

Windows XP Service Pack 2 Group Policy Settings for MetaLAN and BlackProbe Versions 1.x

Overview

Windows XP Service Pack 2

Windows XP Service Pack 2 introduces several fundamental changes to the way Windows XP communicates on a network. By default, a new Windows Firewall is installed and enabled. The Firewall gives the workstation better security against malicious programs and network users. It also disables some service, management and diagnostic functionality in Windows. This is desirable on an Internet connection.

Reason for Windows Firewall Configuration

On a LAN connection the default setting for Windows firewall can disable network services, remote desktop, WMI, ping and many other applications that require network access to function. MetaLAN will not be able to remote control or gather information from XP computers on your network with the default settings for Windows Firewall in XP Service Pack 2. **The need for configuring Windows firewall is not unusual as most suppliers of Network Management Software will have to release recommended configurations to Windows Firewall to allow their software to function as intended.** On most Windows 2000+ Domains the best way to configure Windows Firewall on multiple XP Clients is to use Group Policy.

Requirements for Creating Windows Firewall Group Policy

- Account that has administrative rights to create group policies on the domain. usually a member of the built-in "domain admins" security group.
- Windows Server 2003 Administration Tools Pack. Downloadable from Microsoft.
- Windows XP Service Pack 2 Downloadable from Microsoft.

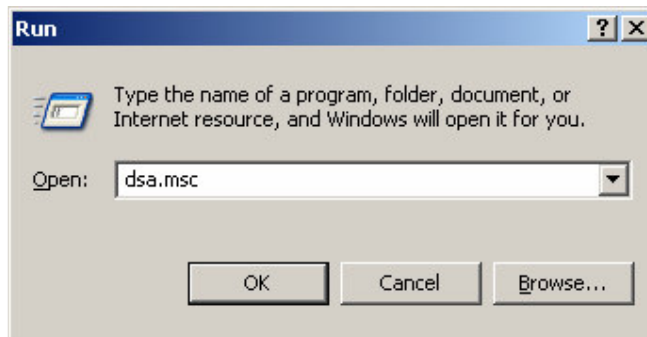
Steps Involved

1. Install XP Services Pack 2 on the XP Workstation.
2. Install the "**Windows Server 2003 Administration Tools Pack**" if not installed the XP Workstation..
3. Create a Group Policy for XP Service Pack 2 Firewall.

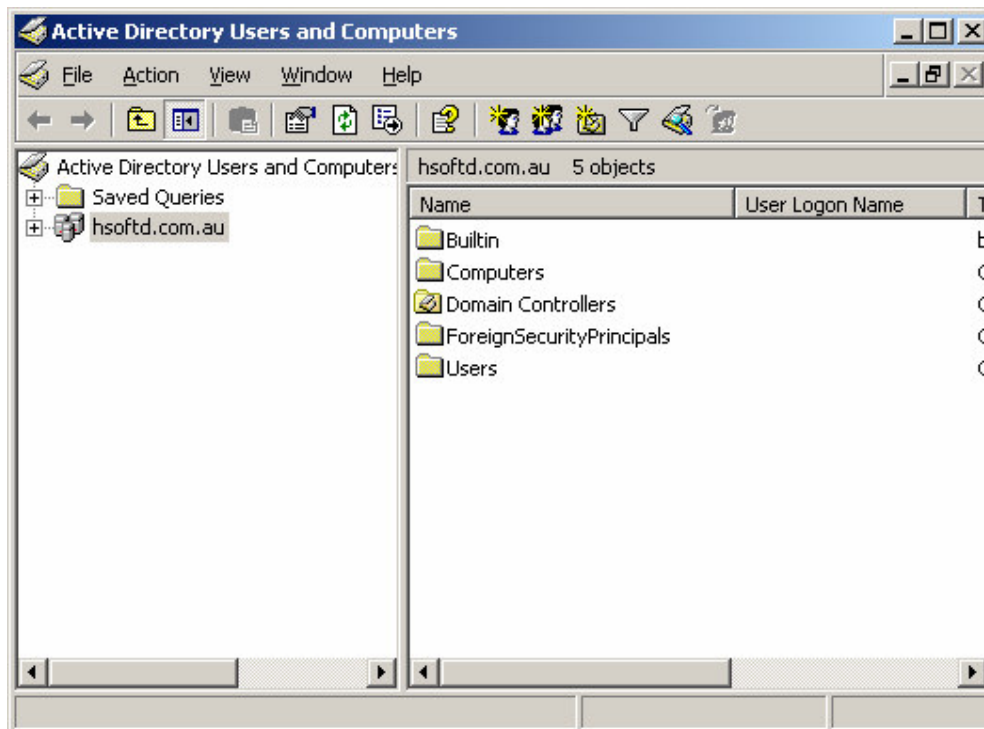
Create a Group Policy for XP Service Pack 2 Firewall.

You will need an Windows XP computer with Service Pack 2 and "Windows Server 2003 Administration Tools Pack" installed to complete the following steps. They can be downloaded from Microsoft's website.

1. On the XP computer Click [**Start**] [**Run**] and type "**dsa.msc**" and click [**OK**].

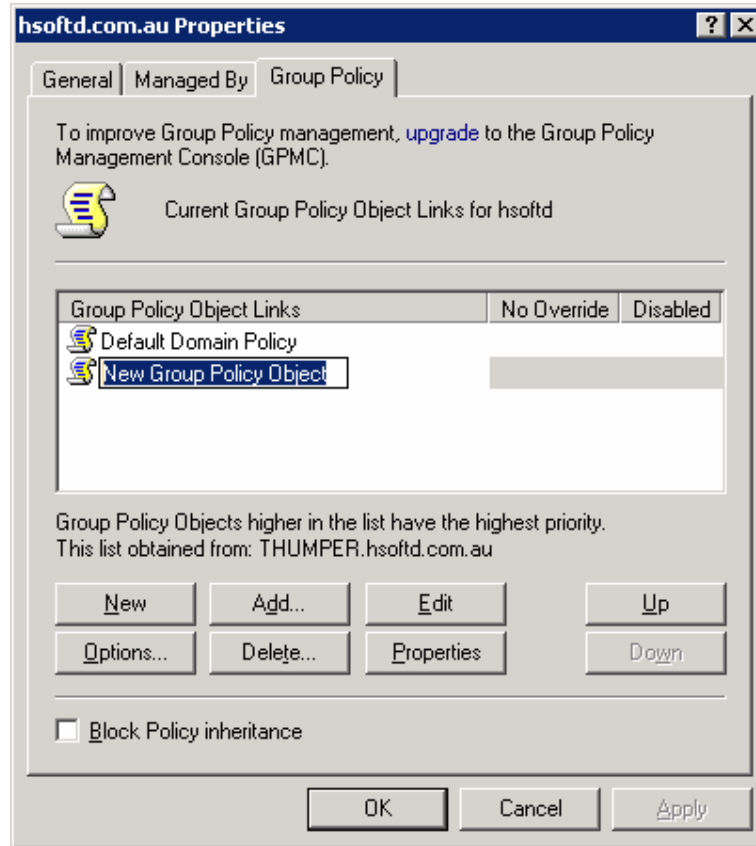


2. Select the Domain you wish to add the Group Policy to.

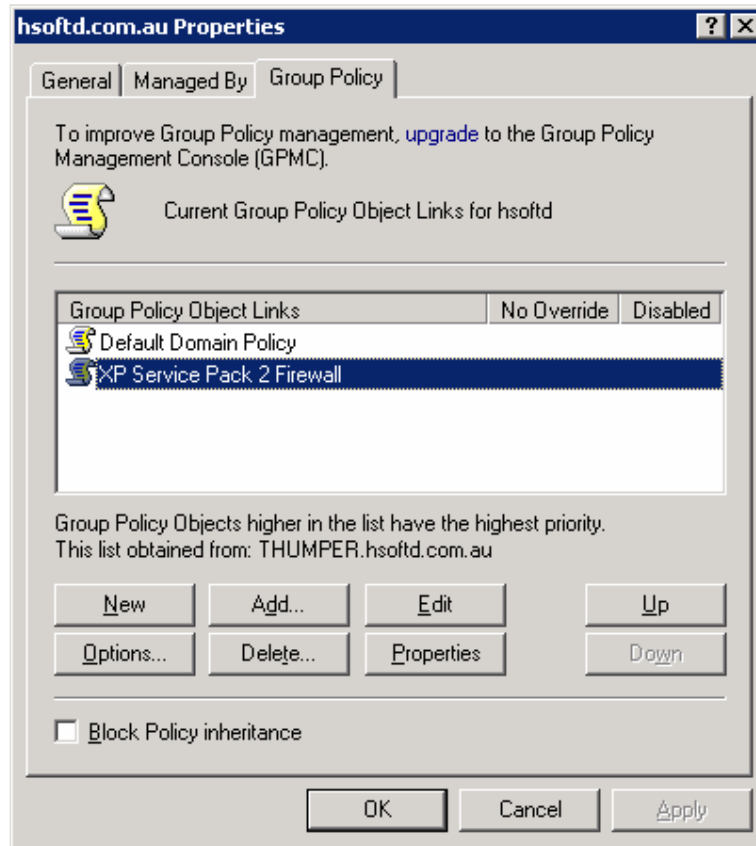


3. Right click the domain and click [Properties].

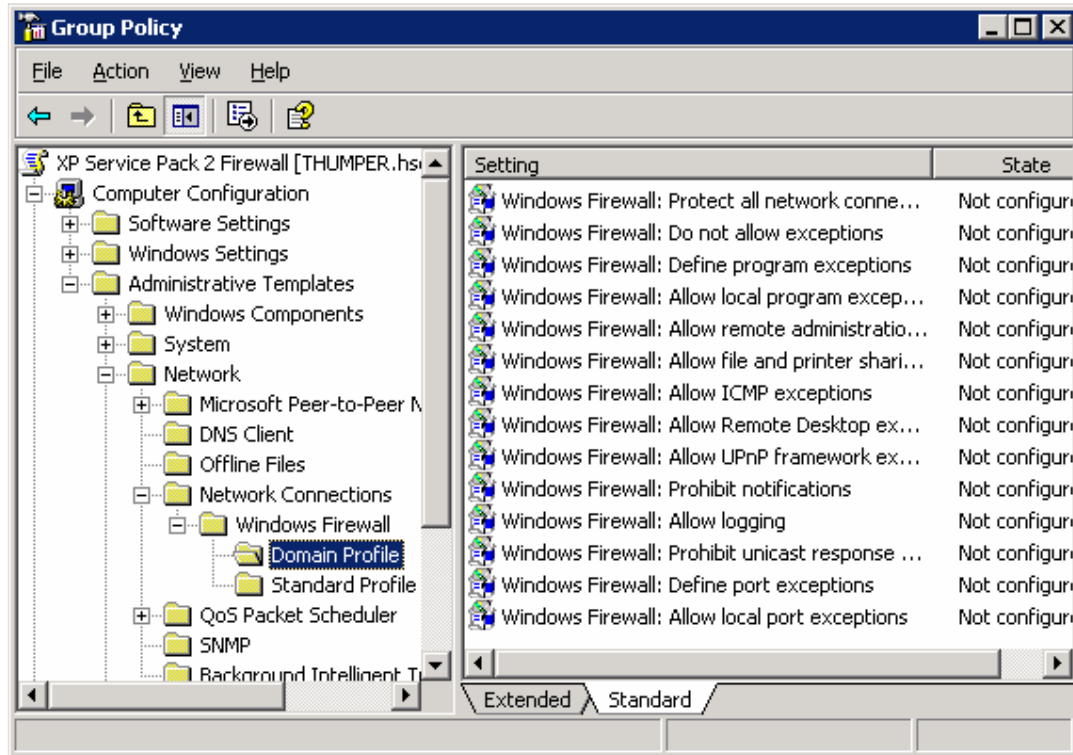
4. On the [Group Policy] tab click [New].



5. Give the Group Policy Object a descriptive name like **"XP Service Pack 2 Firewall"**.



6. Now with the new Group Policy selected click **[Edit]**. The Group Policy Editor MMC will launch with your new Group Policy.
7. Expand **[Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile]**.



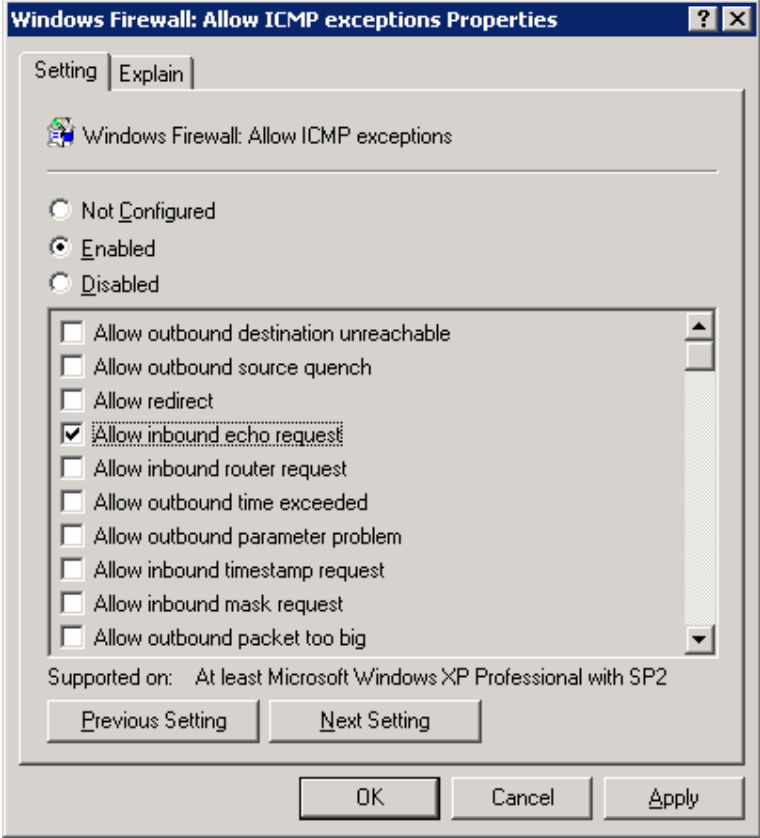
- Configure the following settings. Double click a setting to edit it. Click **[OK]** to accept a new setting.

Settings not specified here can be set to any setting your network requires.

Setting	State
<p data-bbox="284 489 878 520">Windows Firewall: Allow remote administration</p> <p data-bbox="284 525 1133 646">Select [Enabled] and enter the networks you will allow connections from in the dialog. Enter "*" for all networks or follow the instructions provided on the "Setting" and "Explain" tab to allow administration from the networks you specify.</p> <div data-bbox="342 674 1097 1507" style="border: 1px solid black; padding: 5px;"> <p data-bbox="347 680 1092 709">Windows Firewall: Allow remote administration exception Prop... [?] [X]</p> <p data-bbox="370 730 532 760">Setting Explain</p> <p data-bbox="386 793 922 823">Windows Firewall: Allow remote administration exception</p> <p data-bbox="386 869 558 970"> <input type="radio"/> Not Configured <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled </p> <p data-bbox="396 995 776 1024">Allow unsolicited incoming messages from:</p> <p data-bbox="402 1037 808 1071">*</p> <p data-bbox="396 1096 467 1125">Syntax:</p> <p data-bbox="396 1129 831 1323"> 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" </p> <p data-bbox="386 1335 1006 1365">Supported on: At least Microsoft Windows XP Professional with SP2</p> <p data-bbox="389 1377 597 1407">Previous Setting</p> <p data-bbox="607 1377 815 1407">Next Setting</p> <p data-bbox="639 1453 776 1482">OK</p> <p data-bbox="792 1453 928 1482">Cancel</p> <p data-bbox="945 1453 1081 1482">Apply</p> </div>	<p data-bbox="1177 489 1295 520">Enabled</p>

Click **[OK]** to accept the new setting.

Setting	State
<p data-bbox="284 279 990 306">Windows Firewall: Allow file and printer sharing exception</p> <p data-bbox="284 310 1133 432">Select [Enabled] and enter the networks you will allow connections from in the dialog. Enter "*" for all networks or follow the instructions provided on the "Setting" and "Explain" tab to allow administration from the networks you specify.</p> <div data-bbox="342 464 1097 1297" style="border: 1px solid gray; padding: 5px;"> <p data-bbox="347 470 1092 497">Windows Firewall: Allow file and printer sharing exception Prop... [?] [X]</p> <p data-bbox="370 520 532 548">Setting Explain</p> <p data-bbox="386 579 927 611">Windows Firewall: Allow file and printer sharing exception</p> <p data-bbox="386 659 557 758"> <input type="radio"/> Not Configured <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled </p> <p data-bbox="396 783 773 810">Allow unsolicited incoming messages from:</p> <p data-bbox="402 827 808 856">*</p> <p data-bbox="396 884 467 911">Syntax:</p> <p data-bbox="396 919 829 1108">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"</p> <p data-bbox="386 1125 1003 1152">Supported on: At least Microsoft Windows XP Professional with SP2</p> <p data-bbox="418 1167 570 1194">Previous Setting</p> <p data-bbox="656 1167 808 1194">Next Setting</p> <p data-bbox="695 1241 727 1268">OK</p> <p data-bbox="824 1241 889 1268">Cancel</p> <p data-bbox="980 1241 1036 1268">Apply</p> </div> <p data-bbox="284 1329 760 1356">Click [OK] to accept the new setting.</p>	<p data-bbox="1177 279 1295 306">Enabled</p>

Setting	State
Windows Firewall: Allow ICMP exceptions	Enabled
<p>Without the ability to "Ping" computers via ICMP MetaLAN will not be able to determine if a computer is online. The only setting that is required is "Allow inbound echo request"</p>	
<p>Select [Enabled] and check [Allow inbound echo request].</p>	
 <p>The screenshot shows the 'Windows Firewall: Allow ICMP exceptions Properties' dialog box. It has two tabs: 'Setting' and 'Explain'. Under the 'Setting' tab, there are three radio buttons: 'Not Configured', 'Enabled' (which is selected), and 'Disabled'. Below these are several checkboxes for different ICMP exceptions. The 'Allow inbound echo request' checkbox is checked, while all other checkboxes are unchecked. At the bottom of the dialog, there are buttons for 'Previous Setting', 'Next Setting', 'OK', 'Cancel', and 'Apply'. A note at the bottom of the dialog states 'Supported on: At least Microsoft Windows XP Professional with SP2'.</p>	
<p>Click [OK] to accept the new setting.</p>	

Setting	State
<p data-bbox="285 249 808 275">Windows Firewall: Define port exceptions</p> <p data-bbox="285 281 1154 401"><i>This setting will allow Remote Control sessions using VNC. If you do not wish to use VNC or you always use Windows Terminal Services or Remote Desktop to control client computers this setting is not required.</i></p> <p data-bbox="285 432 516 457">Select [Enabled].</p> <div data-bbox="342 491 1097 1325" data-label="Image"> </div>	<p data-bbox="1179 249 1292 275">Enabled</p>
<p data-bbox="285 1356 467 1381">Click [Show].</p> <p data-bbox="285 1419 1149 1444">In the Define port exceptions dialog click [Show]. Now click [Add].</p> <div data-bbox="350 1478 1089 1667" data-label="Image"> </div> <p data-bbox="285 1698 1149 1787">In the Add Item dialog type "5900:TCP:*.enabled:VNCServer" If you wish to allow connections from specific networks only, follow the instruction provided on the "Setting" and "Explain" tab.</p> <p data-bbox="285 1818 1073 1877">Click [OK] to add the new item. Click [OK] to close the show contents window and click [OK] to accept the new setting.</p>	

Internet Links

Help installing **Windows XP Service Pack 2**:

<http://support.microsoft.com/default.aspx?scid=fh;EN-US;windowsxpsp2>

Windows Server 2003 Administration Tools Pack:

<http://www.microsoft.com/downloads/> and search for "Windows Server 2003 Administration Tools Pack".

Support for **MetaLAN** or **BlackProbe**:

<http://support.hammer-software.com>