

Re: GPO for Remote Desktop and Firewall Settings

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.group_policy/2005-07/msg00244.html

- *From:* "Bruce Sanderson" <bsanders@xxxxxxxx>
 - *Date:* Fri, 22 Jul 2005 13:00:14 -0700
-

Remote Desktop has to be enabled on the target computer and appropriate user accounts (or groups) authorized. This is independant of any Firewall settings (well, you have to also make the appropriate firewall exceptions – looks like you have that in hand) and also independant of Remote Assistance. These settings will work with computers running Windows 2000 SP2 or later, Windows XP (any SP) and Windows 2003 Server.

To enable Remote Desktop via GPO:

Computer Configuration

Windows Settings

Security Settings

Local Policies

User Rights Assignment

Allow log on through Terminal Services – specify the users accounts or groups that you want to be able to use Remote Desktop

Administrative Templates

Windows Components

Terminal Services

Allow users to connect remotely using Terminal Services

Make sure that the target computers are actually using the Domain Firewall Profile and your exceptions via GPO are actually applied:

netsh firewall show state

If you think the firewall is blocking the Remote Desktop, turn on the firewall logging (Firewall configuration, Advanced tab, Security Logging, Log dropped packets).

--

Bruce Sanderson MVP Printing

<http://members.shaw.ca/bsanders>

It is perfectly useless to know the right answer to the wrong question.

"Smurfman" <smurfman@xxxxxxxxxxxxxxxx> wrote in message
<news:1A67FEC2-9472-4B9E-AA13-221CA631A494@xxxxxxxxxxxxxxxx>

Re: GPO for Remote Desktop and Firewall Settings

> Thanks guys, in answer to your post Denis, I think I have it set
> correctly...
> pasted below is the settings as shown in the GPO Edit, thanks.
>
> J
>

> Windows Firewall: Allow remote administration exception Enabled
> Allow unsolicited incoming messages from: localsubnet
>
> Syntax:
> Type "*" to allow messages from any network, or
> else type a comma-separated list that contains
> any number or combination of these:
> IP addresses, such as 10.0.0.1
> Subnet descriptions, such as 10.2.3.0/24
> The string "localsubnet"
> Example: to allow messages from 10.0.0.1,
> 10.0.0.2, and from any system on the
> local subnet or on the 10.3.4.x subnet,
> type the following:
> 10.0.0.1,10.0.0.2,localsubnet,10.3.4.0/24
>

>
>
>
>
> "Denis Wong @ Hong Kong" wrote:
>
>> Hi,
>>
>> Have you set this?
>>
>> Comp Config\Administrative Templates\Network\Network Connections\Windows
>> Firewall\Domain Profile\Windows Firewall: Allow Remote Desktop exception
>>
>> At least Microsoft Windows XP Professional with SP2
>>
>> "Allows this computer to receive Remote Desktop requests. To do this,
>> Windows Firewall opens TCP port 3389. If you enable this policy
>> setting,
>> Windows Firewall opens this port so that this computer can receive Remote
>> Desktop requests. You must specify the IP addresses or subnets from which
>> these incoming messages are allowed. In the Windows Firewall component of
>> Control Panel, the Remote Desktop check box is selected and
>> administrators
>> cannot clear it. If you disable this policy setting, Windows Firewall
>> blocks this port, which prevents this computer from receiving Remote
>> Desktop
>> requests. If an administrator attempts to open this port by adding it to
>> a
>> local port exceptions list, Windows Firewall does not open the port. In
>> the

Re: GPO for Remote Desktop and Firewall Settings

>> Windows Firewall component of Control Panel, the Remote Desktop check box
>> is
>> cleared and administrators cannot select it. If you do not configure
>> this
>> policy setting, Windows Firewall does not open this port. Therefore, the
>> computer cannot receive Remote Desktop requests unless an administrator
>> uses
>> other policy settings to open the port. In the Windows Firewall component
>> of
>> Control Panel, the Remote Desktop check box is cleared. Administrators
>> can
>> change this check box."
>>
>> br,
>> Denis
>>
>> "Smurfman" <smurfman@xxxxxxxxxxxxxxxx> wrote in message
>> news:188C662C-7D06-46E6-A515-160FD000E871@xxxxxxxxxxxxxxxx
>> > Hello, I am attempting to get the Remote Desktop feature to work.
>> >
>> > I have a GPO that is doing some of the following according to the GPO
>> Results
>> > I have pasted below the settings that were applied. On the client I am
>> > seeing the Remote assistance and the 135 port enabled, via a policy,
>> > but
>> > what
>> > I do not see happen is the enabling of the Remote Desktop. Thus I am
>> getting
>> > denied access, with the error related to the system not being
>> > available.
>> >
>> > I must have missed something obvious, but basically I am looking to
>> > enable
>> > the remote desktop feature in which I would initiate the connection and
>> the
>> > user could say yes or no...rather than the user asking me for
>> > assistance...i'll cross that bridge when I get there...
>> >
>> > Any ideas? Thanks
>> > J
>> >
>> >
>> >

>> > Offer Remote Assistance Enabled Level 2 – Lockdown
>> > Permit remote control of this computer: Allow helpers to remotely
>> > control
>> > the computer
>> > Helpers:
>> > DOMAIN\Domain Admins
>> > DOMAIN\User One
>> > DOMAIN\User Two

