Security

How to Configure Windows Firewall in a Small Business Environment using Group Policy

Introduction

This document explains how to configure the features of Windows Firewall on computers running Microsoft Windows XP Professional Service Pack 2 (SP2) in a Small or Medium Business (SMB) environment. The environment might include domain controllers running Microsoft Windows Small Business Server 2003, Microsoft Windows Server 2003, or Microsoft Windows 2000 server.

The most efficient way to manage Windows Firewall settings in an organization's network is to use Microsoft Active Directory services and the Windows Firewall settings in Group Policy. Active Directory and Group Policy allow you to centrally configure settings for Windows Firewall and apply those settings to all Windows XP SP2 clients.

Windows XP SP2 includes new administrative templates for group policy objects to enhance security for your client computer and domain, including functionality for Windows Firewall. To apply these templates, you might have to install hotfixes, depending on the operating system of the domain server or workstation in use.

After these templates are applied any Group Policy updates will include settings for Windows Firewall. Group Policy updates are sent from the domain controller to all members of the domain, and may also be requested by a domain member through the use of the GPUpdate utility.

To setup Windows Firewall, you perform tasks in the Group Policy Object Editor and you must be a member of the domain administrators group.

Table 1 lists the default settings for Windows Firewall.

Table 1 Default Windows Firewall settings

Option	Default Configuration	Modify when
Network connection settings	All connections	You no longer require the protection of Windows Firewall on a specific network connection, or you require individual settings for each network connection
Program exceptions	Remote Assistance only	You need to receive connections from other programs or services to your computer
Port exceptions	None	You require connections from another computer's programs that use specific ports on your computer
ICMP exceptions	None	You require other computers to verify that your computer exists and that TCP/IP is configured correctly
Notifications	On	You no longer wish to receive notification when other computers attempt to connect to your computer and fail
Logging	Off	You require a record of connections, or connection attempts, made to your computer
Don't Allow Exceptions	Off	You learn that your computer has a security vulnerability or you use your computer in a less secure environment such as an airport lounge

The tasks to configure Windows Firewall using Group Policy are:

- Add hotfixes to the GPO administrative workstations and Windows Small Business Server 2003
- Update Group Policy objects (GPOs) that already exist
- Configure Windows Firewall settings with Group Policy
- Apply configuration with GPUpdate
- Verify Windows Firewall settings are applied

Complete the tasks described in this document to help keep your computer safe from computer worms and other malicious code and continue to allow connections to and from the Internet.

Microsoft strongly recommends that you test any Windows Firewall Group Policy settings in a test environment before you deploy them in your production environment to ensure that your Windows Firewall Group Policy configuration does not cause downtime or loss of productivity.

For definitions of security-related terms, see the following:

- "Microsoft Security Glossary" on the Microsoft Web site at http://go.microsoft.com/fwlink/?LinkId=35468

Before You Begin

IMPORTANT: The instructions in this document were developed with the Start menu that appears by default when you install your operating system. If you have modified your Start menu, the steps might differ slightly.

Windows XP SP2 can be used as a Windows domain client in an Active Directory domain using domain controllers that run one of the following:

- Windows Server 2003
- Windows Small Business Server 2003
- Windows 2000 Server SP3 or later

In most networks, the network hardware firewall, proxy, and other security systems provide a level of protection from the Internet to network computers.

If you do not have a host firewall (a locally installed software firewall), such as Windows Firewall, on your computer's network connections, you are vulnerable to malicious programs that might be introduced by other computers when they attach to your network. Also, you are vulnerable when you use your computer away from your network, such as when you use a laptop computer at home or you connect to a hotel or airport network.

Before you install hotfixes make sure that you have a good backup of the computer, including a backup of the registry.

For more information on how to back up the registry, see the following:

- Microsoft Knowledge Base article 322756 on the Microsoft Help and Support Web site at http://go.microsoft.com/fwlink/?linkid=36365

Adding Hotfixes to Administrative Workstations and Windows Small Business Server 2003

If you manage Group Policy Object settings on computers that run earlier operating systems or service packs (for example, Windows XP with SP1 or Windows Server 2003), you must install a hotfix (KB842933) so policy settings appear correctly in the Group Policy Object Editor.

If you use Small Business Server 2003 you must install an additional hotfix (KB872769). By default SBS 2003 turns off the Windows Firewall. The hotfix resolves this issue.

Note: The hotfixes listed are not included as part of Windows Update and must be installed separately. The hotfixes must be applied to all affected computers individually.

KB842933 applies to the following:

- Microsoft Windows Server 2003, Web Edition
- Microsoft Windows Server 2003, Standard Edition
- Microsoft Windows Server 2003, Enterprise Edition
- Microsoft Windows Server 2003, 64-Bit Enterprise Edition
- Microsoft Windows XP Professional SP1
- Microsoft Windows Small Business Server 2003, Premium Edition
- Microsoft Windows Small Business Server 2003, Standard Edition
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Professional

KB872769 applies to the following:

- Microsoft Windows Small Business Server 2003, Standard Edition
- Microsoft Windows Small Business Server 2003, Premium Edition

Note: For more information or to obtain these hotfixes, see the following:

- Microsoft Knowledge Base Article 842933 on the Microsoft Help and Support Web site at http://go.microsoft.com/fwlink/?linkid=35474
- Microsoft Knowledge Base Article 872769 on the Microsoft Help and Support Web site at http://go.microsoft.com/fwlink/?linkid=35477

Requirements to perform this task

- Credentials: You must log onto the client computer as a member of the Domain Admins security group or Local Administrators security group.
- Tools: The appropriate downloaded hotfix for your operating system as explained in the Knowledge Base articles 842933 and 872769.

Adding Hotfix 842933 to Windows Small Business Server 2003, Windows 2000 Server SP3 or later, Windows XP SP1, or Windows Server 2003

To add the hotfix

1. From the Windows desktop, click **Start**, click **Run**, type the path and filename of the downloaded hotfix and then click **OK**.
2. On the **Welcome to KB842933 Setup Wizard** page, click **Next**.
3. On the **License** page, click **I Agree**, and then click **Next**.
4. On the **Completing the KB842933 Setup Wizard** page, to finish the hotfix installation and restart the computer, click **Finish**.
5. Repeat the above steps for all affected computers (servers and management workstations).

Adding Hotfix 872769 to Windows Small Business Server 2003

To add the hotfix

1. From the Windows desktop, click **Start**, click **Run**, type the path and filename of the downloaded 872769 hotfix and then click **OK**.
2. On the **Welcome to KB872769 Setup Wizard** page, click **Next**.
3. On the **License** page, click **I Agree**, and then click **Next**.
4. On the **Completing the KB872769 Setup Wizard** page, to finish the hotfix installation and restart the computer, click **Finish**.

Updating Existing Group Policy Objects

Windows XP SP2 adds additional settings in the administrative templates. To configure these new settings you must update each GPO with the new administrative templates found in Windows XP SP2. If you do not update the Group Policy Objects, settings related to the Windows Firewall are not available.

On a Windows XP SP2-based computer, you can use Microsoft Management Console (MMC) with the Group Policy Object Editor Snap-in installed to update GPOs.

After a GPO has been updated, you can configure the network protection settings that are appropriate for your computers that run Windows XP SP2.

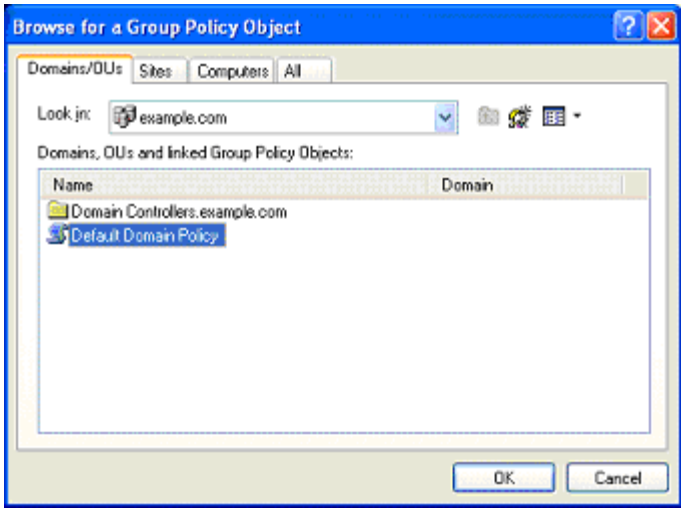
Requirements to perform this task

- Credentials: You must log on to a Windows XP SP2 computer that is an Active Directory domain client, as a member of the Domain Admins, or the Group Policy Creator/Owner security group.
- Tools: Microsoft Management Console (MMC) with the Group Policy Object Editor snap-in installed.

Updating Group Policy Objects

To update Group Policy Objects with Windows XP SP2 new administrative templates

1. From the Windows XP SP2 desktop, click **Start**, click **Run**, type **mmc**, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**.
3. On the **Standalone** tab, click **Add**.
4. In the **Available Standalone Snap-ins** list, locate then click **Group Policy Object Editor**, and then click **Add**.
5. In the **Select Group Policy Object** dialog box, click **Browse**.



6. In the **Browse for a Group Policy Object** dialog box, select the Group Policy object that you want to update with the new Windows Firewall settings.
7. Click **OK**, and then click **Finish** to close the Group Policy Wizard. This applies the new administrative template to the selected GPO.
8. In the **Add Standalone Snap-in** dialog box, click **Close**.
9. In the **Add/Remove Snap-in** dialog box, click **OK**.
10. Close the MMC, click **File** then click **Exit**. Do not save changes to the console settings.

    Note: Although you do not save console changes, the above procedure imports the new administrative templates from Windows XP SP2 into the GPO. The templates must be imported into each defined GPO.
11. Repeat the steps for every GPO used to apply Group Policy to Windows XP SP2-based computers.

    Note: To update your GPOs 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 the following:

    - "Enterprise Management with the Group Policy Console" on the Microsoft Windows Server System Web site at http://go.microsoft.com/fwlink/?linkID=35479

Configuring Windows Firewall Settings Using Group Policy

There are two sets of Windows Firewall settings to configure:

- **Domain profile**. These settings are used by computers that are connected to a network that contains domain controllers for the domain of which the computers are a member.
- **Standard profile**. These settings are used by computers when they are not connected to your network, for example, when you travel with a laptop computer.

If you do not configure standard profile settings, the default values remain unchanged. Microsoft highly recommends that you configure both domain and standard profile settings, and that you enable the Windows Firewall for both profiles. The only exception is if you are already using a third-party host firewall product (a locally installed software firewall). Microsoft recommends that you disable Windows Firewall if you are already using a third-party host firewall product.

The standard profile settings are typically more restrictive than the domain profile, because the standard profile settings do not include applications and services that are only used in a managed domain environment.

In a GPO, both the domain profile and standard profile contain the same set of Windows Firewall settings. Windows XP SP2 relies on network determination to apply correct profile settings.

Note: For more information about network determination, see the following:

- "Network Determination Behavior for Network-Related Group Policy Settings" on the Microsoft TechNet Web site at http://go.microsoft.com/fwlink/?linkid=35480

This section describes the possible Windows Firewall settings in a GPO, the recommended settings for a SMB environment, and demonstrates how to configure the four major types of GPO settings.

Requirements to perform this task

- Credentials: You must log on to a Windows XP SP2 computer that is an Active Directory domain client, as a

member of the Domain Admins security group, or the Group Policy Creator/Owner security group.

- Tools: Microsoft Management Console (MMC) with the Group Policy Object Editor snap-in installed.

  Note: To open a GPO you use either an MMC with the Group Policy Object Editor snap-in, or the Active Directory Users and Computers console. To use the Active Directory Users and Computers console on a Windows XP client computer, you must first run adminpak.msi from the Windows Server 2003 CD.

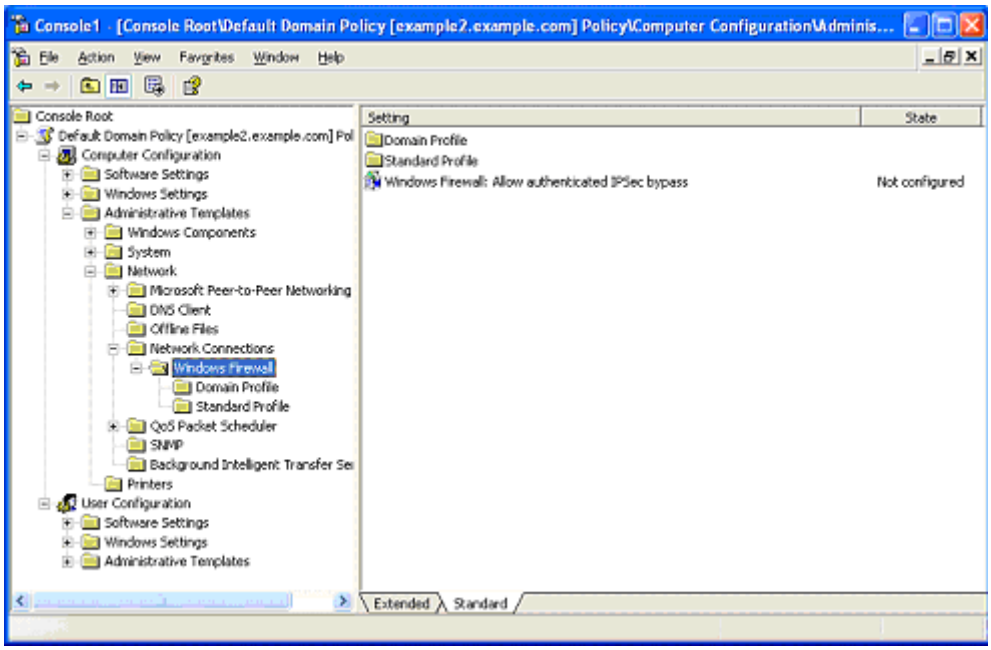
Configuring Windows Firewall Settings Using Group Policy

You use the Group Policy snap-in to modify the Windows Firewall settings in the appropriate GPOs.

After you configure the Windows Firewall settings, wait for the settings to be applied to client computers by the standard refresh cycles, or use the GPUpdate utility on the client computer. By default these refresh cycles are every 90 minutes, with a random offset of + or - 30 minutes. The next refresh of Computer Configuration Group Policy downloads the new Windows Firewall settings and applies them to computers that run Windows XP SP2.

To configure Windows Firewall settings using Group Policy

1. From the Windows XP SP2 desktop, click **Start**, click **Run**, type **mmc**, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**.
3. On the **Standalone** tab, click **Add**.
4. In the **Available Standalone Snap-ins** list, locate then click **Group Policy Object Editor**, and click **Add**.
5. In the **Select Group Policy Object** dialog box, click **Browse**.
6. Select the Group Policy Object you are going to configure, click **OK** then click **Finish**.
7. Click **Close** to close the **Add Stand-alone Snap-in** box then on the **Add/Remove Snap-in** box, click **OK**.
8. In the console tree of the Group Policy Object Editor, open **Computer Configuration**, **Administrative Templates**, **Network**, **Network Connections**, and then **Windows Firewall**.



9. Double-click **Windows Firewall: Allow authenticated IPSec bypass**.

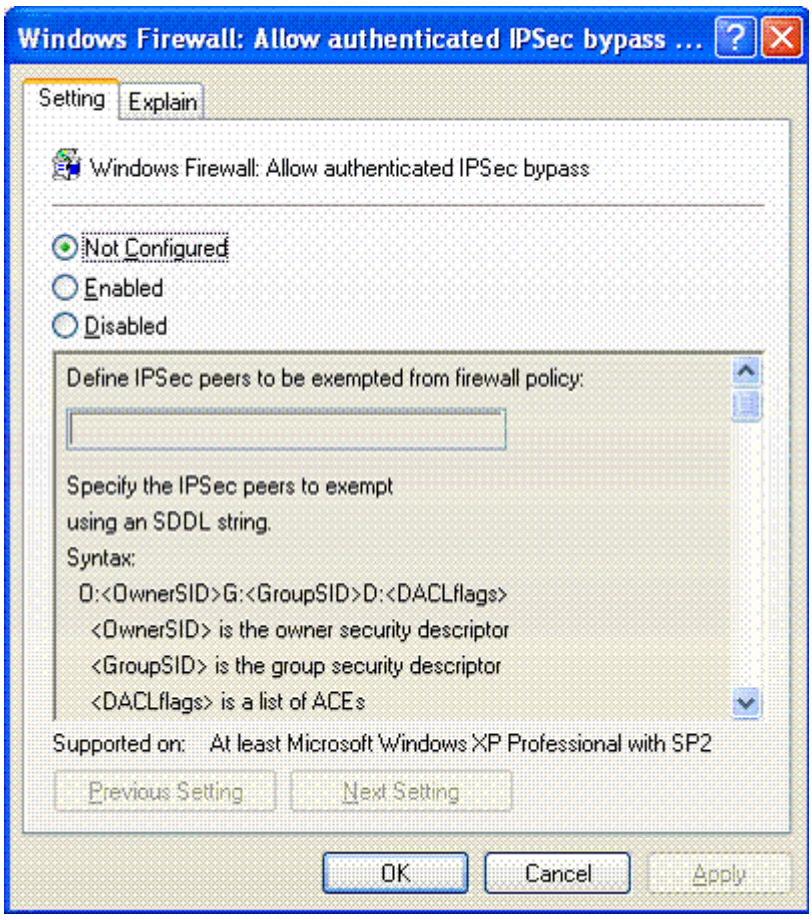


Table 2 summarizes the Allow authenticated IPSec bypass options.

Table 2 Allow authenticated IPSec bypass settings

Setting	Description	Notes
Not Configured	This GPO does not change the current configuration of Windows Firewall	
Enabled	Windows Firewall does not process IPSec-secured traffic except from users or groups listed in the policy.	The syntax for listing users and groups uses the SDDL standard. For more information, see the following: • "Security Descriptor Definition Language" on the MSDN Web site at http://go.microsoft.com/fwlink/?linkid=35503
Disabled	Windows Firewall processes IPSec-secured traffic.	

10. Use the information in table 2 and either click **Enabled**, **Disabled** or **Not Configured**.

    Note: If you click Enabled, you can create a list of users or groups that are allowed to send IPSec secured traffic to your computer.

11. Click **OK**.

12. Select either **Domain Profile** or **Standard Profile**.

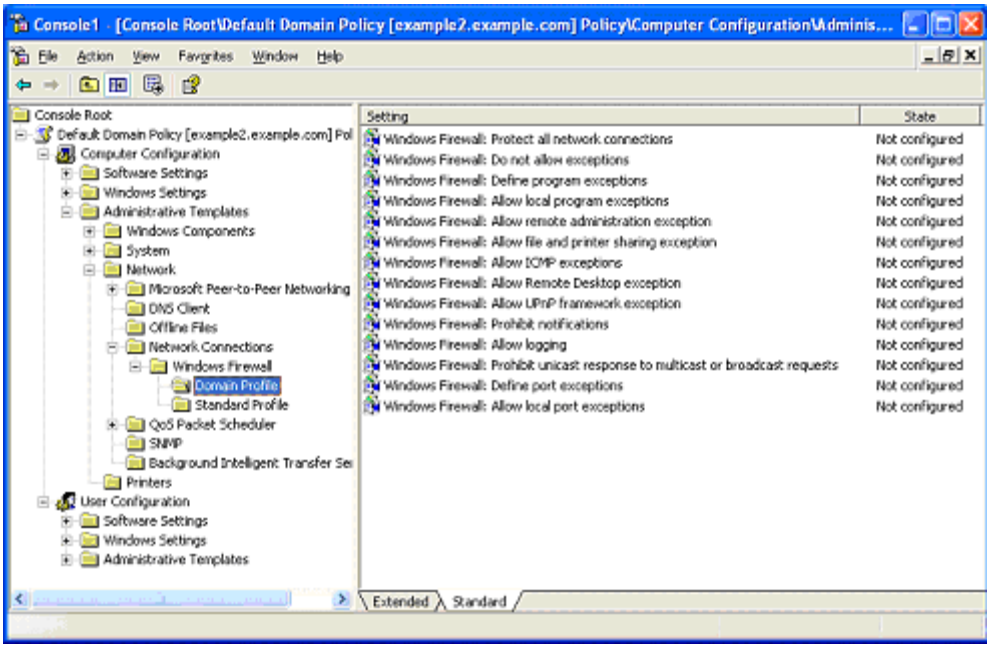


Table 3 summarizes the Windows Firewall Group Policy recommended settings for the domain and standard profiles.

Table 3 Windows Firewall recommended settings for a Small or Medium Business

Setting	Description	Domain Profile	Standard Profile
Protect all network connections	Specifies that all network connections have Windows Firewall enabled	Enabled	Enabled
Do not allow exceptions	Specifies that all unsolicited incoming traffic is dropped, including excepted traffic	Not configured	Enabled, unless you must configure program exceptions
Define program exceptions	Defines excepted traffic in terms of program file names	Enabled and configured with the programs (applications and services) used by the computers running Windows XP SP2 on your network	Enabled and configured with the programs (applications and services) used by the computers running Windows XP SP2 on your network
Allow local program exceptions	Enables local configuration of program exceptions	Disabled, unless you want local administrators to configure program exceptions locally	Disabled
Allow remote administration exception	Enables remote configuration using tools	Disabled, unless you want to be able to remotely administer your computers with MMC snap-ins	Disabled
Allow file and print sharing exception	Specifies whether file and printer sharing traffic is allowed	Disabled, unless the computers running Windows XP SP2 are sharing local resources	Disabled
Allow ICMP exceptions	Specifies the types of ICMP messages that are allowed	Disabled, unless you wish to use the ping command to troubleshoot	Disabled
Allow Remote Desktop exception	Specifies whether the computer can accept a Remote Desktop-based	Enabled	Enabled

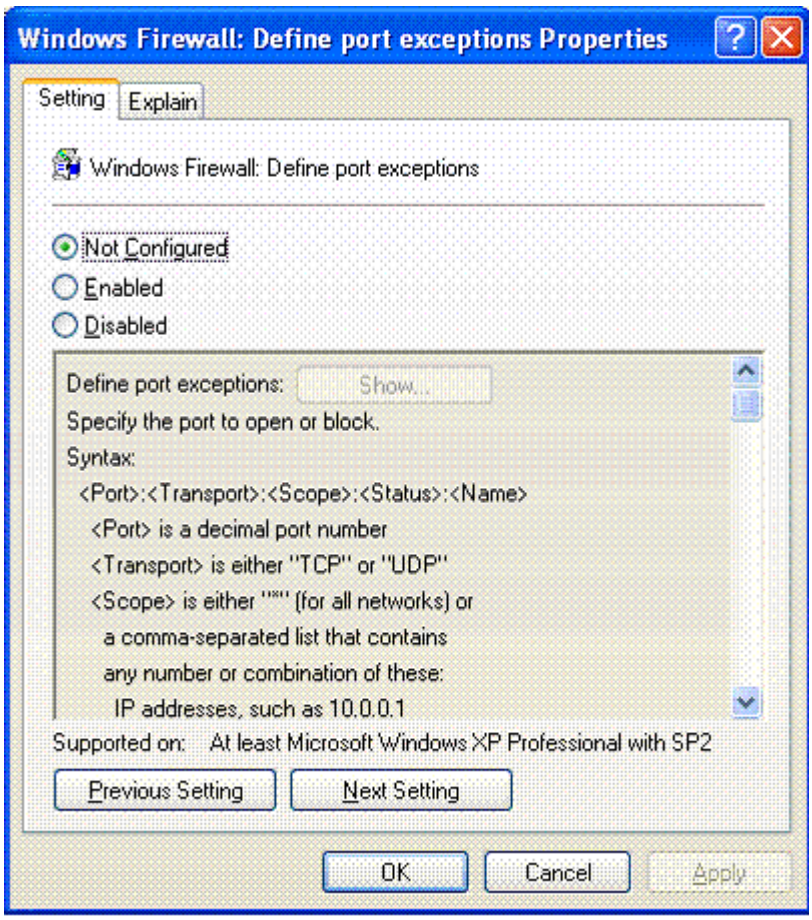
	connection request		
Allow UPnP framework exception	Specifies whether the computer can receive unsolicited UPnP messages	Disabled	Disabled
Prohibit notifications	Disables notifications	Disabled	Disabled
Allow logging	Allows traffic logs and configures log file settings	Not configured	Not configured
Prohibit unicast response to multicast or broadcast requests	Discards the unicast packets received in response to a multicast or broadcast request message	Enabled	Enabled
Define port exceptions	Specifies excepted traffic in terms of TCP and UDP	Disabled	Disabled
Allow local port exceptions	Enables local configuration of port exceptions	Disabled	Disabled

13. Double-click each setting listed in table 3 and then either click **Enabled**, **Disabled** or **Not Configured** and then click **OK**.

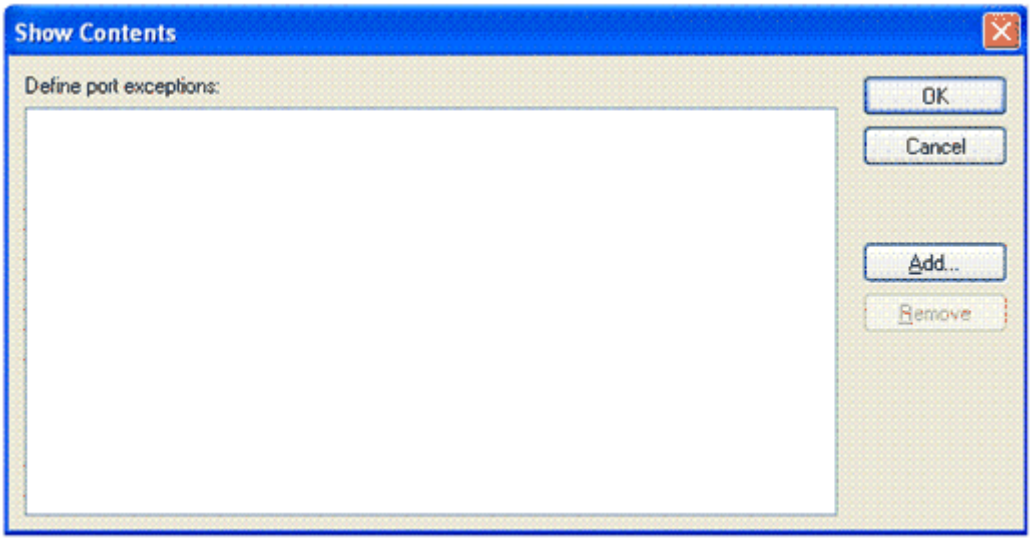
Enabling Exceptions for Ports

To Enable exceptions for ports

1. In either the **Domain Profile** or **Standard Profile** settings area, double-click **Windows Firewall: Define port exceptions**.



2. Click **Enabled**, and then click **Show**.



3. Click **Add**.

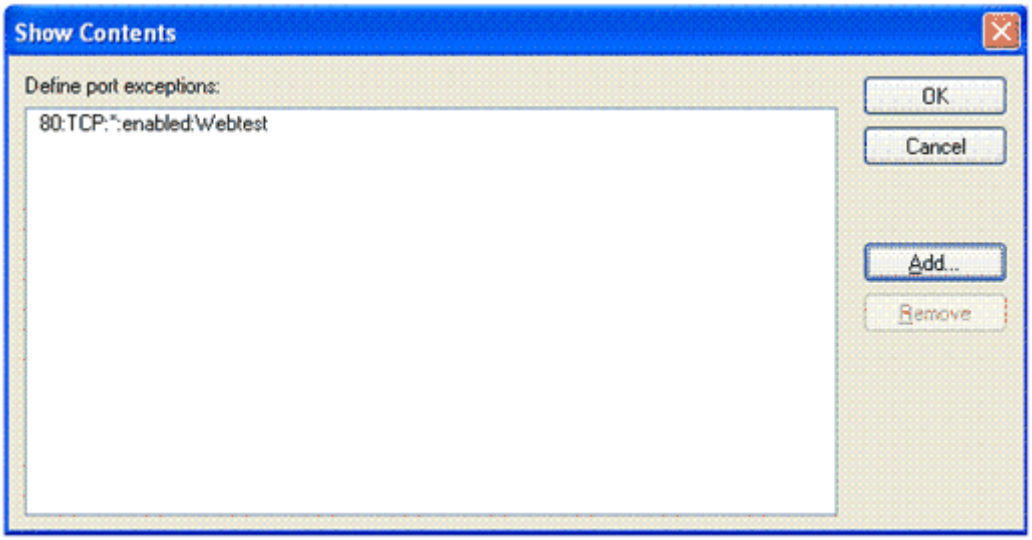
4. Type the information about the port that you want to block or enable. Use this syntax:

port:transport:scope:status:name

Where port is the port number, transport is TCP or UDP, scope is either * (for all computers) or a list of the computers that are allowed to access the port, status is either enabled or disabled, and name is a text string used as a label for this entry.

This example is named WebTest and enables TCP port 80 for all connections.

5. Click **OK** to close **Add Item**.

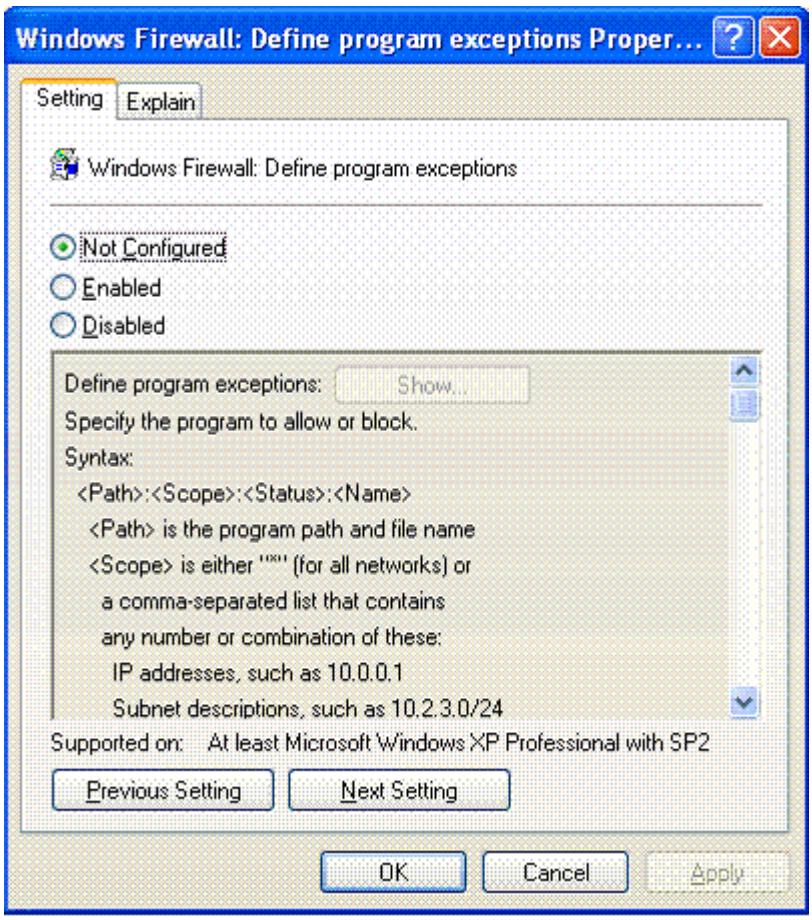


6. Click **OK** to close **Show Contents**.
7. Click **OK** to close **Windows Firewall: Define port exceptions Properties**.

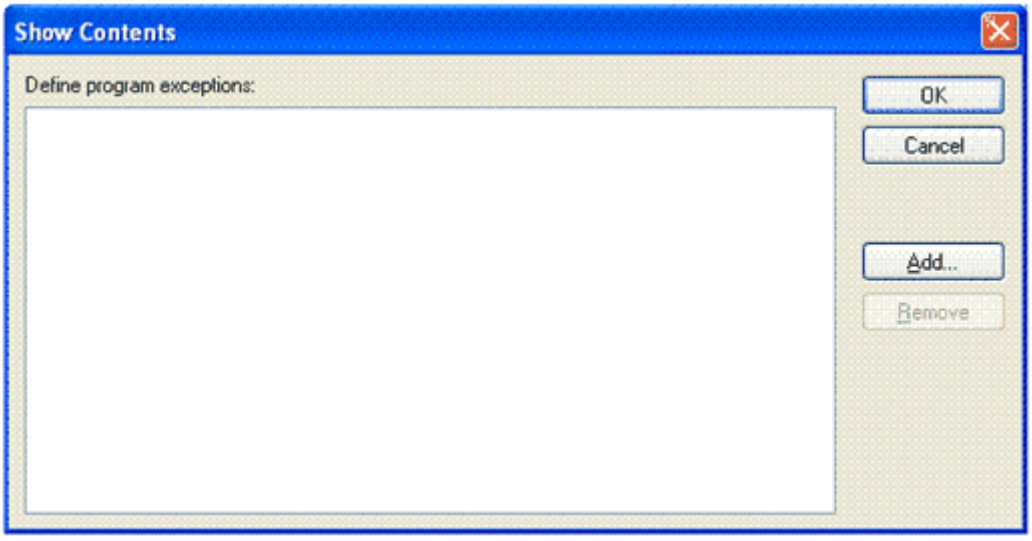
Enabling Exceptions for Programs

To Enable exceptions for programs

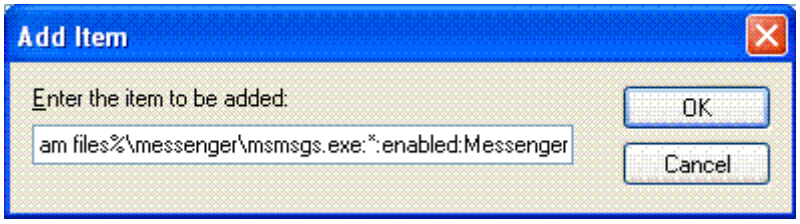
1. In either the **Domain Profile** or **Standard Profile** settings area, double-click **Windows Firewall: Define program exceptions**.



2. Click **Enabled**, and then click **Show**.



3. Click **Add**.



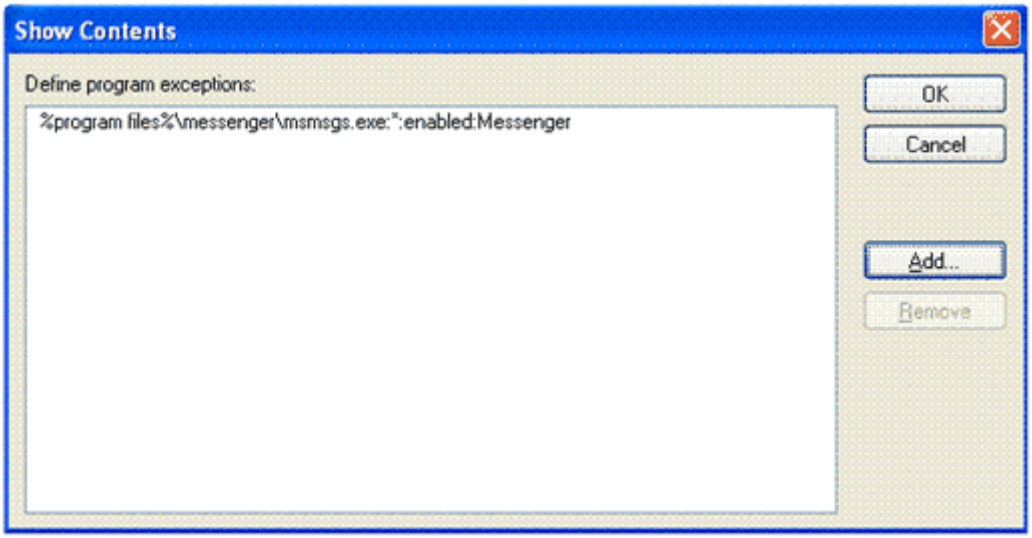
4. Type the information about the program that you want to block or enable. Use this syntax:

path:scope:status:name

Where path is the program path and file name, scope is either * (for all computers) or a list of the computers that are allowed to access the program, status is either enabled or disabled, and name is a text string used as a label for this entry.

This example is named Messenger and enables the Windows Messenger program %program files% \messenger\msmsgs.exe for all connections.

5. Click **OK** to close **Add Item**.

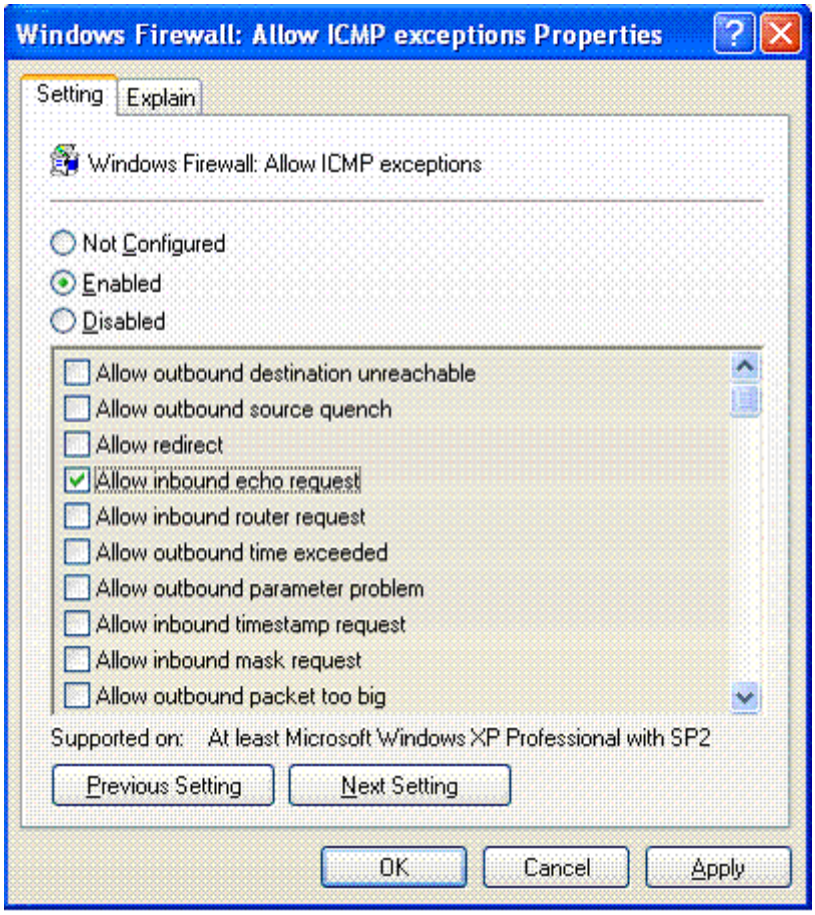


6. Click **OK** to close **Show Contents**.
7. Click **OK** to close **Windows Firewall: Define program exceptions Properties**.

Configuring Basic ICMP Options

To Configure basic ICMP options

1. In either the **Domain** or **Standard** Profile settings area, double-click **Windows Firewall: Allow ICMP exceptions**.
2. Click **Enabled**.

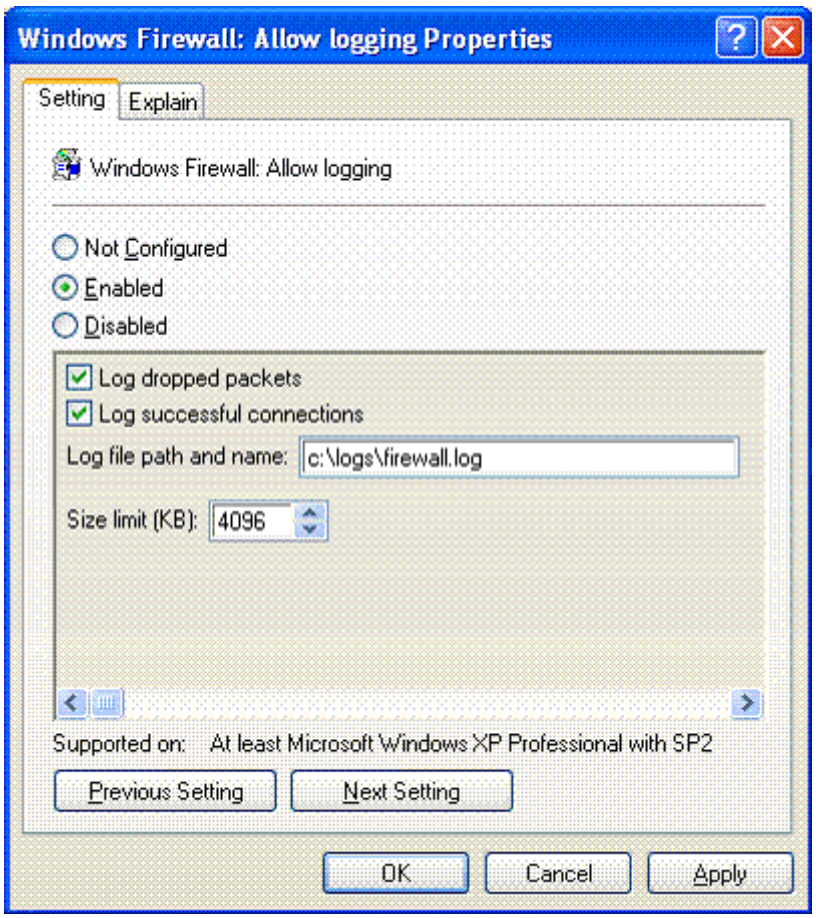


3. Select the appropriate ICMP exception or exceptions to enable.
   This example selects Allow inbound echo request.
4. Click **OK** to close **Windows Firewall: Allow ICMP exceptions Properties**.

Logging Dropped Packets and Successful Connections

To log dropped packets and successful connections

1. In either the **Domain** or **Standard** Profile settings area, double-click **Windows Firewall: Allow logging**.



2. Click **Enabled**, select **Log dropped packets** and **Log successful connections** type a log file path and name, leave the default for the log file size, and then click **OK**.

   Note: You must ensure that the log file is saved in a secured location to prevent accidental or deliberate modification.

3. When you have completed making changes to the Windows Firewall settings, you close the console.

   Note: When you close the console, you are prompted to save the console. Whether you save the console or not your GPO settings will be saved.

4. If prompted to save console settings, click **No**.

Applying Configuration with GPUpdate

The GPUpdate utility refreshes Active Directory–based Group Policy settings. After configuring Group Policy, you can wait for the settings to apply to client computers by the standard refresh cycles. By default these refresh cycles are every 90 minutes, with a random offset of + or - 30 minutes.

To refresh Group Policy between standard cycles, use the GPUpdate utility.

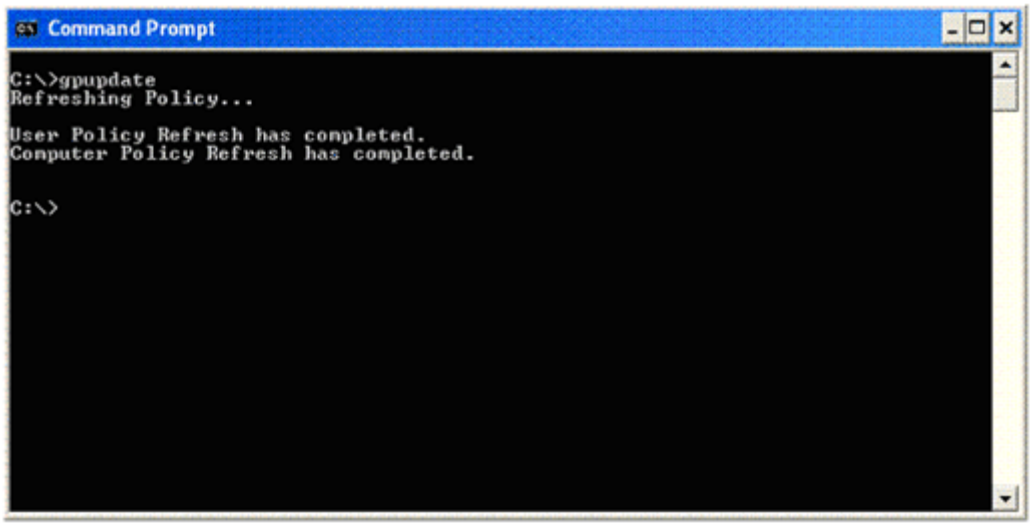
Requirements to perform this task

- Credentials: You must be logged on to a Windows XP SP2 computer that is an Active Directory domain client, as a member of the Domain Users group.

Running GPUpdate

To run GPUpdate

1. From the Windows XP SP2 desktop, click **Start**, click **Run**.
2. In the **Open** box, type **cmd**, and then click **OK**.
3. At the command prompt, type **GPUpdate**, and then press ENTER.



4. To close the command prompt, type **Exit** and press ENTER.

Verifying Windows Firewall Settings Are Applied

Note: When you use Group Policy to configure Windows Firewall you can prevent access to some elements of the configuration for local administrators. If you have prevented access, some tabs and options in the Windows Firewall dialog box are unavailable on user's local machines.

Requirements to perform this task

- Credentials: You must be logged on to a Windows XP SP2 computer that is an Active Directory domain client, as a member of the Domain Users group.

To verify Windows Firewall settings are applied

1. From the Windows XP SP2 desktop, click **Start**, and then click **Control Panel**.
2. Under **Pick a category**, click **Security Center**.

3. Under **Manage security settings for**, click **Windows Firewall**.
4. Click the **General**, **Exceptions**, and **Advanced** tabs, and verify that the configuration in Group Policy is also applied to Windows Firewall, on the client computer.

   Note: If your configuration settings are not applied, you must troubleshoot Group Policy application. To troubleshoot Group Policy application see the following:

   - "Troubleshooting Group Policy in Windows Server 2003" on the Microsoft Download Center at

http://go.microsoft.com/fwlink/?linkid=35481

Related Information

For more information about Windows XP SP2 firewalls, see the following:

- "Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2" on the Microsoft Download Center Web site at http://go.microsoft.com/fwlink/?linkid=35303
- "Understanding Windows Firewall Introduction" on the Microsoft Windows XP Web site at http://go.microsoft.com/fwlink/?linkid=35305

For more information about Windows XP SP2 security, see the following:

- "Windows XP Security Guide, Updated for Service Pack 2" on the Microsoft Download Center Web site at http://go.microsoft.com/fwlink/?linkid=35309
- "Windows XP Security Guide Appendix A: Additional Guidance for Windows XP Service Pack 2" on the Microsoft TechNet Web site at http://go.microsoft.com/fwlink/?linkid=35465

For definitions of security-related terms, see the following:

- "Microsoft Security Glossary" on the Microsoft Web site at http://go.microsoft.com/fwlink/?linkid=35468

Send feedback to Microsoft