Windows Firewall on
Windows® XP Service Pack 2,
Windows Server® 2003 Service Pack 1 and
Windows Vista:
Group Policy Setup for
Diskeeper® Corporation Products

1.0 Overview

By default, Service Pack 2 (SP2) for Windows XP, Service Pack 1 for Windows Server 2003, and Windows Vista enable the Windows Firewall, previously known as Internet Connection Firewall (ICF). More detailed information on Windows XP SP2 can be found on the Microsoft® website at http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/winxpsp2.mspx.

Note: For simplicity, this document refers to Windows XP SP2 throughout, although the information presented here also applies to Windows Server 2003 SP1 and Windows Vista.

The firewall's behavior is such that by default, file and print sharing is disabled, and most TCP and UDP ports are blocked. In regards to Diskeeper Corporation products, this means we cannot PushInstall™ our products to remote machines, or communicate with them freely once they are installed (e.g., setting schedules and polling) without implementing this solution.

This document contains a technical overview of how to utilize Active Directory® Group Policy to configure the functionality of Windows Firewall to allow Diskeeper Corporation products to function fully.

Note: There are two DCOM permissions settings that must also be configured on remote systems in order to fully support Diskeeper Corporation products. Although we have not determined a way of changing these settings directly via Group Policy, Diskeeper Corporation has a batch scripts available to automate this procedure. These scripts are available at www.diskeeper.com/sp2. This White Paper also presents information on making these changes manually.

2.0 Executive Summary

1. Since Group Policy at the domain level is automatically propagated to all machines that fall under the scope of a given policy, it is an excellent method of distributing these types of settings from a central location to many machines at once.
2. Additional modifications may be possible to further lock down the Firewall and still not compromise function — especially if only individual products or combinations of two products are installed.
3. The setup shown here addresses Group Policy in a Windows 2000 or 2003 Active Directory Domain. No investigation at this point has been done on the possible configuration of Group Policy in a Windows NT 4.0 Domain.

4. A script that can be copied to target machines and run locally is available to configure the Windows Firewall on machines where Active Directory can't be used. See www.diskeeper.com/sp2 for additional information about this script.

3.0 Group Policy

Group Policy is used to define how programs and resources behave on a given system or for a particular user. It can be used to define items such as changing the way the desktop looks or changing the way communication occurs over the network — such as through Windows Firewall.

While Group Policy can be applied to the local computer, an Active Directory Organizational Unit, Domain or Site, this document will focus on the application of the specific Group Policy relating to Windows Firewall at a Domain level.

4.0 Creating a Group Policy

The first step is to create a Group Policy specifically to control Windows Firewall. The initial steps below are a modified form of the steps found on the Microsoft website in the document Deploying TCP/IP Windows Firewall Settings With Group Policy. Further customizations deal with enabling Diskeeper Corporation products to work in conjunction with Windows Firewall.

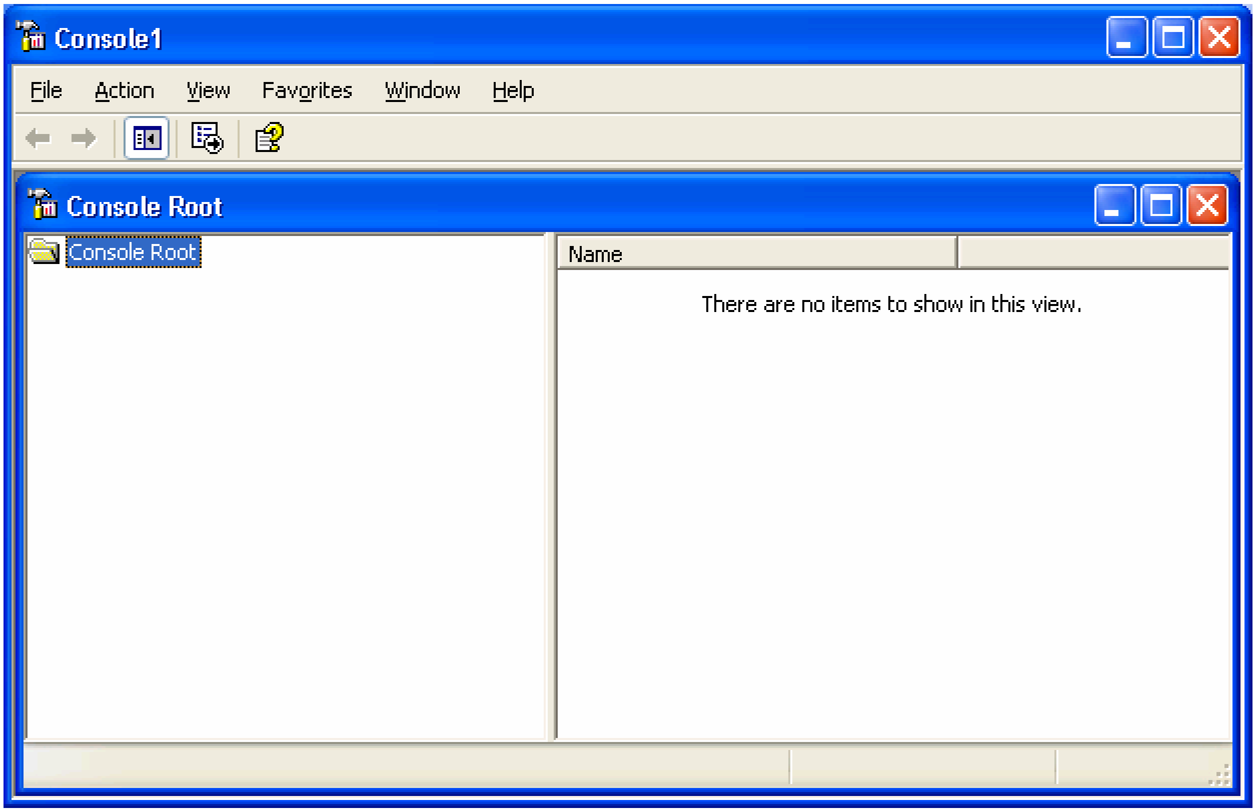
4.1 Install XP SP2

The first step is to install Windows XP SP2 on a machine. For this example, the machine will also have to be a member of an Active Directory Domain.

4.2 Create a Group Policy on the Domain

Once SP2 has been installed and the system rebooted, log in to the machine with a domain account with sufficient credentials to edit the domain Group Policy (such as a domain administrator).

1. From the Windows XP desktop on which you just installed SP2, click **Start**, **Run**, and then type **mmc** and click **OK**. This will open a blank MMC (Microsoft Management Console) console.

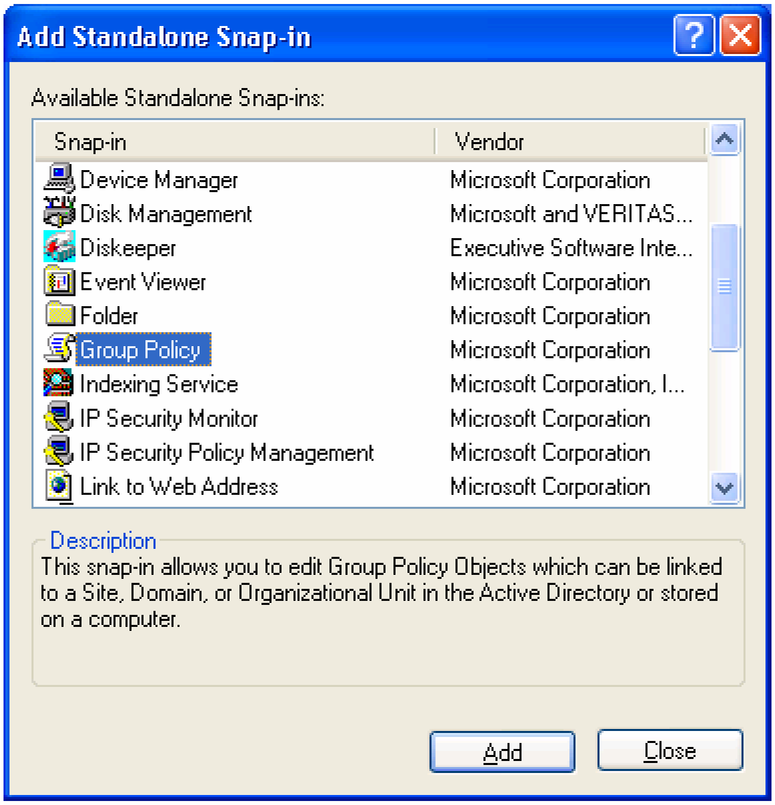


There are no items to show in this view.

2. Now click **File**, then **Add/Remove Snap-in**.

3. On the **Standalone** tab, click **Add**.

4. On the Add Standalone Snap-in screen, scroll down to the **Group Policy** selection, click on it, then click **Add**.



Add Standalone Snap-in

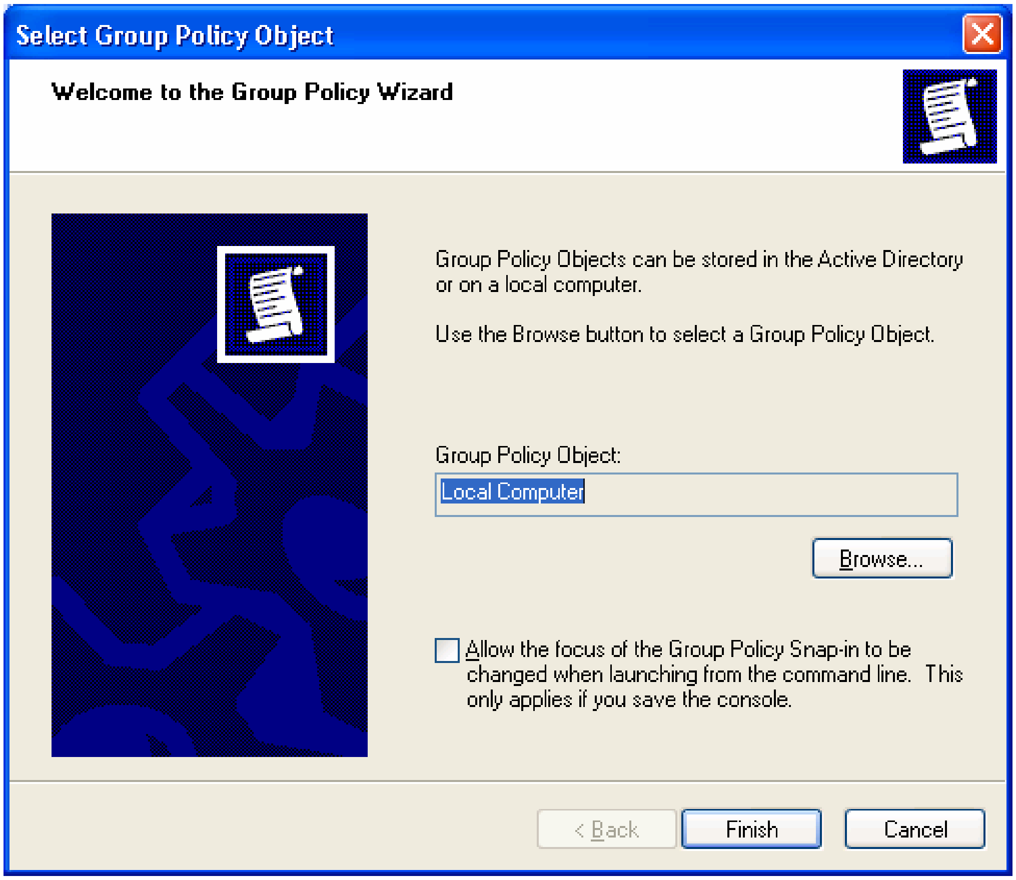
Available Standalone Snap-ins:

Snap-in	Vendor
Device Manager	Microsoft Corporation
Disk Management	Microsoft and VERITAS...
Diskeeper	Executive Software Inte...
Event Viewer	Microsoft Corporation
Folder	Microsoft Corporation
Group Policy	Microsoft Corporation
Indexing Service	Microsoft Corporation, I...
IP Security Monitor	Microsoft Corporation
IP Security Policy Management	Microsoft Corporation
Link to Web Address	Microsoft Corporation

Description

This snap-in allows you to edit Group Policy Objects which can be linked to a Site, Domain, or Organizational Unit in the Active Directory or stored on a computer.

5. On the Select Group Policy Object screen shown next, click **Browse**.



Select Group Policy Object

Welcome to the Group Policy Wizard

Group Policy Objects can be stored in the Active Directory or on a local computer.

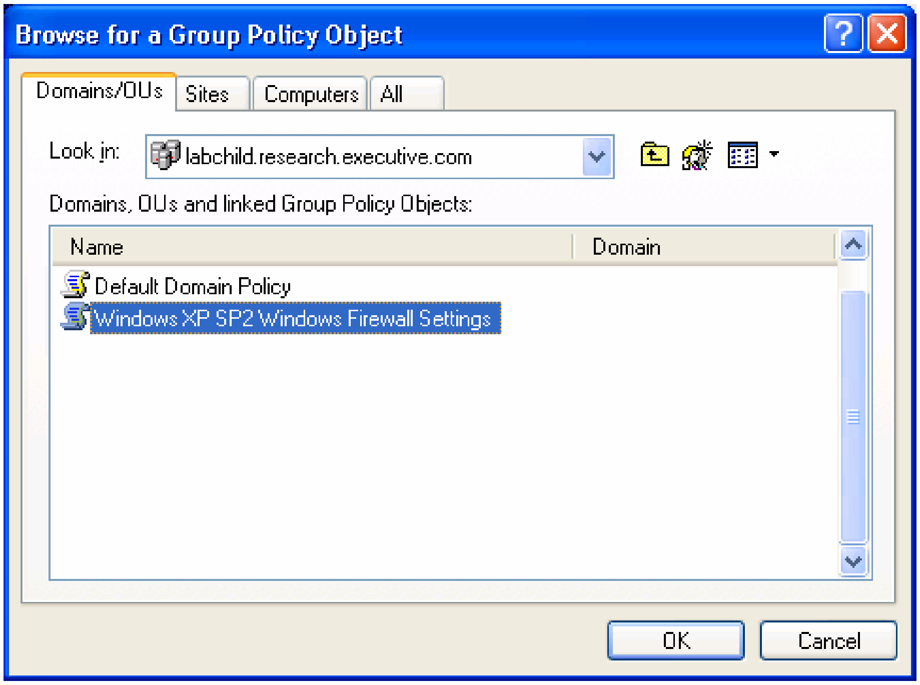
Use the Browse button to select a Group Policy Object.

Group Policy Object:

Local Computer

☐ Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.

6. On the Browse for a Group Policy Object Screen
    a. Click the **Domains/OU** tab.
    b. Select the appropriate domain from the **Look in:** drop-down selection box.
    c. Click the **Create New Group Policy Object** button (on the upper right next to the View Menu button).
    d. Next, name the new Group policy object. In the example shown below, it is called *Windows XP SP2 Windows Firewall Settings*.



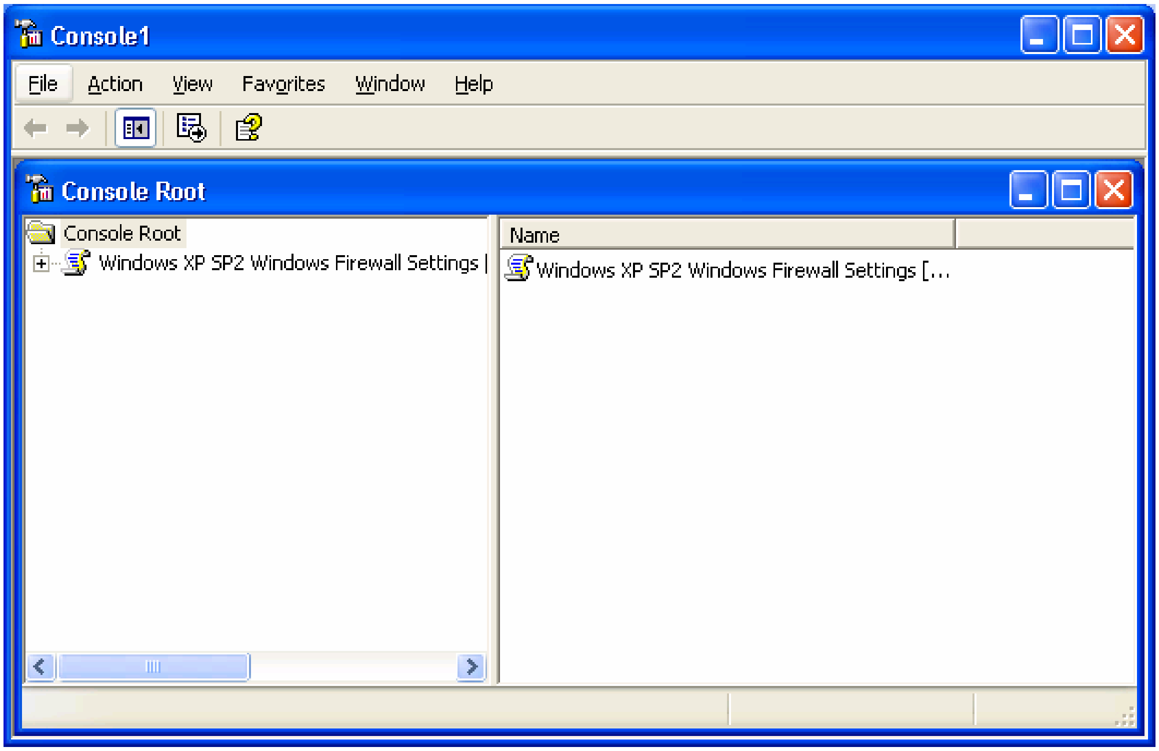
Browse for a Group Policy Object

Look in: labchild.research.executive.com

Domains, OUs and linked Group Policy Objects:

Name	Domain
Default Domain Policy	
Windows XP SP2 Windows Firewall Settings	

7. Click **OK**, **Finish**, **Close**, and then **OK**. Now you will see the new object in the MMC console window.



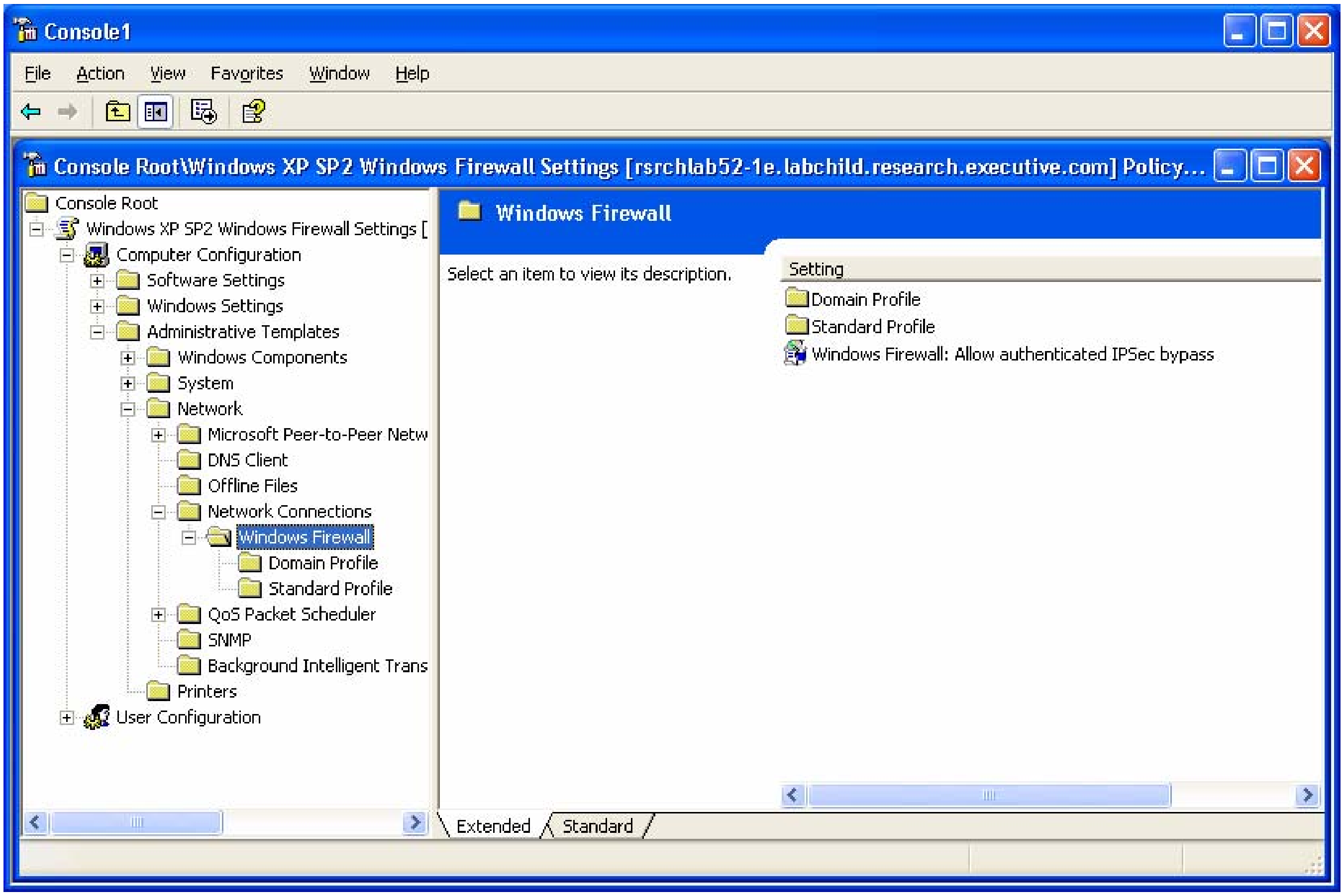
Console1

Console Root

Console Root
Windows XP SP2 Windows Firewall Settings |

Name	
Windows XP SP2 Windows Firewall Settings [...	

At this point the new Policy Object is created. Within the policy under Computer Configuration | Administrative Templates | Network | Network Connections | Windows Firewall, you can see the settings for the Windows Firewall.



5.0 Customizing the Windows Firewall Group Policy Settings

NOTE: If set incorrectly, Group Policy can cause a domain-wide dysfunction. It is imperative that you understand the nature and effects of any policy changes made.

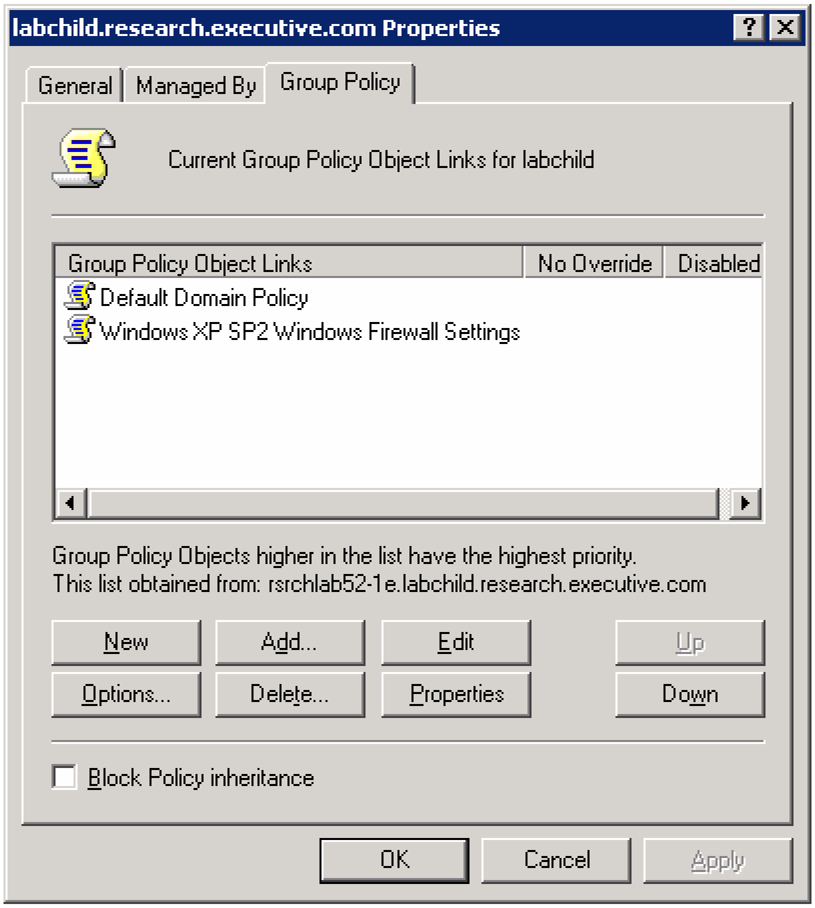
The policy created for the domain in the above manner is actually now stored on the domain. Rather than save and come back to the local MMC console to edit the policy or make future changes, this document will address using the Active Directory Users and Computers MMC to modify the policy. This is one of the Domain Controller-side MMCs that will be typically used to edit domain-wide policy. Note you must always initially create the policy using a workstation on which SP2 has been applied. It is the new modifications to the SP2 Group Policy administrative templates that store the information for the Windows Firewall and these modifications must first be “copied” to a new policy for them to be available.

5.1 Open the New Group Policy on the Domain Controller

1. Log on to a Domain Controller on the domain in which you just created the above Policy Object.

2. Open Active Directory Users and Computers via Administrative Tools or by clicking **Start**, **Run**, typing **dsa.msc**, then clicking **OK**.

3. In the Active Directory Users and Computers MMC, make sure that you are connected to the domain in which you created the policy, then right click the domain name in the left window and select **Properties**. Now click the **Group Policy** tab.



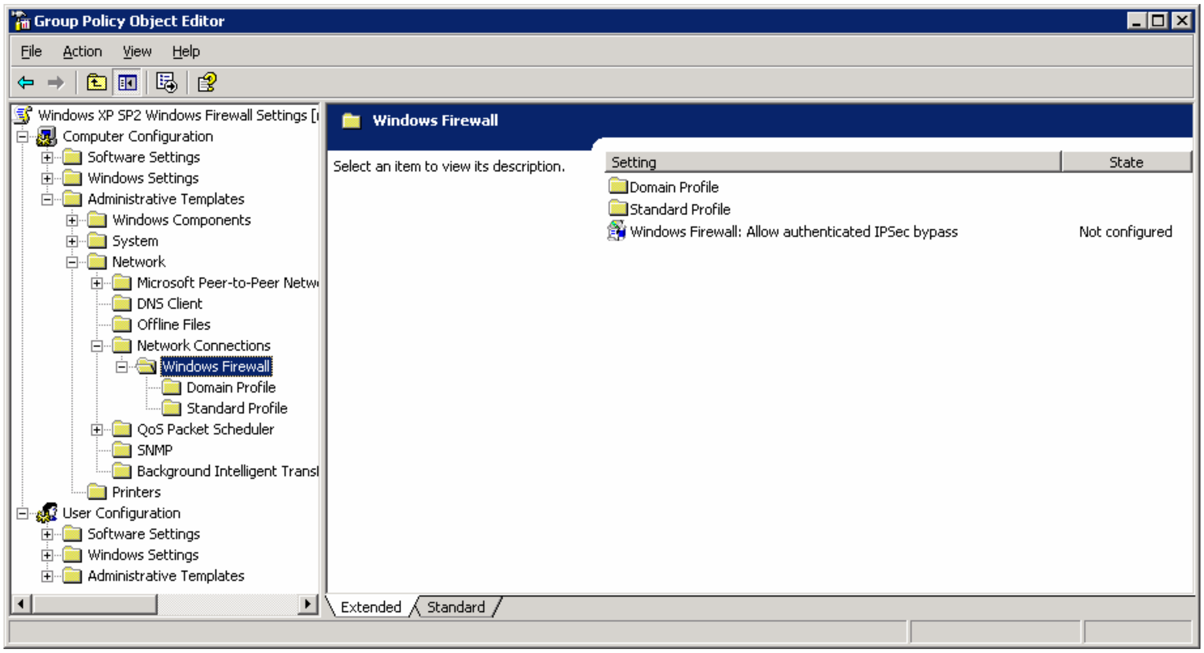
Current Group Policy Object Links for labchild

Group Policy Object Links	No Override	Disabled
Default Domain Policy		
Windows XP SP2 Windows Firewall Settings		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: rsrchlab52-1e.labchild.research.executive.com

□ Block Policy inheritance

4. Click the new **Group Policy Object** link, then click **Edit**. Now navigate to the location of the policy settings for Windows Firewall.



Select an item to view its description.

Setting	State
Domain Profile	
Standard Profile	
Windows Firewall: Allow authenticated IPSec bypass	Not configured

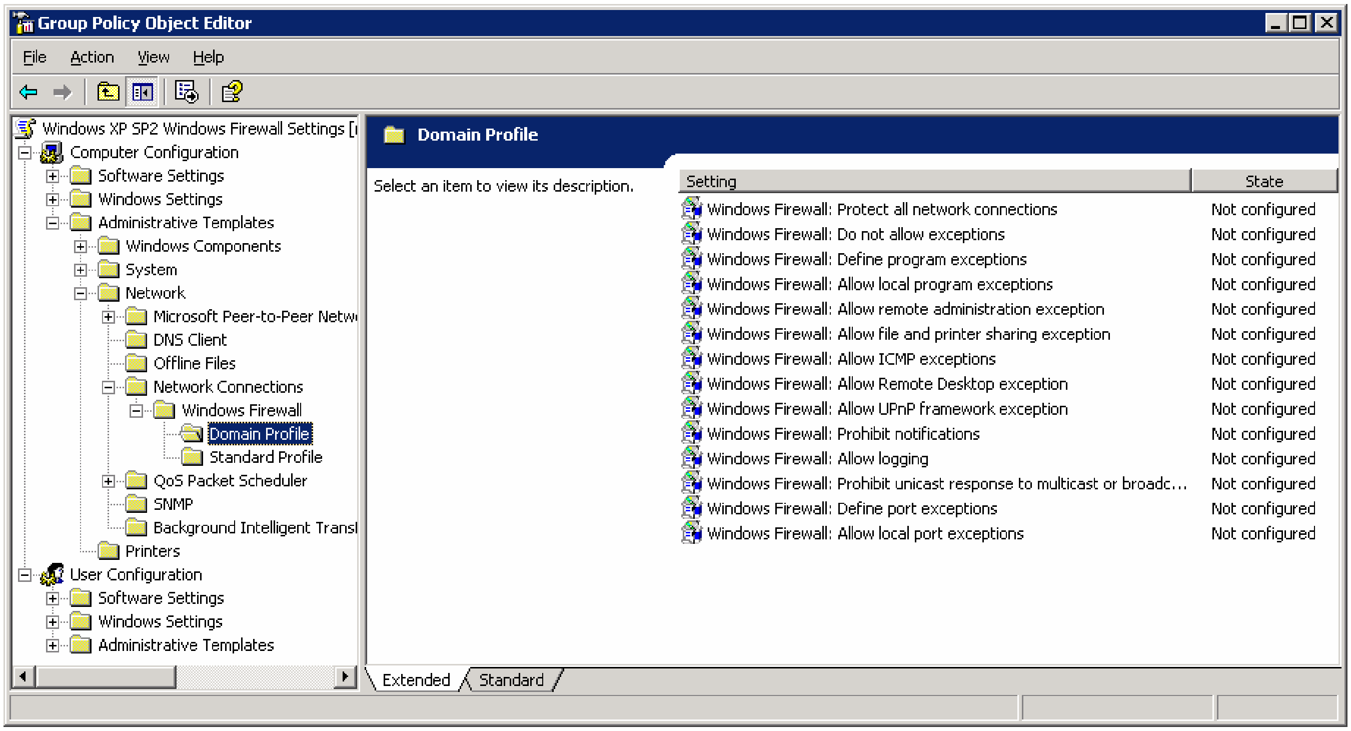
We are now ready to being editing the policy for Diskeeper Corporation Products.

5.2 *Configure the Windows Firewall*

Below is a list of suggested settings copied from the Microsoft document listed above, modified to include File and Print Sharing and other settings. For example, these settings will enable the target machine to be a PushInstall recipient, and additionally in Sitekeeper, able to be scanned without an agent.

As noted in the illustration above, there are two profiles: Domain and Standard. This document will only focus on the domain profile. While identical settings could be used, it is advisable to “lock down” the firewall in the Standard Profile. In such instances, such as a laptop that is out of the office, remote installation and communication features of Diskeeper Corporation products may not be needed.

Populate the Domain Profile settings with the values indicated below:

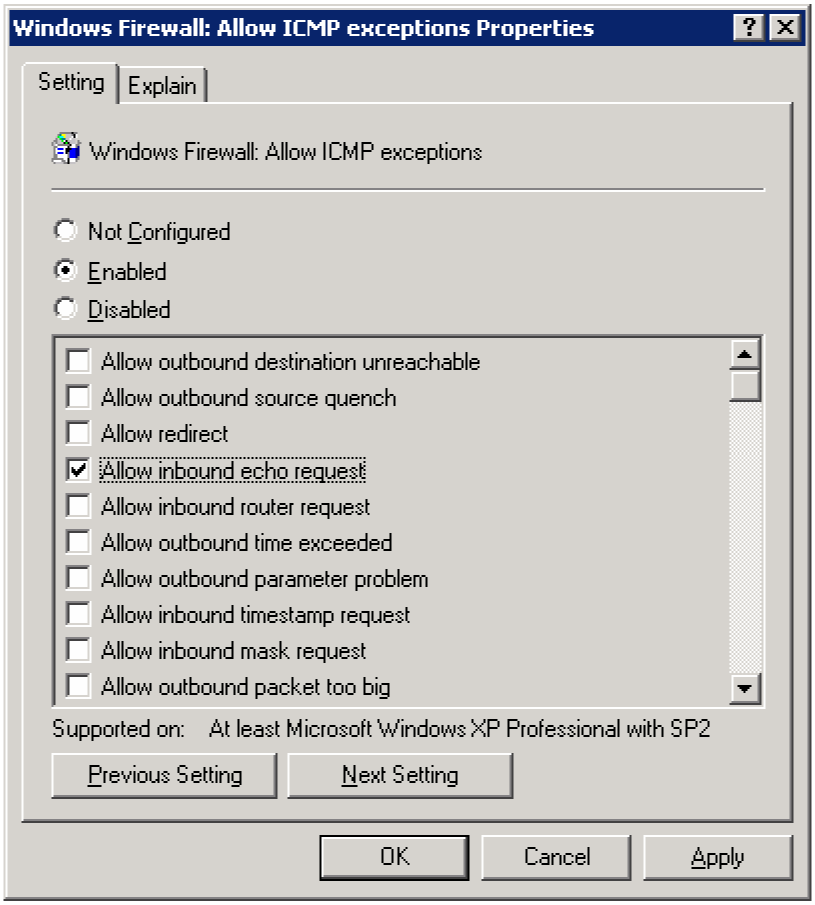


Select an item to view its description.

Setting	State
Windows Firewall: Protect all network connections	Not configured
Windows Firewall: Do not allow exceptions	Not configured
Windows Firewall: Define program exceptions	Not configured
Windows Firewall: Allow local program exceptions	Not configured
Windows Firewall: Allow remote administration exception	Not configured
Windows Firewall: Allow file and printer sharing exception	Not configured
Windows Firewall: Allow ICMP exceptions	Not configured
Windows Firewall: Allow Remote Desktop exception	Not configured
Windows Firewall: Allow UPnP framework exception	Not configured
Windows Firewall: Prohibit notifications	Not configured
Windows Firewall: Allow logging	Not configured
Windows Firewall: Prohibit unicast response to multicast or broadc...	Not configured
Windows Firewall: Define port exceptions	Not configured
Windows Firewall: Allow local port exceptions	Not configured

- Windows Firewall: Protect all network connections — Enabled.
- Windows Firewall: Do not allow exceptions — Not configured.
- Windows Firewall: Define program exceptions — Not configured.
- Windows Firewall: Allow local program exceptions — Enabled.
- Windows Firewall: Allow remote administration exception — Enabled. This allows Sitekeeper to gather inventory on the machine via WMI. It also enables versions of Diskeeper prior to V9.0 to communicate to the machine via DCOM and allows Undelete® Server to connect to Undelete on the machine to access the Recovery Bin and to modify Undelete properties. Configure to allow all messages from any network by typing an asterisk (*) in the text box. Note this is <u>not</u> necessary for Diskeeper 9.0 and later versions.
- Windows Firewall: Allow file and print sharing exception — Enabled. This is needed for all versions of Diskeeper. It is also needed for Diskeeper, Undelete and Sitekeeper PushInstall features, and Sitekeeper scanning without an agent. Use an asterisk in this setting as well to allow all messages. If you will not be using Undelete or Diskeeper PushInstall to the machines in this domain, and you run the Sitekeeper agent on the machines, you do not need to enable this exception.

- Windows Firewall: Allow ICMP exceptions — Enabled. While Sitekeeper can IP scan a Windows XP Professional SP2 machine with all ICMP exceptions disabled, this setting needs to be tested further with Windows XP Home Edition SP2 to determine the effect. Additional settings may be required or it may be possible to set to Disabled.



Windows Firewall: Allow ICMP exceptions Properties

Windows Firewall: Allow ICMP exceptions

○ Not Configured
● Enabled
○ Disabled

□ Allow outbound destination unreachable
□ Allow outbound source quench
□ Allow redirect
☑ Allow inbound echo request
□ Allow inbound router request
□ Allow outbound time exceeded
□ Allow outbound parameter problem
□ Allow inbound timestamp request
□ Allow inbound mask request
□ Allow outbound packet too big

Supported on: At least Microsoft Windows XP Professional with SP2

- Windows Firewall: Allow Remote Desktop exception — Enabled only if you use Remote Desktop to connect to Windows XP SP2-based computers. In this example we will use Enabled. Use an asterisk in this setting as well to allow all messages.

- Windows Firewall: Allow UPnP framework exception — Enabled only if you use UPnP devices on your network. In this case we will use Not Configured.

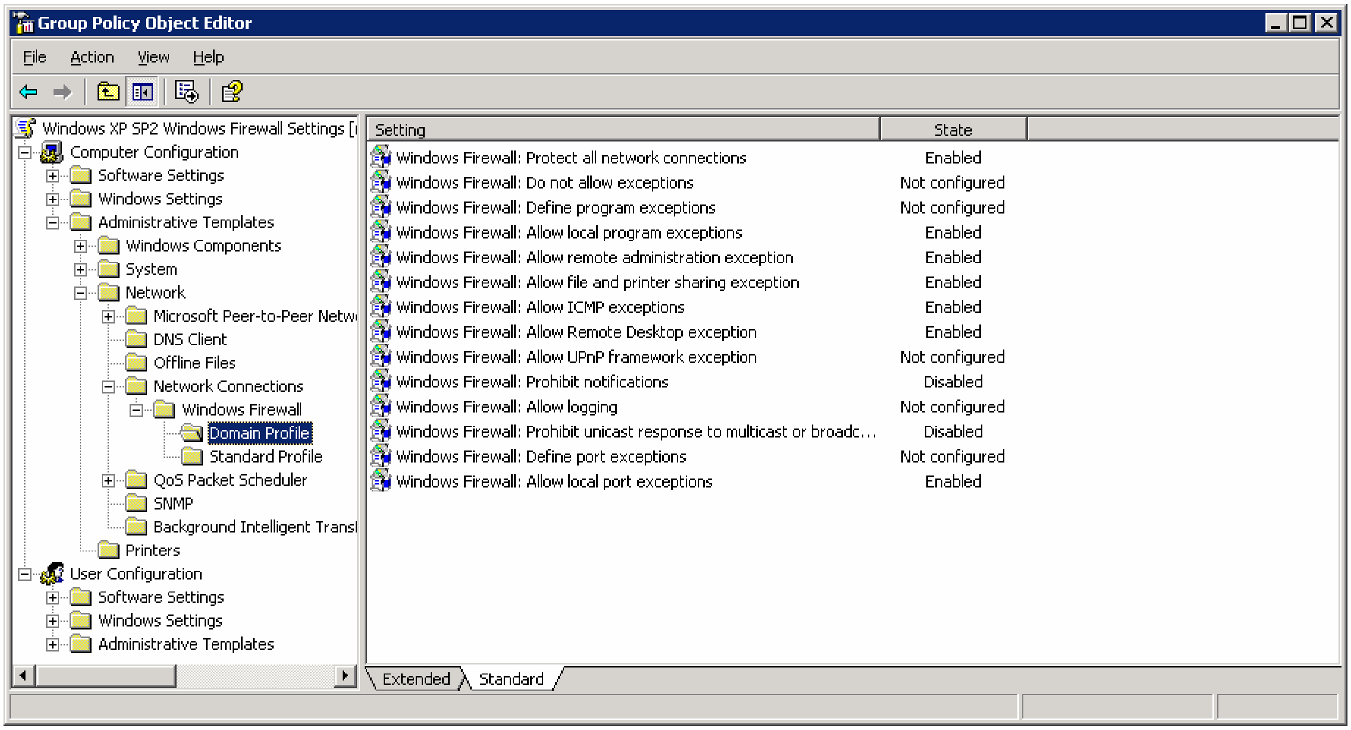
- Windows Firewall: Prohibit notifications — Disabled.

- Windows Firewall: Allow logging — Not configured.

- Windows Firewall: Prohibit unicast response to multicast or broadcast requests — Disabled.

- Windows Firewall: Define port exceptions — Not configured.

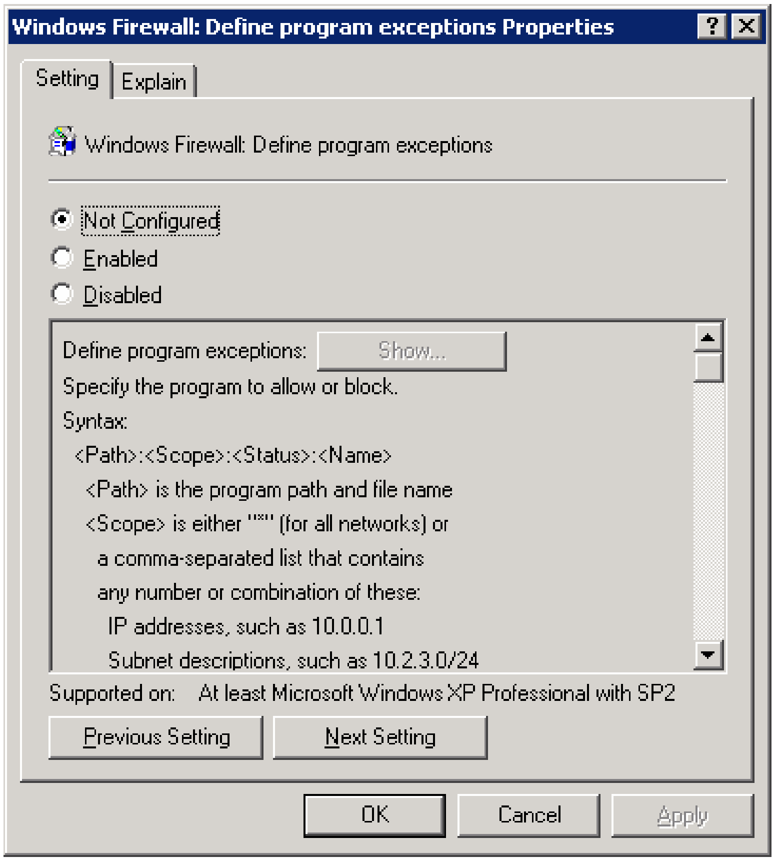
- Windows Firewall: Allow local port exceptions — Enabled.



Setting	State
Windows Firewall: Protect all network connections	Enabled
Windows Firewall: Do not allow exceptions	Not configured
Windows Firewall: Define program exceptions	Not configured
Windows Firewall: Allow local program exceptions	Enabled
Windows Firewall: Allow remote administration exception	Enabled
Windows Firewall: Allow file and printer sharing exception	Enabled
Windows Firewall: Allow ICMP exceptions	Enabled
Windows Firewall: Allow Remote Desktop exception	Enabled
Windows Firewall: Allow UPnP framework exception	Not configured
Windows Firewall: Prohibit notifications	Disabled
Windows Firewall: Allow logging	Not configured
Windows Firewall: Prohibit unicast response to multicast or broadc...	Disabled
Windows Firewall: Define port exceptions	Not configured
Windows Firewall: Allow local port exceptions	Enabled

5.2.1 Defining Diskeeper Corporation Program Exceptions

The next step is to create program exceptions. Open the setting for Windows Firewall: Define program exceptions.



Windows Firewall: Define program exceptions

● Not Configured
○ Enabled
○ Disabled

Define program exceptions: Show...

Specify the program to allow or block.

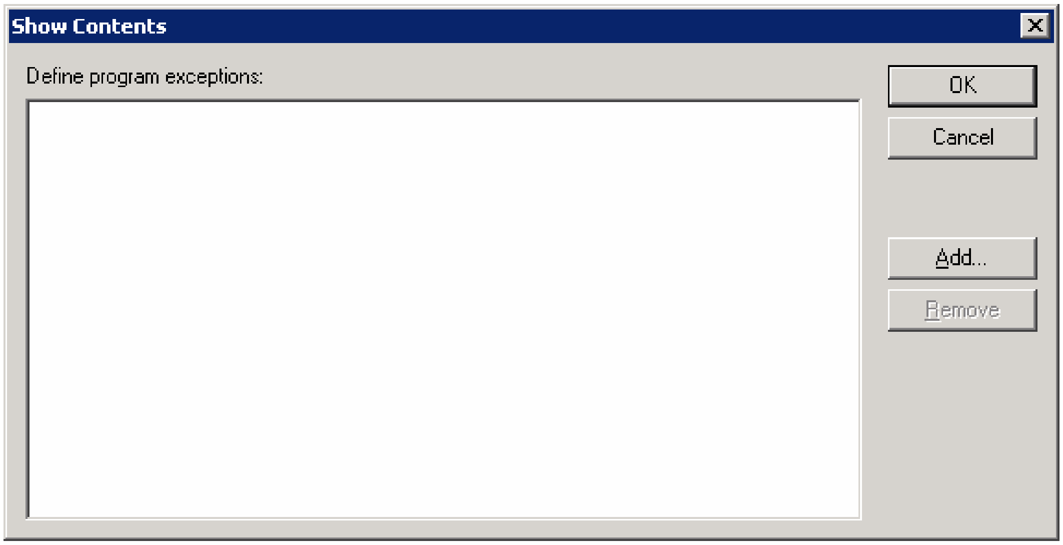
Syntax:

```
 <Path>:<Scope>:<Status>:<Name>
   <Path> is the program path and file name
   <Scope> is either "*" (for all networks) or
     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
```

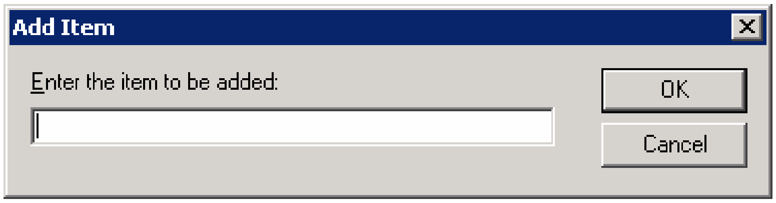
Supported on: At least Microsoft Windows XP Professional with SP2

1. Set the State to **Enabled**.

2. Then click the **Show...** button.



3. In the Show Contents window, click **Add...**



4. Enter the following lines as appropriate for the Diskeeper Corporation products you are running, one at a time, exactly as entered below. These examples reflect the default installation location for each respective product. If you installed one or more products to other locations, you must edit the path(s) to match the product location. After each entry, click the **OK** button, then click **Add...** again until finished.

For Diskeeper 2007 and Diskeeper 10.0:

```
%ProgramFiles%\Diskeeper Corporation\Diskeeper\DkService.exe:*:enabled:DkService
```

For Diskeeper 9.0:

```
%ProgramFiles%\Executive Software\Diskeeper\DkService.exe:*:enabled:Dk9Service
```

For Diskeeper 8.0:

```
%SystemRoot%\System32\mmc.exe:*:enabled:MicrosoftManagementConsole
%ProgramFiles%\Executive Software\Diskeeper\DkService.exe:*:enabled:DiskeeperService
%ProgramFiles%\Executive Software\Diskeeper\DfrgNtfs.exe:*:enabled:DiskeeperNtfsEngine
%ProgramFiles%\Executive Software\Diskeeper\DfrgNtfs1.exe:*:enabled:DiskeeperNtfs1Engine
%ProgramFiles%\Executive Software\Diskeeper\DfrgFat.exe:*:enabled:DiskeeperFatEngine
```

For Diskeeper Server 7.0:

```
%SystemRoot%\System32\mmc.exe:*:enabled:MicrosoftManagementConsole
%ProgramFiles%\Executive Software\DiskeeperServer\DkService.exe:*:enabled:Dk7SrvrService
%ProgramFiles%\Executive Software\DiskeeperServer\DfrgNtfs.exe:*:enabled:Dk7SrvrNtfsEngine
%ProgramFiles%\Executive Software\DiskeeperServer\DfrgFat.exe:*:enabled:Dk7SrvrFatEngine
```

For Diskeeper Workstation 7.0:

```
%ProgramFiles%\Executive Software\DiskeeperWorkstation\DkService.exe:*:enabled:Dk7WksService
%ProgramFiles%\Executive Software\DiskeeperWorkstation\DfrgNtfs.exe:*:enabled:Dk7WksNtfsEngine
%ProgramFiles%\Executive Software\DiskeeperWorkstation\DfrgFat.exe:*:enabled:Dk7WksFatEngine
```

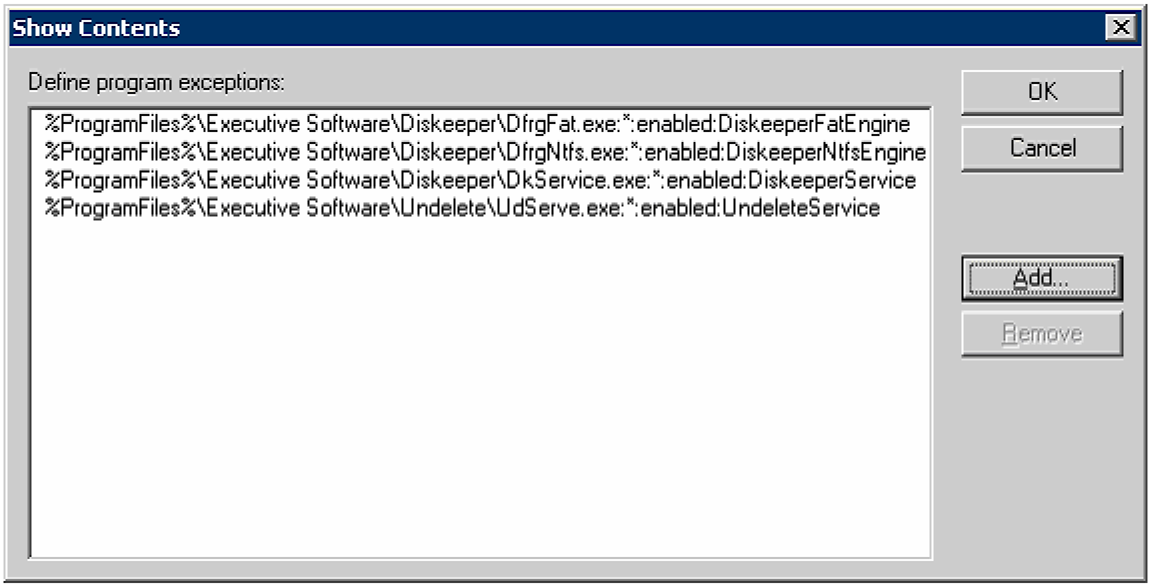
For Sitekeeper Agent:

```
%ProgramFiles%\Executive Software\Sitekeeper Agent\SKAgent.exe:*:enabled:SitekeeperAgent
```

For Undelete:

```
%ProgramFiles%\Executive Software\Undelete\UdServe.exe:*:enabled:UndeleteService
```

5. The final Show Contents screen should be similar to this:



```
%ProgramFiles%\Executive Software\Diskeeper\DfrgFat.exe:*:enabled:DiskeeperFatEngine
%ProgramFiles%\Executive Software\Diskeeper\DfrgNtfs.exe:*:enabled:DiskeeperNtfsEngine
%ProgramFiles%\Executive Software\Diskeeper\DkService.exe:*:enabled:DiskeeperService
%ProgramFiles%\Executive Software\Undelete\UdServe.exe:*:enabled:UndeleteService
```

6. Click **OK**, then **OK** again to close the Define program exception Properties window.

5.2.2 Defining Diskeeper Corporation Port Exceptions

Port exceptions are defined similarly to program exceptions as described above. Open the setting **Windows Firewall: Define port exceptions**. Set the state to **Enabled,** click the **Show** button, then click **Add.** The following lines are used in the Add Item edit box to enable the ports used by Diskeeper Corporation products:

For Diskeeper 2007 and Diskeeper 10.0 (if you prefer to specify ports rather than DkService.exe):

```
31038:TCP:*:enabled:DkServiceEndPoint0
31058:TCP:*:enabled:DkServiceEndPoint1
```

For Diskeeper 9.0 (if you prefer to specify ports rather than DkService.exe):

```
31038:TCP:*:enabled:DkServiceEndPoint0
31058:TCP:*:enabled:DkServiceEndPoint1
```

For Diskeeper 7.0 and 8.0:

```
135:TCP:*:enabled:DiskeeperDCOM
```

For Sitekeeper:

```
31041:TCP:*:enabled:SitekeeperRPC
31040:TCP:*:enabled:SkPIServerRPC
31042:TCP:*:enabled:SKAgentRPC
4500:UDP:*:enabled:SkIPSec4500
500:UDP:*:enabled:SkIPSec500
```

For Sitekeeper SQL access:

```
1434:UDP:*:enabled:SitekeeperSQL
```

5.2.3 Applying the New Policy Settings

To test the new policy, you must force the application of the new settings to your Group Policy. Open a command window on the Windows XP SP2 machine by clicking **Start | Run** and type **cmd**. Then click **OK**.

In the command window displayed, type **gpupdate** then press **Enter**. This forces an update of the Group Policy. You should now be able to test and confirm the policy setting allow your Diskeeper Corporation products to function as you need them.

6.0 More Information

More information about Windows XP SP2, Windows Server 2003 SP1, Windows Vista, and Diskeeper Corporation products is available at www.diskeeper.com/sp2.