

Re: Domain Policy

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2007-10/msg00027.html>

- *From:* Shabbir Jadliwala <ShabbirJadliwala@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 19 Oct 2007 06:33:03 -0700
-

Hi Steven,

Thanks very much.. I finally got that fixed.. Couldn't find the key for MMC, but found one, which would allow me to use Registry locally, and from there on, I was able to find Microsoft Management Console and enable the AD and got the policy removed.

Well, it was a good learning experience.. Never changed so many registry keys, specially on the PDC.

Thanks again,

Shabbir

"Steven L Umbach" wrote:

You can delete those subkeys or change the value to 0 as I believe you will see they are currently 1. They are preventing you from accessing your MMC snapins. You may have to logoff and logon the DC when done for the changes to take.

Steve

"Shabbir Jadliwala" <ShabbirJadliwala@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:DA2FBCA3-1472-412A-BED1-8B164982CAFF@xxxxxxxxxxxxxxxxxxxxx

Hi Steve,

I found the MMC key in Registry under HKLM\Software\Microsoft\MMC, but there is no place where it says to disable access.. I only has {.....} sub keys for different applications and wasn't sure how to enable them?

Any help is really appreciated.

Re: Domain Policy

Best Regards,

Shabbir

"Steven L Umbach" wrote:

First from the server you can access the registry remotely see if you can manage Group Policy remotely to undo your changes. While on that server enter MMC in the run box to open Management Console and then add the Group Policy Object Editor and instead of local computer select another computer – browse and browse for and select the domain controller and you may then be able to edit domain level Group Policy.

If that does not work use the registry editor. You are not looking for the policy itself but you want to edit/remove the registry keys that are locking you out to give you a change to then edit Group Policy to remove those settings. You want to look for registry keys/entries under HKCU\Software\Policies\Microsoft\Windows such as system where if you see DisableCMD you want to delete that dword entry. Under HKCU\Software\Policies\Microsoft\Windows\MMC if you see any items listed {numbers and letters} either remove the {numbers and letters} or change the restrict run values to 0. After that you should be able to open access ADUC and edit Group Policy though you may need to logoff/logon the domain controller or reboot the server first.

Group Policy enforces those registry settings and the next time Group Policy is applied those registry entries will return which is why it is important that you edit Group Policy ASAP after gaining access

Re: Domain Policy

starting with those
settings that locked you out..

Steve

"Shabbir Jadliwala"

<ShabbirJadliwala@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote

in

message

news:541A33B4-26D2-4E3D-9859-943BE629B265@xxxxxxxxxxxxxxxxxxxx

Hi Steven,

I can't get on the Registry locally on the
server as well. But can do
it
remotely from another server, which is not a
Domain Controller. I tried
searching my policy in there, but couldn't
find it in there. Is there
any
other place I can find it?

Thanks for your help.

Best Regards,

Shabbir

"Steven L Umbach" wrote:

Try logging onto a domain
computer [non critical
workstation] as
domain
admin and see if you can
run regedit or if you can run
a tool called
Dial
a
Fix from a flash drive or
such as it can detect and
remove many Group
Policy
restrictions. If that works
then you can use MMC
snapin for Group
Policy
to

Re: Domain Policy

manage the Group Policy on a domain controller to make changes to undo the harm. Otherwise if you can use regedit look for and delete the Group Policy restrictions seen under the keys listed below which will buy you time to make changes to Group Policy.

Steve

<http://www.softpedia.com/get/System/System-Miscellaneous/Dial-a-fix.shtml>

-- Dial a fix

Table 1 Approved Registry Key Locations for Group Policy Settings

For Computer Policy Settings:
For User Policy Settings:
HKLM\Software\Policies (The preferred location)
HKCU\Software\Policies (The preferred location)

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies

"Shabbir Jadliwala"

<Shabbir

Jadliwala@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote

in

message

news:733AF4FD-9341-47EB-8363-EC442BA03A66@xxxxxxxxxxxxxxxxxxxx

I have had set up a policy to block all

Re: Domain Policy

users with
any rights
other
then
the
basic ones.
But by
mistake I
have had
applied to
all, instead
of the
group,
and now I
can do any
changes to
it myself,
even though
I am logged
in
as
the
Administrator.

Is there any
way, I can
get it reset
back to
original. I
don't have
access
to my local
drives or
command
prompt or
AD or
anything
right now.

Any help
would be
really
appreciated.

Best
Regards,

Shabbir

Re: Domain Policy