>> >> >>>> Components, Windows Installer.
>>> >> >>>>
>>> >> >>>> Now, if I try to install an MSI package on the 2003 server or on
>> my
>>> > XP
>>> >> >>>> Pro workstations, it will not run and says that policies are
>>> > preventing
>>> >> >>>> it from running, and if I log off and back on again, the user
>>> >> >>>> name
>>> >> >>>> is
>>> >> >>>> blank, too.
>>> >> >>>>
>>> >> >>>> Why is a GPO that is under the newly created "Terminal Server"
>>> >> >>>> OU
>>> > being
>>> >> >>>> applied to the users on their XP workstations? I thought the
>>> >> >>>> whole
>>> >> >>>> purpose of the separate OU for the terminal server was to
>>> >> >>>> restrict
>>> >> >>>> application of the GPO within it to only the terminal server in
>> the
>>> >> >>>> Terminal Server OU.
>>> >> >>>>
>>> >> >>>> What am I doing wrong?
>>> >> >>>>
>>> >> >>>> Gregg Hill
>>> >> >>>>
>>> >> >>>
>>> >> >>>
>>> >> >>
>>> >> >
>>> >> >
>>> >> > Ha@@y
>>> >> >
>>> >> > HarryKrishna.nospam@online.ie
>>> >>
>>> >>
>>> >>
>>> >
>>> >
>>>
>>>
>>
>>
>
>
```

Re: Getting desperate: GPO applying incorrectly, PLEASE HELP ME!!