

RE: Group Policy Connundrum – Stick with it, its confusing!!!

RE: Group Policy Connundrum – Stick with it, its confusing!!!

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2007-10/msg00041.html>

- *From:* "Roger A. Grimes" <roger@xxxxxxxxxxxxxxxx>
 - *Date:* Tue, 2 Oct 2007 19:08:28 -0400
-

Yes, GPO's can only be applied to OUs. Those OUs can contain user or computer objects. If you want to apply a particular GPO to a user account, you must configure the appropriate settings to the User Configuration object of the GPO (vs. Computer Configuration object), link the GPO to the OU (or let it be inherited into the OU from a parent OU) that contains the appropriate user accounts, and the user accounts must have the Read and Apply Group Policy permissions on the GPO in question. That latter portion can be accomplished using security groups to set the correct permissions.

Roger

*Roger A. Grimes, InfoWorld, Security Columnist
*CPA, CISSP, CISA, MCSE: Security (2000/2003), CEH, yada...yada...
*email: roger_grimes@xxxxxxxxxxxxxxxx or roger@xxxxxxxxxxxxxxxx
*Author of Windows Vista Security: Securing Vista Against Malicious Attacks (Wiley)
*<http://www.amazon.com/Windows-Vista-Security-Securing-Malicious/dp/0470101555>

-----Original Message-----

From: Jon Petre [<mailto:jono-31@xxxxxxxxxxxxxxxx>]
Sent: Tuesday, October 02, 2007 12:42 PM
To: Roger A. Grimes
Cc: security-basics@xxxxxxxxxxxxxxxx
Subject: RE: Group Policy Connundrum – Stick with it, its confusing!!!

Hi Roger,

OK. I have ran a couple of the test's that you recommended and would really appreciate your input:

This is the output from gpreresult on the local workstation – I have omitted the computer policies and just included the user policies.

RE: Group Policy Connundrum – Stick with it, its confusing!!!

RE: Group Policy Connundrum – Stick with it, its confusing!!!

CN=D*****,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=P*****Ltd,DC=local
Last time Group Policy was applied: 02/10/2007 at 10:36:05
Group Policy was applied from: dcserver.*****.local
Group Policy slow link threshold: 500 kbps

Applied Group Policy Objects

Default Domain Policy
No Internet

The following GPOs were not applied because they were filtered out

Small Business Server Internet Connection Firewall
Filtering: Denied (WMI Filter)
WMI Filter: PreSP2

Small Business Server Windows Firewall
Filtering: Not Applied (Empty)

Small Business Server Client Computer
Filtering: Not Applied (Empty)

Small Business Server Domain Password Policy
Filtering: Not Applied (Empty)

Small Business Server Lockout Policy
Filtering: Disabled (GPO)

Small Business Server Remote Assistance Policy
Filtering: Disabled (GPO)

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
No Internet
SageMMS
Terminal Services Users
Branch Users
Web Workplace Users

Resultant Set Of Policies for User:

RE: Group Policy Connundrum – Stick with it, its confusing!!!

Software Installations

N/A

Public Key Policies

N/A

Administrative Templates

GPO: No Internet
Setting: Software\Policies\Microsoft\Internet
Explorer\Control Panel
State: Enabled

Folder Redirection

N/A

Internet Explorer Browser User Interface

GPO: No Internet
Large Animated Bitmap Name: N/A
Large Custom Logo Bitmap Name: N/A
Title BarText: P***** Ltd
UserAgent Text: N/A
Delete existing toolbar buttons: No

Internet Explorer Connection

HTTP Proxy Server: 0.0.0.0:80
Secure Proxy Server: 0.0.0.0:80
FTP Proxy Server: 0.0.0.0:80
Gopher Proxy Server: 0.0.0.0:80
Socks Proxy Server: 0.0.0.0:80
Auto Config Enable: No
Enable Proxy: Yes
Use same Proxy: Yes

Internet Explorer URLs

GPO: No Internet
Home page URL: N/A
Search page URL: N/A
Online support page URL: N/A

Internet Explorer Security

Always Viewable Sites: N/A
Password Override Enabled: False

RE: Group Policy Connundrum – Stick with it, its confusing!!!

GPO: No Internet
Import the current Content Ratings Settings: No
Import the current Security Zones Settings: No
Import current Authenticode Security Information: No
Enable trusted publisher lockdown: No

Internet Explorer Programs

GPO: No Internet
Import the current Program Settings: No

From this I can see the policy that applies the false proxy but I can not see my exceptions that are in place!! This is rather confusing for me.

After further investigation I believe I am right in saying that GP's are applied to OU's and not security groups. If this is the case, then the AD infrastructure that I am working on is setup incorrectly. All the users are placed in one OU. After carrying out an RSOP on the OU, and then drilling down, I find that no proxy settings are been enabled!! As you can probably see, I am actually quite confused now.

Can you shed further light on this confusing matter. If you require further info, I will be most happy to oblige.

Thanks

Jon

From: "Roger A. Grimes" <roger@xxxxxxxxxxxxxxxx>
To: "Jon Petre"
<jono-31@xxxxxxxxxxxxxxxx>,<security-basics@xxxxxxxxxxxxxxxx>
Subject: RE: Group Policy Connundrum – Stick with it, its confusing!!!
Date: Sun, 30 Sep 2007 15:07:01 -0400

Jon,

There are lots of ways to troubleshoot.

Try running an rsop.msc on the workstation and look at the relevant results.

Or you can run gpresult.exe /v >gpresult.txt && gpresult.txt and look at it in a text file.

RE: Group Policy Connundrum – Stick with it, its confusing!!!

RE: Group Policy Connundrum – Stick with it, its confusing!!!

Are the correct settings being pushed down? If so, then it might be a GPO application problem. You can turn on group policy logging and see what is not being applied, and why.

If rsop.msc and gpresult show the correct settings, are the correct registry edits being made under HKCU\Software\Policies?

I'll help you troubleshoot.

Roger

*Roger A. Grimes, Senior Security Consultant *Microsoft Application Consulting and Engineering (ACE) Services
*http://blogs.msdn.com/ace_team/default.aspx
*CPA, CISSP, CISA MCSE: Security (2000/2003), CEH, yada...yada...
*email: roger@xxxxxxxxxxxxxx or rogrim@xxxxxxxxxxxxxx *Author of Windows

Vista Security: Security Vista Against Malicious Attacks (Wiley)
*<http://www.amazon.com/Windows-Vista-Security-Securing-Malicious/dp/0470101555>
0
101555

-----Original Message-----
From: listbounce@xxxxxxxxxxxxxxxxxxxxx
[\[mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx\]](mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx)
On Behalf Of Jon Petre
Sent: Friday, September 28, 2007 5:09 AM
To: security-basics@xxxxxxxxxxxxxxxxxxxxx
Subject: Group Policy Connundrum – Stick with it, its confusing!!!

Hello List,

I have an issue at a customers site regarding GP that goes a little like this:

I have created a policy named no internet. I have created a security group named the same. In this group are so many users based across the country that I want to limit the internet usage, therefore I have created a false proxy @ 0.0.0.0 that all their internet use has to pass

RE: Group Policy Connundrum – Stick with it, its confusing!!!

through. This gives the expected result where no pages are displayed regardless of which site the user goes to. I have also created some exceptions for this policy, which do not use the proxy, i.e.

www.homepageofcompany.com, www.siteiwanttoallow.com,
www.theusercangohere.co.uk.

This is done by setting the 'user configuration > Internet Explorer > Connection > Proxy Settings > Exceptions'. The desired output is that user's logon and can access these sites, but any other non specified site wont work.

----I hope this makes sense so far----

Then by setting the 'Admin Template > Windows Components > Internet Explorer > Disable Changing Proxy Settings' to enabled effectively grays out the proxy settings in internet explorer and stops the user from altering the settings.

OK, this is where the issues start. When I toggle the 'Admin Template >

Windows Components > Internet Explorer > Disable Changing Proxy Settings'

between enable and disable, and update the policy on the local machine via GPUPDATE, or even from the server by forcing the update, everything

works and the proxy is enabled and disabled as specified.

However, when I try to make changes to any part of the user config, the policy does not seem to initialise. What I mean is any sites I add to the exception list do not appear and the end result is the user can not access any sites at all. I have logged on and off, and re-booted workstation all to no effect.

Any suggestions on why the user configuration portion of the Group Policy does not work would be much appreciated. I am sure all the permissions are set correctly, i.e. the apply GP settings, read settings etc. If they wasn't, then surely no part of the policy would work, would it?

TIA,

Jono

The next generation of Hotmail is here! <http://www.newhotmail.co.uk>

RE: Group Policy Connundrum – Stick with it, its confusing!!!

Get Pimped! FREE emoticon packs from Windows Live –
<http://www.pimpmylive.co.uk>