

► Configuring the Windows XP SP2/Vista Firewall for UserLock

Due to the modification of the Firewall's activation setting, that occurs when Service Pack 2 is deployed on a XP workstation, all incoming network requests are blocked instantly. This means complete loss of all remote access to the workstation, even a straight forward ping! The workstation also becomes completely invisible to all network tools, so you are no longer able to administer it. In particular you will not be able to deploy the *UserLock* agent and remotely logoff users using the UserLock administration console.

To fix this, the Firewall settings need specific updating. You can do this directly on the workstation but if you are in charge of a Windows network, the best way is to configure the firewall using Group or System Policies.

- - - - -

.: Change Firewall settings using Group Policy :. (for Windows 2000/2003/2008 domains)

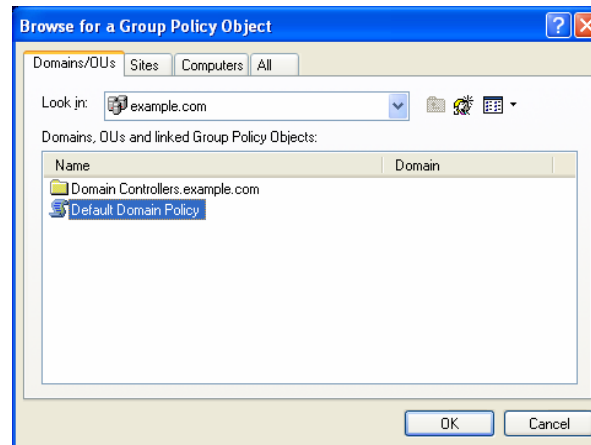
■ Step 1: Update your Group Policy Objects with the new Firewall Settings

Important: this step is not needed for Windows Server 2003 SP2 or Windows server 2008.

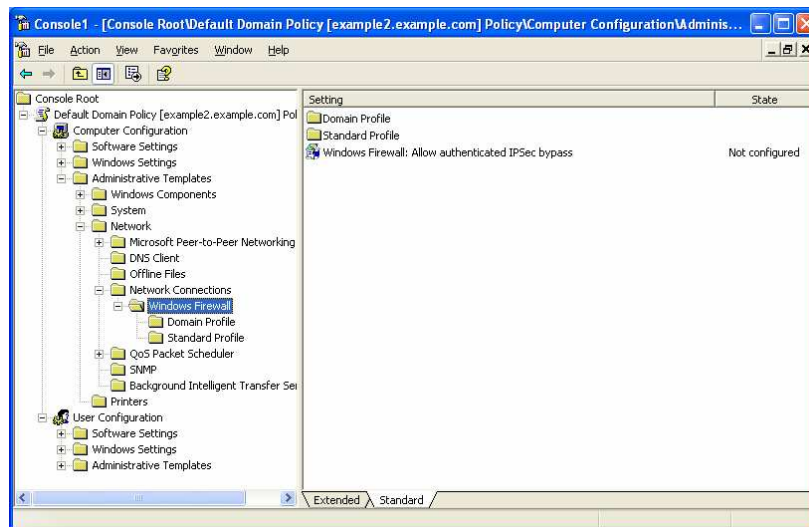
→ *This section is an extract of the Microsoft document “[Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2](#)”. For more information you can download this document directly from the Microsoft web site.*

To update your Group Policy Objects with the new Windows Firewall settings using the Group Policy Snap-In (provided with Windows XP), you need to do the following:

1. Install Windows XP SP2 on a computer that is a member of the domain that contains the computer accounts of the other computers running Windows XP on which you plan to install Windows XP SP2.
2. Restart the computer and log on to the Windows XP with SP2-based computer as a member of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group.
3. From the Windows XP desktop, click **Start**, click **Run**, type **mmc**, and then click **OK**.
4. On the **File** menu, click **Add/Remove Snap-in**.
5. On the **Standalone** tab, click **Add**.
6. In the **Available Standalone Snap-ins** list, click **Group Policy Object Editor**, and then click **Add**.
7. In the **Select Group Policy Object** dialog box, click **Browse**.
8. In the **Browse for a Group Policy Object**, click the Group Policy object that you want to update with the new Windows Firewall settings. An example is shown in the following figure.



9. Click **OK**.
10. Click **Finish** to complete the Group Policy Wizard.
11. In the **Add Standalone Snap-in** dialog box, click **Close**.
12. In the **Add/Remove Snap-in** dialog box, click **OK**.
13. In the console tree, open **Computer Configuration, Administrative Templates, Network, Network Connections**, and then **Windows Firewall**. An example is shown in the following figure.



Repeat this procedure for every Group Policy object that is being used to apply Group Policy to computers that will have Windows XP SP2 installed.

► **Note** To update your Group Policy objects for network environments using Active Directory and Windows XP SP1, Microsoft recommends that you use the Group Policy Management Console, a free download. For more information, see [Group Policy Management Console with Service Pack 1](#).

End of the extract from the Microsoft document "Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2"

■ Step 2: Configure Firewall Settings in the Group Policy to enable UserLock

Edit the relevant group policy as explained in the previous section and go to “*Computer configuration/Administrative templates/Network/Network connections/Windows Firewall/Domain profile*”

➤ Enable the setting “*Windows firewall: Allow remote administration exception*”

For extra security, you can specify the IP address of the server as allowed source (instead of * or *localsubnet*). This will eradicate potential auto-contamination from BLASTER like worms.

➤ Enable the setting “*Windows firewall: Allow ICMP exceptions*”, select *Allow inbound request* and click *Ok*.

➤ Enable the setting (For version 3 only) “*Define program exceptions*”, click on *Show*, click *Add* and enter the following line:

```
“%SystemRoot%\system32\LogoffAgent.exe:*:Enabled:UserLock”
```

→ Click *Ok* twice.

Important! If you do this on Windows server 2008 you will see inbound added in the name of most exceptions but this is still the same exception.

■ Step 3: Deploy the UserLock agent and logoff a user on a XP SP2 workstation

At this stage the Group Policy is configured but firewall settings are not yet replicated on all workstations. In order to rapidly test a single XP SP2 workstation, you can manually update it using the command: *gpupdate*. You should then be able to deploy the UserLock agent on it, or remotely logoff a connected user using the UserLock administration console.

- - - - -

..: Change Firewall Settings using System Policy :. (for Windows NT 4 domains)

■ Step 1: Update System Policy with the new Firewall Settings

→ *This section is an extract of the Microsoft document “[Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2](#)”. For more information you can download this document directly from the Microsoft web site.*

➤ Computers running Windows XP that are members of a Windows NT 4.0 domain use System Policy instead of Group Policy. In order to deploy Windows Firewall settings for these computers, you must add the Windows Firewall policy template (the *Wfnt.adm* file), configure Windows Firewall settings, and then distribute the new System Policy file to your Windows NT 4.0 domain controllers. Windows NT System Policy settings are stored in the *Ntconfig.pol* file in the *Netlogon* share of the Windows NT 4.0 domain controller. For more information about Windows NT System Policy, see the [Implementing Profiles and Policies for Windows NT 4.0](#) white paper at http://www.microsoft.com/ntserver/techresources/management/prof_policies.asp.

To configure Windows Firewall settings as part of Windows NT System Policy, do the following:

1. Download the *Wfnt.adm* file from the [Microsoft Download Center](#) at <http://www.microsoft.com/downloads/details.aspx?FamilyID=d67c7085-4bff-4056-8e7e-3d583214e728&DisplayLang=en>.
2. If you are administering Windows NT System Policy from a computer running Windows XP Professional or Windows 2000, install the Windows 2000 Administrative Tools by double-clicking the *Adminpak.msi* file in the *\I386* folder of the Windows 2000 Server product CD if needed. If you are administering Windows NT System Policy from a computer running Windows NT 4.0, skip this step.

3. Click **Start**, click **Run**, type **poledit.exe**, and then click **OK**.

4. From the **System Policy Editor**, click **Options**, and then click **Policy Template**.
5. In the **Policy Template Options** dialog box, click **Add**.
6. In the **Open Template File** dialog box, select the **Wfnt.adm** file from Step 1, and then click **OK**.

End of the extract from the Microsoft document “Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2”

■ Step 2: Configure Firewall Settings in System Policy

- Run *poledit.exe*
- Open the policy file “*Ntconfig.pol*” (or create it if needed) in the *netlogon* share (Commonly in the folder *c:\winnt\system32\repl\import\scripts*) on the domain controller.
- Go to “*Default computer\Windows Firewall\Domain profile*”
- Enable the setting “**Windows firewall: Allow remote administration exception**”
For extra security, you can specify the IP address of the server as allowed source (instead of * or *localsubnet*). This will eradicate potential auto-contamination from BLASTER like worms.
- Enable the setting “**Windows firewall: Allow files and printers exception**”
If possible, restrict the source to IP as explained above.
- Enable the setting “**Windows firewall: Allow ICMP exceptions**”, select *Allow inbound request* and click *Ok*.
- Enable the setting (For UserLock 3 only) “**Define program exceptions**”, click on *Show*, click *Add* and enter the following line:
“**%SystemRoot%\system32\LogoffAgent.exe:*:Enabled:UserLock**”
Click *Ok* twice.
- The System Policy is now configured. Make sure that the file is correctly replicated in the *netlogon* share of all domain controllers.

■ Step 3: Deploy the UserLock agent and logoff a user on a XP SP2 workstation

At this stage the System Policy is configured but Firewall Settings are not yet replicated on all workstations. In order to rapidly test a single XP SP2 workstation, you can reboot it. You should then be able to deploy the UserLock agent on it, or remotely logoff a connected user using the UserLock administration console.

.: Change Firewall Settings manually .:

On each XP SP 2 workstation you need to remotely access, go to the *Control Panel*, display “*Windows Firewall*”, go to the *Exceptions* tab and do the following:

- Enable the **File and printer sharing exception**.
For extra security you can specify the IP address of the server as allowed source (instead of * or *localsubnet*). To do this, edit the *File and printer sharing* exception, click on *Change Scope*, select *Custom list* and enter the IP address.
- For **Windows Vista workstations** you should also allow the **ICMP protocol** in the “*Windows firewall with advanced security*” console available in administration tools. In Inbound rules, enable the “*Networking - Echo request*” rule for the domain profile.
- Add a port exception with **RPC** as name (for UserLock 3 only), **135** as port and with **TCP** selected. If possible, restrict the source to IP as explained above.

- **Add an application exception (for UserLock 3 only) with**
`%SystemRoot%\system32\LogoffAgent.exe` as path. If you are not allowed to do this because the file is not available download the reg file at the following link and execute it:
<http://www.isdecisions.com/download/AllowLogoffAgent.zip>

You should then be able to deploy the UserLock agent on it, or remotely logoff a connected user using the UserLock administration console.

➤ **References :**

Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2
<http://www.microsoft.com/downloads/details.aspx?familyid=4454e0e1-61fa-447a-bdcd-499f73a637d1&displaylang=en>