

APPLICATION NOTE

Windows XP Service Pack 2 - Remote Administration Enable

The default installation of Windows XP, Service Pack 2 automatically enables the Windows Firewall. This is an advantage in one sense and a problem in another. It's an advantage because, in its default configuration, the firewall allows no outside communication to the client. Of course, it's a disadvantage for the same reason – Desktop Auditor needs to communicate by Remote Procedure Call (RPC) with the remote machines and the firewall prevents this. To overcome this, we need to enable remote administration on the target PCs.

To enable remote administration on XP nodes with Service Pack 2 installed, use one of the following three methods.

1. Locally enable remote administration

The simplest approach, if there are not many nodes to deal with, is to enable remote administration locally on each node. On each machine with Win XP Service Pack 2, do the following:

1. Click **Start**, click **Run**, type **gpedit.msc**, and then click **OK**.
2. Under **Console Root**, expand **Computer Configuration**, expand **Administrative Templates**, expand **Network**, expand **Network Connections**, expand **Windows Firewall**, and then click **Domain Profile**.
3. Right-click **Windows Firewall: Allow remote administration exception**, and then click **Properties**.
4. Click **Enabled**, and then click **OK**.

2. Use a script

If you have a significant number of nodes, then an alternative approach is to use a script. Bear in mind that, as Service Pack 2 has turned off all remote administration, the script must be run locally on the machine. This looks like 'Catch 22' - to be able to do things remotely, you must first do something locally. The only way round this would be Group Policy deployment. You will need to deploy a group policy which runs this script as a start-up script (not a login script - a start-up script runs under system rights while a log-in script runs under user rights and users will not have administrative rights to change firewall settings so the script would fail). You can see the use of a script which looks at firewall remote admin settings on <http://www.microsoft.com/technet/scriptcenter/solutions/appcompat/fwremoteadminsettings-vbs.mspx> . Here is a simpler script which you can cut and paste into a notepad document and save with .vbs extension:

```
set objFW=createobject("HNetCfg.FwMgr")
set objPol = objFW.LocalPolicy.CurrentProfile
set objAS = objPol.RemoteAdminSettings
objAS.Enabled = True
```

It will set the remote enable settings to true on the local computer.

3. Use Group Policy

A third approach is to use group policy.

If you try to use Group Policy Management Console's (GPMC's) Group Policy Results Wizard to determine the effect of policies on a specific Service Pack 2 machine on which the firewall is enabled, you get an error message.

To correct this problem, you could disable the firewall, but that isn't a good idea. Instead, leave it enabled and open only the port necessary to allow remote procedure call (RPC) communication (port 135). Create a GPO that opens port 135 and link the GPO to the domain level. The *Windows Firewall: Allow remote administration exception* policy does this; you'll find it under Computer Configuration\Administrative Templates\Network\Network\Connections\Windows Firewall\Domain Profile. Simply enable this policy setting - you can optionally specify from which addresses the target machine should allow requests (you could put the IP address of the Desktop Auditor server here) - and the Group Policy Results Wizard will continue to work as it did before you loaded SP2. Be aware that this policy also opens port 445, which allows Server Message Block (SMB) traffic so that administrators can manipulate files on remote machines.

© Robiac Ltd., February 2005