



Operating System

Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2

Microsoft Corporation

Published: August 2004

Updated: April 2005

Abstract

Microsoft® Windows® XP Service Pack 2 (SP2) includes the Windows Firewall, a replacement for the Internet Connection Firewall (ICF) provided in previous versions of Windows XP. Windows Firewall is a stateful host-based firewall that discards unsolicited incoming traffic, providing a level of protection for computers against malicious users or programs. To provide better protection for computers connected to any kind of network (such as the Internet, a home network, or an organization network), Windows XP SP2 enables Windows Firewall on all network connections by default. This new behavior can impair some types of communications. This article describes how to deploy the appropriate configuration settings for Windows Firewall on an organization network so that it is enabled and providing protection, and so that needed communications are not impaired.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2004 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows Server, Windows NT, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Overview	1
New Features of Windows Firewall.....	1
Enabled by Default for All of the Connections of the Computer.....	1
New Global Configuration Options that Apply to All Connections.....	2
New Windows Firewall Component of Control Panel.....	2
New Operating Mode	3
Startup Security	3
Incoming Traffic Scoping.....	3
Excepted Traffic Can Be Specified by Program Filename.....	3
Built-in Support for IPv6	4
New Configuration Options	4
Configuration Using Group Policy Settings	5
Windows XP SP2 and the Impact to Enterprise Networks	6
Allowing Users to Install Windows XP SP2 from Windows Update.....	7
Using Windows XP SP2 Windows Firewall and IPSec.....	7
Deploying Windows Firewall Settings With Group Policy	9
Step 1: Updating Your Group Policy Objects With the New Windows Firewall Settings.....	9
Step 2: Specifying Windows Firewall Settings for Your Group Policy Objects.....	11
Recommended Settings for Windows Firewall Group Policy Settings.....	13
Group Policy Settings in Mixed Windows XP Environments	13
Deploying Windows Firewall Settings Without Group Policy	15
Appendix A: Windows Firewall Group Policy Settings	17
Windows Firewall: Allow Authenticated IPSec Bypass.....	17
Windows Firewall: Protect All Network Connections	19
Windows Firewall: Do Not Allow Exceptions	20
Windows Firewall: Define Program Exceptions.....	21
Windows Firewall: Allow Local Program Exceptions	23
Windows Firewall: Allow Remote Administration Exception.....	24
Windows Firewall: Allow File and Print Sharing Exception.....	25
Windows Firewall: Allow ICMP Exceptions.....	27

Windows Firewall: Allow Remote Desktop Exception	28
Windows Firewall: Allow UPnP Framework Exception	29
Windows Firewall: Prohibit Notifications	30
Windows Firewall: Allow Logging.....	31
Windows Firewall: Prohibit Unicast Response to Multicast or Broadcast Requests	32
Windows Firewall: Define Port Exceptions	33
Windows Firewall: Allow Local Port Exceptions	35
Appendix B: Netsh Command Syntax for the Netsh Firewall Context.....	37
add allowedprogram	37
set allowedprogram.....	38
delete allowedprogram.....	39
set icmpsetting	39
set multicastbroadcastresponse	40
set notifications	41
set logging.....	41
set opmode	42
add portopening	42
set portopening	43
delete portopening	44
set service	45
show commands	46
reset	46
Appendix C: Deploying Windows Firewall Settings in a Windows NT 4.0 Domain	47
Appendix D: Allowing Remote Assistance Support	48
Enabling Solicited Remote Assistance	48
Enabling Offer-based Remote Assistance	48
Appendix E: Example of Using the Unattend.txt File.....	49
Appendix F: Example of Using the Netfw.inf File.....	51
Appendix G: Port Numbers for Microsoft Applications and Services	52
Appendix H: Windows Firewall in Windows Server 2003 Service Pack 1	53
Summary	54
Related Links	55

Overview

Windows XP Service Pack 2 (SP2) includes the Windows Firewall, a replacement for the feature previously known as the Internet Connection Firewall (ICF). Windows Firewall is a stateful host firewall that drops all unsolicited incoming traffic that does not correspond to either traffic sent in response to a request of the computer (solicited traffic) or unsolicited traffic that has been specified as allowed (excepted traffic). This behavior of Windows Firewall provides a level of protection from malicious users and programs that use unsolicited incoming traffic to attack computers. With the exception of some Internet Control Message Protocol (ICMP) messages, Windows Firewall does not drop outgoing traffic.

Windows Firewall is also included with Windows Server™ 2003 Service Pack 1 (SP1). For more information, see "Appendix H: Windows Firewall in Windows Server 2003 Service Pack 1" in this article.

New Features of Windows Firewall

In Windows XP SP2, there are many new features for the Windows Firewall, including the following:

- Enabled by default for all of the connections of the computer
- New global configuration options that apply to all connections
- New Windows Firewall component of Control Panel
- New operating mode
- Startup security
- Incoming traffic scoping for IPv4
- Excepted traffic can be specified by program filename
- Built-in support for IPv6
- New configuration options
- Configuration using group policy settings

Enabled by Default for All of the Connections of the Computer

In Windows XP with Service Pack 1 (SP1) and Windows XP with no service packs installed, ICF is disabled by default for all connections, unless enabled for an Internet connection by the Network Setup Wizard or Internet Connection Wizard. You can manually enable ICF through a single checkbox on the **Advanced** tab of the properties of a connection, from which you can also configure the set of excepted traffic by specifying Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports.

Windows Firewall in Windows XP SP2 is globally enabled by default. This means that, by default, all the connections of a computer running Windows XP with SP2 have Windows Firewall enabled, including LAN (wired and wireless), dial-up, and virtual private network (VPN) connections. New connections also have Windows Firewall enabled by default.

Although this provides more protection for Windows XP-based computers, this default behavior can have consequences for the information technology (IT) department of an organization network with regards to application compatibility and the ability to manage the computers on the network. For more information, see "Windows XP SP2 and the Impact to Enterprise Networks" in this article.

New Global Configuration Options that Apply to All Connections

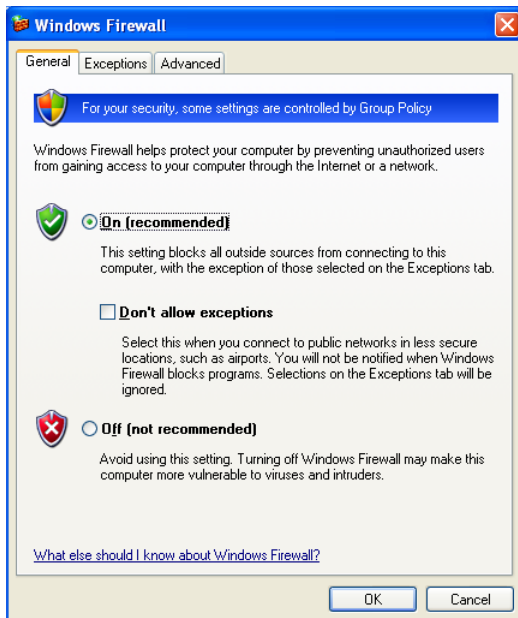
Windows Firewall in Windows XP SP2 allows you to configure settings that apply to all the connections of the computer (global configuration). In Windows XP with SP1 and Windows XP with no service packs installed, ICF settings are configured per connection, which means that if you want to enable ICF on multiple connections and configure excepted traffic, you must configure each connection separately. When you change a global Windows Firewall setting, the change is applied to all the connections on which Windows Firewall is enabled.

Windows Firewall in Windows XP SP2 also allows per-connection configuration. Connection-specific configuration overrides global configuration.

New Windows Firewall Component of Control Panel

The settings for ICF in Windows XP with SP1 and Windows XP with no service packs installed consist of the **Protect my computer and network by limiting or preventing access to this computer from the Internet** check box on the **Advanced** tab of the properties of a connection, and a **Settings** button from which you can configure excepted traffic, logging settings, and excepted ICMP traffic.

In Windows XP SP2, the check box on the **Advanced** tab of the properties of a connection has been replaced with a **Settings** button, which launches the new Windows Firewall component in Control Panel, from which you can configure general settings, exceptions for programs (applications and services), connection-specific settings, log settings, and excepted ICMP traffic. The following figure shows the new **Windows Firewall** dialog box.



You can also configure Windows Firewall from the new Security Center.

For a detailed description of the settings and options of the new Windows Firewall component in Control Panel, see [Manually Configuring Windows Firewall in Windows XP Service Pack 2](#).

The only users who can make changes to Windows Firewall settings are those who log on to the computer with a user account that is a member of the local Administrators group, referred to throughout this article as local administrators. When you configure Windows Firewall in an organization network using Group Policy,

depending on the Group Policy settings, some of the local Windows Firewall configuration options might be grayed out and unavailable, even for local administrators.

New Operating Mode

With Windows XP with SP1 and Windows XP with no service packs installed, ICF is either enabled (allows solicited and excepted traffic) or disabled (allows all traffic).

With Windows XP SP2, you can select a new operating mode corresponding to the **Don't allow exceptions** check box on the **General** tab of the new **Windows Firewall** dialog box. When Windows Firewall is running in this new mode, all unsolicited incoming traffic is dropped, including excepted traffic. This new mode can be used when connecting to the Internet from a public location, such as a hotel or airport, or inside an organization network to temporarily lock down computers during a network attack or when a malicious program is spreading. Once the network attack is over and appropriate updates are installed to prevent future attacks, then Windows Firewall can be placed in the normal operating mode that allows excepted traffic. All of the original settings for excepted traffic are maintained.

Startup Security

In Windows XP with SP1 and Windows XP with no service packs installed, ICF is active on the connections on which it is enabled when the Internet Connection Firewall (ICF)/Internet Connection Sharing (ICS) service is started successfully. Therefore, when a computer running Windows XP with SP1 and Windows XP with no service packs installed is started, there is a delay between when the computer is active on the network and when the connections are protected with ICF. This delay makes the computer vulnerable to attacks during startup.

In Windows XP SP2, there is a startup Windows Firewall policy to perform stateful packet filtering, which allows the computer to perform basic networking startup tasks using Dynamic Host Configuration Protocol (DHCP) and the Domain Name System (DNS) protocol to configure the computer and communicate with a domain controller to obtain Group Policy updates. Once the Windows Firewall (WF)/Internet Connection Sharing (ICS) service is started, it uses its configuration and removes the startup policy. The startup policy settings cannot be configured.

Incoming Traffic Scoping

In Windows XP with SP1 and Windows XP with no service packs installed, the excepted traffic can originate from any IPv4 address. In Windows XP SP2, Windows Firewall allows you to specify that excepted traffic can originate from any IPv4 address, from an IPv4 address that is directly reachable (based on IPv4 routing table entries), from one or more specific IPv4 addresses, or from one or more ranges of IPv4 addresses. This is known as configuring the incoming traffic scope.

For incoming IPv6 traffic, Windows Firewall allows you to specify that excepted traffic can originate from any IPv6 address or from an IPv6 address that is directly reachable (based on IPv6 routing table entries).

For more information about the behavior of Windows Firewall for different types of traffic scopes, see [Manually Configuring Windows Firewall in Windows XP Service Pack 2](#).

Excepted Traffic Can Be Specified by Program Filename

In Windows XP with SP1 and Windows XP with no service packs installed, you manually configure excepted traffic by specifying the set of TCP and UDP ports that correspond to the traffic of a specific program, which can be either an application or service. This can make configuration difficult for users that

do not know the set of TCP and UDP ports for the application or service or how to find them. Also, this configuration does not work for applications that do not listen on a specific set of UDP or TCP ports.

To make the specification of excepted traffic easier, it is possible in Windows XP SP2 to configure excepted traffic by either specifying the set of TCP or UDP ports or the filename of the program (application or service). When the program runs, Windows Firewall monitors the ports on which the program listens and automatically adds them to the list of excepted traffic.

To allow you to quickly enable exceptions for commonly allowed incoming unsolicited traffic, Windows Firewall has pre-defined exceptions, such as File and Printer Sharing and Remote Assistance. Additionally, the notification mechanism in Windows Firewall allows local administrators to automatically add new programs to the excepted programs list after being prompted with a Windows Security Alert message.

Built-in Support for IPv6

Windows Firewall replaces the Internet Protocol version 6 (IPv6) Internet Connection Firewall functionality that is provided in the [Advanced Networking Pack for Windows XP](#). IPv6 support is included with the Windows Firewall and automatically enabled on all IPv6 connections. Both IPv4 and IPv6 share the same settings for excepted traffic. For example, if you except file and print sharing traffic, then both IPv4 and IPv6-based unsolicited incoming file and print sharing traffic is allowed. For more information, see Appendix B.

Note Windows Firewall does not support the same scope options for IPv6 traffic as IPv4 traffic.

New Configuration Options

With Windows XP with SP1 and Windows XP with no service packs installed, the only way to enable or disable ICF is through the Network Connections folder, the Network Setup Wizard, and the Internet Connection Wizard. To configure excepted traffic, you must either use the Network Connections folder or your application must be ICF-aware, in which case it automatically enables excepted traffic when needed.

With Windows XP SP2, Windows Firewall has the following additional configuration options:

- Netsh commands

Netsh is a command-line tool through which you can configure settings for network components. To configure a component, it must support a set of commands through a Netsh context. Windows XP with SP1 and Windows XP with no service packs installed have no Netsh context for ICF. With Windows XP SP2, you can now configure Windows Firewall settings through a series of commands in the **netsh firewall** context. Using Netsh, you can create scripts to automatically configure a set of Windows Firewall settings for both IPv4 and IPv6 traffic. You can also use netsh commands to display the configuration and status of the Windows Firewall. For more information, see Appendix B.

- New configuration application programming interfaces (APIs)

With Windows XP with SP1 and Windows XP with no service packs installed, there are ICF APIs by which applications can automatically configure excepted traffic and configure ICF settings for each connection. You can continue to use the ICF APIs for connection-specific settings. With Windows XP SP2, there are new APIs through which you can configure Windows Firewall global settings for all the items that are available through the Windows Firewall component in Control Panel. You can use these APIs to create customized configuration programs that can be run by individual users or by

management software on an organization network. For information about the new Windows Firewall APIs, see [Windows Firewall](#) in the Windows Software Development Kit (SDK).

NOTE: When applications create exceptions using the ICF or Windows Firewall APIs, the user is not notified. If the application using the ICF or Windows Firewall APIs does not specify an exception name, the exception is not displayed in the exceptions list on the **Exceptions** tab of the Windows Firewall item in Control Panel. You can view exceptions with no names from the display of the **netsh firewall show state** command.

- Extensive support to configure settings using Group Policy

For more information, see the following section, "Configuration Using Group Policy Settings".

Configuration Using Group Policy Settings

To centralize the configuration of large numbers of computers in an organization network that use the Active Directory® directory service, Windows Firewall settings for computers running Windows XP with SP2 can be deployed through Computer Configuration Group Policy. A new set of Computer Configuration Group Policy Windows Firewall settings allow a network administrator to configure Windows Firewall operational modes, excepted traffic, and other settings using a Group Policy object.

When you configure Windows Firewall in an organization network using Group Policy, some of the local Windows Firewall configuration options can be grayed out and unavailable, even for local administrators.

When using the new Windows Firewall Group Policy settings, you can configure two different profiles:

- Domain profile

The domain profile is the set of Windows Firewall settings that are needed when the computer is connected to the network that contains the domain controllers of the organization. For example, the domain profile might contain excepted traffic for the applications needed by a managed computer in an enterprise network.

- Standard profile

The standard profile is the set of Windows Firewall settings that are needed when the computer is not connected to the network that contains the domain controllers of the organization. A good example is when an organization laptop is taken on the road and connects to the Internet using a public broadband or wireless Internet service provider. Because the organization laptop is directly connected to the Internet, the standard profile should contain more restrictive settings than the domain profile.

Note It is strongly recommended that you enable Windows Firewall for both profiles, unless you are already using a third-party host firewall product.

Windows XP SP2 relies on network determination to determine which profile settings to apply. For more information, see [Network Determination Behavior for Network-Related Group Policy Settings](#).

For more information about Windows Firewall Group Policy settings, see "Deploying TCP/IP Windows Firewall Settings With Group Policy" in this article

For information about troubleshooting Windows Firewall, see [Troubleshooting Windows Firewall in Microsoft Windows XP Service Pack 2](#).

Windows XP SP2 and the Impact to Enterprise Networks

For enterprise networks, the default behavior of having Windows Firewall enabled on all network connections might have a significant impact on the types of communication that can occur once Windows XP SP2 is installed. For many enterprise networks using Windows XP with SP1 and Windows XP with no service packs installed, ICF is disabled on all connections connected to the enterprise network because enterprise networks typically are not directly connected to the Internet. The enterprise network firewall, proxy, and other security systems provide a level of protection from the Internet to intranet network computers. However, the absence of host firewalls such as Windows Firewall on intranet connections leaves computers vulnerable to malicious programs brought onto the intranet by computers that are attached directly to the intranet.

For example, an employee connects an organization laptop to a home network that does not have adequate protections. Because the organization laptop does not have a host firewall enabled on its network connection, it gets infected with a malicious program (such as a virus or worm) that uses unsolicited incoming traffic to spread to other computers. The employee then brings his or her laptop back to the office and connects it to the organization intranet, effectively bypassing the security systems that are at the edge of the intranet. Once connected to the intranet, the malicious program begins to infect other computers. If Windows Firewall was enabled by default, the laptop computer might not get infected with the malicious program when connected to their home network. Even if the laptop computer is infected, when it is connected to the intranet, the local intranet computers might not become infected because they also have Windows Firewall enabled.

If the Windows XP with SP2-based computers are running client-based programs, then enabling Windows Firewall does not impair communications. Web access, email, Group Policy, and management agents that request updates from a management server are examples of client-based programs. For client-based programs, the client computer always initiates the communication and all response traffic from a server is allowed by Windows Firewall because it is solicited incoming traffic.

However, the consequences to blocking all unsolicited incoming traffic by default can affect network communications if the computers running Windows XP with SP2 are managed, are servers, are listeners, or are peers. The following lists provide examples of components and capabilities of a computer running Windows XP with SP2 for which communication can be impaired by the default enabling of Windows Firewall:

- **The Windows XP with SP2-based computer is managed** Examples of computer management components and features are the following:
 - Simple Network Management Protocol (SNMP) Agent
 - Windows Management Interface (WMI)
 - Remote management using Netsh or a Microsoft Management Console (MMC) snap-in
 - Remote Assistance and Remote Desktop
 - Desktop management software that relies on information being pushed out from a management station
- **The Windows XP with SP2-based computer is acting as a server** Examples of server services included with Windows XP SP2 are the following:
 - Internet Information Services (IIS)

- File and Printer Sharing
- Message Queuing
- Simple TCP/IP Services
- Print Services for UNIX
- **The Windows XP with SP2 computer is acting as a listener** Examples of components included with Windows XP SP2 that listen are the following:
 - UPnP™
 - Routing Information Protocol (RIP) Listener
 - Incoming Connections
- **The Windows XP with SP2-based computer is acting as a peer** Examples include the following:
 - Instant messaging programs
 - Third-party peer-to-peer networking applications

If your network is using any of these components included with Windows XP SP2, provided by Microsoft as separate products, or provided by third parties, then by default, communication might be impaired when Windows XP SP2 is installed. To prevent this from happening, Windows XP SP2 must be deployed with the appropriate Windows Firewall exception settings to allow the computer to act as a managed computer, a server, a listener, or a peer for those applications and services being used on your network.

Because the deployment of Windows XP SP2 can impact communications on your network, it is highly recommended that you test Windows XP SP2 with critical administrative and business applications before deploying it on your production network.

The details of deploying Windows Firewall settings for Windows XP SP2 are described in "Deploying TCP/IP Windows Firewall Settings With Group Policy" and "Deploying Windows Firewall Settings Without Group Policy" in this article.

Allowing Users to Install Windows XP SP2 from Windows Update

When planning your deployment of Windows XP SP2, one of the issues that you must confront is whether you will allow your network users to download and install Windows XP SP2 from Windows Update. Only local administrators can install Windows XP SP2. If this is the case and you allow them to install Windows XP SP2, then after it is installed on a computer, that computer might not be manageable using your management software because Windows Firewall is enabled by default. The computer might not become manageable until Windows Firewall is configured with the appropriate excepted traffic. This can be done using Group Policy settings, a script, or a configuration program.

If you do not allow your users to install Windows XP SP2, then you can use your management software to deploy Windows XP SP2 along with the appropriate Windows Firewall settings (using the Unattend.txt file or the Netfw.inf file) so that at all times during the deployment, the computers on your network are manageable.

Using Windows XP SP2 Windows Firewall and IPSec

Windows Firewall blocks unsolicited incoming traffic. However, you cannot configure Windows Firewall to block outgoing traffic. Internet Protocol security (IPSec), built into Windows XP, can provide this extra level

of protection. Using IPSec policies, you can specify the traffic that is blocked (dropped), permitted (allowed), or protected using cryptography for both outgoing and incoming traffic. In any of these three cases (blocked, permitted, protected), IPSec can be configured for a specific range of source and destination addresses.

If you are already using IPSec to block, permit, or protect traffic, then Windows Firewall on computers running Windows XP with SP2 provides additional protection against attacks based on incoming unsolicited traffic.

IPSec in Windows XP with SP2 is Windows Firewall-aware. When there is an active IPSec policy, the IPSec components of Windows XP with SP2 instruct the Windows Firewall to open UDP ports 500 and 4500 to allow Internet Key Exchange (IKE) traffic.

An additional feature of IPSec support is that you can specify through Group Policy that all IPSec-protected traffic bypass Windows Firewall processing. For more information, see Appendix A.

Deploying Windows Firewall Settings With Group Policy

The best way to manage Windows Firewall settings in an organization network is to use Active Directory and the new Windows Firewall settings in Computer Configuration Group Policy. This method requires the use of Active Directory with either Windows 2000 or Windows Server 2003 domain controllers. Group Policy updates are requested by the domain member computer, and are therefore solicited traffic that is not dropped when Windows Firewall is enabled.

When you use Group Policy to configure Windows Firewall, by default local administrators will be unable to change some elements of its configuration locally, using the Windows Firewall component in Control Panel. Some tabs and options in the Windows Firewall dialog box will be grayed out and unavailable.

The basic steps for deploying Windows Firewall settings for Windows XP SP2 with Active Directory are the following:

1. Update your Group Policy objects with the new Windows Firewall settings.
2. Specify Windows Firewall settings for your Group Policy objects.

The following sections describe these steps in detail.

Notes It is strongly recommended that you test your 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 result in unintended vulnerabilities.

The procedure to update your Group Policy object with the new Windows Firewall settings will replace the System.adm file that is stored for the Group Policy object being modified with the version that is provided with Windows XP SP2, which includes the new Windows Firewall settings. If a Group Policy administrator on your production network performs this procedure, your production environment will be updated.

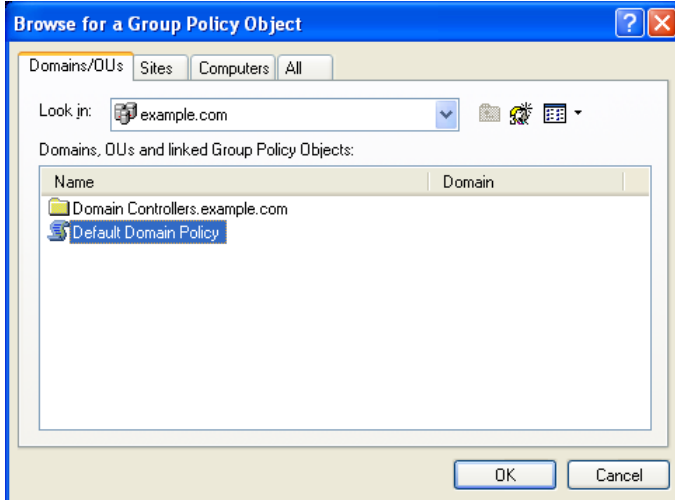
Once you update your Group Policy objects, you can only modify them from a computer running Windows XP with SP2. An update is available through Microsoft Product Support Services (PSS) to allow you to modify Group Policy settings from computers running Windows 2000. Microsoft is working on updates for Windows XP SP1 and Windows Server 2003.

Step 1: Updating Your Group Policy Objects With the New Windows Firewall Settings

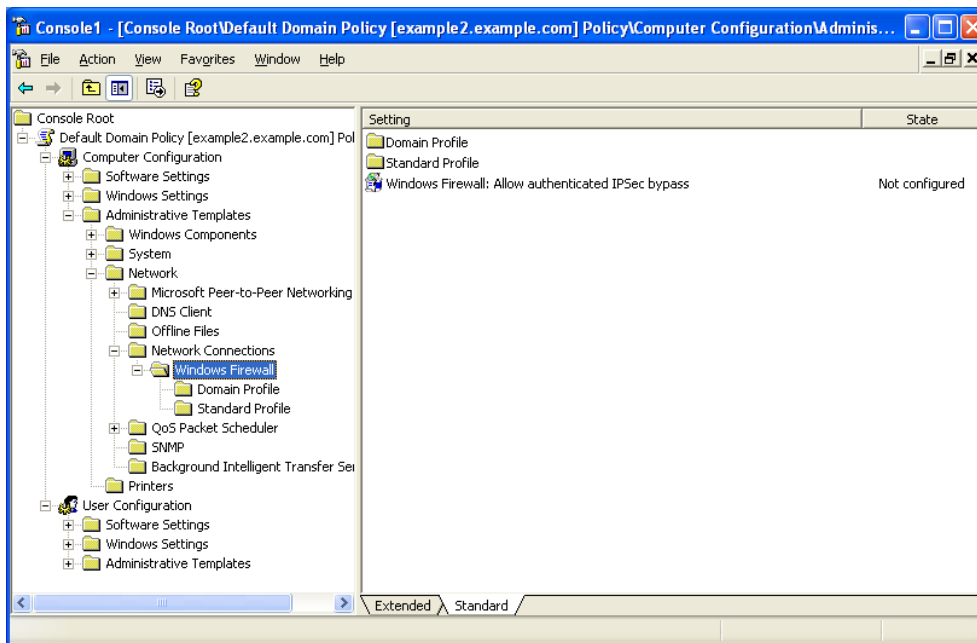
To update your Group Policy objects with the new Windows Firewall settings using the Group Policy snap-in (provided with Windows XP), do the following:

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](#).

Step 2: Specifying Windows Firewall Settings for Your Group Policy Objects

After a Group Policy object has been updated, it can be configured for Windows Firewall settings that are appropriate for Windows Firewall and the use of management, server, listener, or peer applications and services that are being run on your computers running Windows XP with SP2.

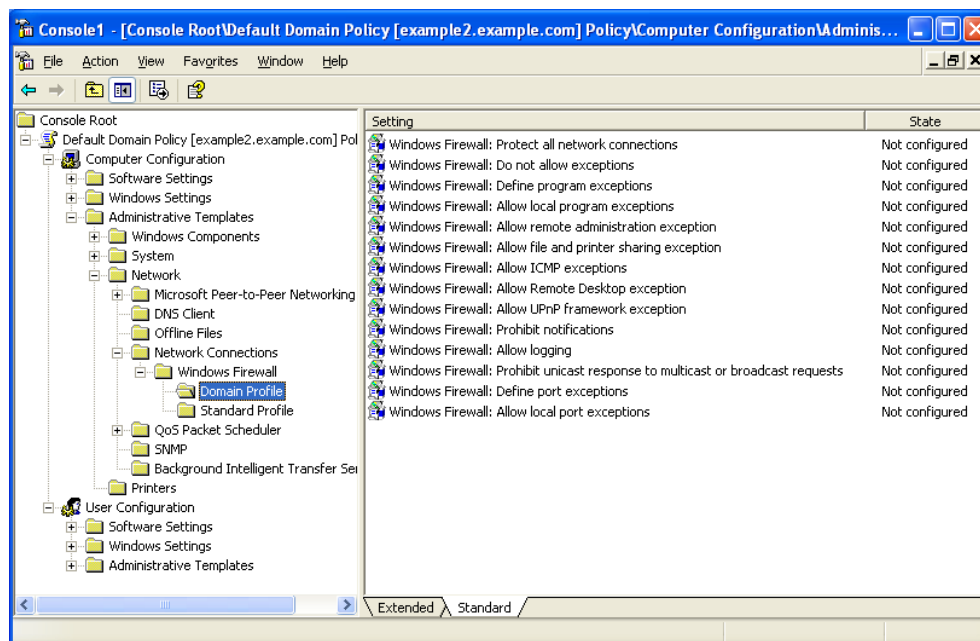
There are two sets of Windows Firewall settings to configure:

- The domain profile settings that are used by the computers when they are connected to a network that contains domain controllers for the domain of which the computer is a member.
- The standard profile settings that are used by the computers when they are connected to a network that does not contain domain controllers for the domain of which the computer is a member.

If you do not configure standard profile settings, their default values are still applied. Therefore, it is highly recommended that you configure both domain and standard profile settings and that you enable the Windows Firewall for both profiles, except if you are already using a third-party host firewall product.

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

Both the domain profile and standard profile contain the same set of Windows Firewall settings, as shown in the following figure.



The Windows Firewall Group Policy settings for the domain and standard profiles consist of the following:

- **Windows Firewall: Protect all network connections** Used to specify that all network connections have Windows Firewall enabled.
- **Windows Firewall: Do not allow exceptions** Used to specify that all unsolicited incoming traffic be dropped, including excepted traffic.
- **Windows Firewall: Define program exceptions** Used to define excepted traffic in terms of program file names.
- **Windows Firewall: Allow local program exceptions** Used to enable local configuration of program exceptions.
- **Windows Firewall: Allow remote administration exception** Used to enable remote configuration using tools such as Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI).
- **Windows Firewall: Allow file and print sharing exception** Used to specify whether file and printer sharing traffic is allowed.
- **Windows Firewall: Allow ICMP exceptions** Used to specify the types of Internet Control Message Protocol (ICMP) messages that are allowed.
- **Windows Firewall: Allow Remote Desktop exception** Used to specify whether the Windows XP-based computer can accept a Remote Desktop-based connection request.
- **Windows Firewall: Allow UPnP framework exception** Used to specify whether the computer can receive unsolicited UPnP messages.
- **Windows Firewall: Prohibit notifications** Used to disable notifications.
- **Windows Firewall: Allow logging** Used to enable logging of discarded traffic, successful connections, and to configure log file settings.
- **Windows Firewall: Prohibit unicast response to multicast or broadcast requests** Used to discard the unicast packets received in response to a multicast or broadcast request message.
- **Windows Firewall: Define port exceptions** Used to specify excepted traffic in terms of TCP and UDP ports.
- **Windows Firewall: Allow local port exceptions** Used to enable local configuration of port exceptions.

For detailed information about these settings, including example dialog boxes, see Appendix A.

Use the Group Policy snap-in to modify the Windows Firewall settings in the appropriate Group Policy objects. Note that you only need to modify Windows Firewall settings for Group Policy objects that are applied to Active Directory system containers (domains, organizational units, and sites) that contain computer accounts corresponding to computers that are or will be running Windows XP with SP2.

Once you configure the Windows Firewall settings, the next refresh of Computer Configuration Group Policy downloads the new Windows Firewall settings and applies them for computers running Windows XP with SP2. Computers that are running Windows 2000, Windows Server 2003 with no service packs installed, Windows XP with SP1, or Windows XP with no service packs installed ignore the new Windows Firewall settings.

Recommended Settings for Windows Firewall Group Policy Settings

The following are the recommendations for the Windows Firewall Group Policy settings for Windows XP SP2:

- **Windows Firewall: Protect all network connections** Enabled
- **Windows Firewall: Do not allow exceptions** Not configured
- **Windows Firewall: Define program exceptions** Enabled and configured with the programs (applications and services) used by the computers running Windows XP with SP2 on your network for managed, server, listener, or peer applications.
- **Windows Firewall: Allow local program exceptions** Enabled, unless you don't want local administrators to be able to configure program exceptions locally.
- **Windows Firewall: Allow remote administration exception** Disabled, unless you want to be able to remotely administer with MMC snap-ins or remotely monitor using WMI computers running Windows XP with SP2.
- **Windows Firewall: Allow file and print sharing exception** Enabled only if the computers running Windows XP with SP2 are sharing local folders and printers.
- **Windows Firewall: Allow ICMP exceptions** Enabled only to allow diagnostic or management capabilities that are based on ICMP traffic.
- **Windows Firewall: Allow Remote Desktop exception** Enabled only if you use Remote Desktop to connect to Windows XP with SP2-based computers.
- **Windows Firewall: Allow UPnP framework exception** Enabled only if you use UPnP devices on your network.
- **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** Enabled and configured with the TCP and UDP ports used by the computers running Windows XP with SP2 on your network for managed, server, listener, or peer programs that cannot be specified by filename.
- **Windows Firewall: Allow local port exceptions** Enabled, unless you don't want local administrators to be able to configure port exceptions locally.

Group Policy Settings in Mixed Windows XP Environments

A mixed Windows XP environment is one in which there are both Windows XP with SP1 or Windows XP with no service packs installed and Windows XP with SP2-based computers present. For computers running Windows XP with SP1 or Windows XP with no service packs installed, the only way to control Windows Firewall behavior through Group Policy is to use the **Prohibit use of Internet Connection Firewall on your DNS domain network** Computer Configuration Group Policy setting in Computer Configuration/Administrative Templates/Network/Network Connections. This Group Policy setting is still present when Group Policy objects are updated for the new Windows Firewall settings. Computers running Windows XP with SP1 or Windows XP with no service packs installed only implement the **Prohibit use of**

Internet Connection Firewall on your DNS domain network Computer Configuration Group Policy setting.

Computers running Windows XP with SP2 implement both the **Prohibit use of Internet Connection Firewall on your DNS domain network** setting and the new Windows Firewall settings in the following way:

- If the **Prohibit use of Internet Connection Firewall on your DNS domain network** setting is enabled and there are no changes to the default values of the new Windows Firewall settings, then Windows Firewall is disabled when connected to the network from which the Group Policy object was obtained.
- If the **Prohibit use of Internet Connection Firewall on your DNS domain network** setting is enabled and the **Windows Firewall: Protect all network connections** setting is enabled, then Windows Firewall is enabled when connected to the network from which the Group Policy object was obtained with new Windows Firewall settings.

Disabling the Use of Windows Firewall Across Your Network

If you are already using a third-party host firewall product, then it is recommended that you disable Windows Firewall. If you are not already using a third-party host firewall product, then it is recommended that you enable Windows Firewall to prevent the spread of malicious programs that make it past the firewall that separates your network from the Internet.

If you decide to disable the use of Windows Firewall across your entire organization network, which contains a mixture of computers running Windows XP with SP2, Windows XP with SP1, and Windows XP with no service packs installed, and you are using a third-party host firewall, then you should configure the following Group Policy settings:

- **Prohibit use of Internet Connection Firewall on your DNS domain network** is set to **Enabled**
- **Domain profile – Windows Firewall: Protect all network connections** is set to **Disabled**
- **Standard profile – Windows Firewall: Protect all network connections** is set to **Disabled**

These settings ensure that Windows Firewall is not used, whether the computers are connected to your organization network or not.

If you decide to disable the use of Windows Firewall across your entire organization network, which contains a mixture of computers running Windows XP with SP2, Windows XP with SP1, and Windows XP with no service packs installed, and you are not using a third-party host firewall, then you should configure the following Group Policy settings:

- **Prohibit use of Internet Connection Firewall on your DNS domain network** is set to **Enabled**
- **Domain profile – Windows Firewall: Protect all network connections** is set to **Disabled**
- **Standard profile – Windows Firewall: Protect all network connections** is set to **Enabled**

These settings ensure that the Windows Firewall is not used on your organization network, but is used when the computers are not connected to the organization network.

Deploying Windows Firewall Settings Without Group Policy

Although Group Policy is the recommended and easiest method to deploy Windows Firewall settings for computers running Windows XP with SP2, there are situations in which this method is not possible or not used. For example, an environment that uses Windows NT® 4.0 domains or that uses workgroups cannot use Active Directory and Group Policy to propagate Windows Firewall settings to multiple computers on an organization network. Another example is an organization that uses Active Directory, but does not use Group Policy to centrally configure user or computer configuration settings. For information about deploying Windows Firewall settings in a Windows NT 4.0 domain, see Appendix C.

When Group Policy cannot be used or is not used, you have the following options to configure Windows Firewall settings for computers running Windows XP with SP2:

- Use the Unattend.txt file to configure Windows Firewall settings

The Unattend.txt file for Windows XP SP2 has options to configure Windows Firewall settings when running an unattended setup of Windows XP SP2. For more information, see Appendix E.

- Use the Netfw.inf file to configure Windows Firewall settings

The Netfw.inf file for Windows XP SP2 can configure the Windows Firewall by specifying a set of registry settings equivalent to the options available from the Windows Firewall component in Control Panel and through Windows Firewall Group Policy settings when a user is performing an interactive setup of Windows XP SP2. For more information, see Appendix F.

- Run a script file that contains Netsh commands to configure Windows Firewall settings

To configure computers running Windows XP with SP2 after SP2 has been installed, you can have your users run a script file, such as a batch file (*.BAT) or a command file (*.CMD), that contains the series of Netsh commands to configure the Windows Firewall operational mode, allowed programs, allowed ports, etc. For more information about using Netsh to configure Windows Firewall, see Appendix B. For more information about the Netsh tool, see [Managing Windows 2000 Networking Components with Netsh](#).

- Run a custom configuration program that uses the new Windows Firewall APIs to configure Windows Firewall settings

To configure computer running Windows XP with SP2 after Windows XP SP2 has been installed, you can have your users run a custom configuration program that uses the new Windows Firewall configuration APIs to configure the Windows Firewall for operation mode, allowed programs, allowed ports, and other settings. For information about the new Windows Firewall APIs, see [Windows Firewall](#) in the Windows Software Development Kit (SDK).

For both the script file or the custom configuration program, you can deploy them to be run by your users in the following ways:

- If you are running management software, configure it to have each computer running Windows XP with SP2 download the script or configuration program and run it or to run it from a network location.
- Send either the script or program file or a link to the script or program file in an email message with instructions that users of computer running Windows XP with SP2 must run it.

- Place the script or program on a Web page and instruct the users of computers running Windows XP with SP2 to access the Web page and run it.

Only local administrators can successfully execute scripts or custom configuration programs from an email message, a file share, or a Web page.

Disabling the Use of Windows Firewall Across Your Network

If you decide to disable the use of Windows Firewall across your entire network, and you are not or cannot use the Windows Firewall Group Policy settings, you can use the Unattend.txt or Netfw.inf to disable Windows Firewall as Windows XP SP2 is being installed. For an example of using Unattend.txt, see Appendix E. For an example of using Netfw.inf, see Appendix F.

Depending on your network policies, your users might elect, either intentionally or accidentally, to install Windows XP SP 2 through Windows Update, rather than through a central network location that contains the modified Netfw.inf file. If this occurs, the modified Netfw.inf file is not read during the installation and Windows Firewall is enabled.

One solution to this possible problem is to create the registry settings on your client computers to disable Windows Firewall before your users have a chance to install Windows XP SP2 from Windows Update. ICF on computers running Windows XP with SP1 and Windows XP with no service packs installed ignores these registry settings. When the user installs Windows XP SP2 from Windows Update and restarts their computer, Windows Firewall reads the registry settings already in place and disables itself.

To add a registry setting on all of your computers running Windows XP, you can use the Regini.exe or Reg.exe tools. For either tool, you create a script file that is read by the tool to add a registry setting. The tool has to be run in the security context of a local administrator account.

Alternately, you can use network management software to change registry settings on managed computers.

The registry keys to add to disable Windows Firewall for both the domain and standard profiles are the following:

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\EnableFirewall=0 (DWORD data type)
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\EnableFirewall=0 (DWORD data type)

Appendix A: Windows Firewall Group Policy Settings

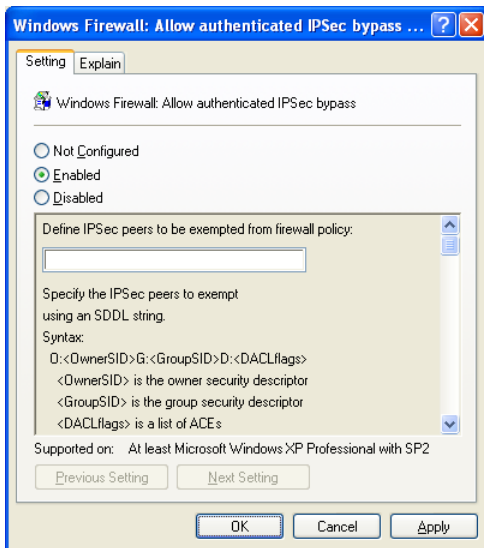
This appendix describes the details of the following Windows Firewall Group Policy settings found in the Group Policy snap-in in the following locations:

- Computer Configuration/Administrative Templates/Network/Network Connections/Windows Firewall
 - Windows Firewall: Allow authenticated IPSec bypass
- Computer Configuration/Administrative Templates/Network/Network Connections/Windows Firewall/Domain Profile and Computer Configuration/Administrative Templates/Network/Network Connections/Windows Firewall/Standard profile
 - Windows Firewall: Protect all network connections
 - Windows Firewall: Do not allow exceptions
 - Windows Firewall: Define program exceptions
 - Windows Firewall: Allow local program exceptions
 - Windows Firewall: Allow remote administration exception
 - Windows Firewall: Allow file and print sharing exception
 - Windows Firewall: Allow ICMP exceptions
 - Windows Firewall: Allow Remote Desktop exception
 - Windows Firewall: Allow UPnP framework exception
 - Windows Firewall: Prohibit notifications
 - Windows Firewall: Allow logging
 - Windows Firewall: Prohibit unicast response to multicast or broadcast requests
 - Windows Firewall: Define port exceptions
 - Windows Firewall: Allow local port exceptions

Note Windows Firewall Group Policy settings are subject to Group Policy inheritance rules and behaviors. For more information, see the topic titled "Policy inheritance" in Windows 2000 Server Help or Windows Server 2003 Help and Support.

Windows Firewall: Allow Authenticated IPSec Bypass

The **Windows Firewall: Allow authenticated IPSec bypass** setting allows you to specify that the Windows Firewall does not process IPSec-secured traffic from specified computers. The following figure shows the **Windows Firewall: Allow authenticated IPSec bypass** setting.



When IPSec is used to secure traffic, IPSec peers must perform mutual computer-level authentication before secured traffic is sent. This mutual authentication is typically performed in an Active Directory environment using Kerberos v5 or with public key certificates. In both cases, credentials that are administered by a central IT organization establish the trust in the IPSec peer.

The **Windows Firewall: Allow authenticated IPSec bypass** setting can be enabled for organization networks that:

- Use IPSec to protect traffic.
- Enable the Windows Firewall.
- Assume that if the traffic is IPSec-protected, then it does not need to be inspected by the firewall.

One common use of this setting is to prevent Windows Firewall from processing the IPSec-protected traffic of a network security vulnerability scanning system.

You can select the following:

- Not Configured (default) or Disabled

Windows Firewall processes IPSec-secured traffic. The difference between the Not Configured and Disabled settings is based on Group Policy inheritance rules.

- Enabled

Windows Firewall does not process IPSec-secured traffic.

When you select Enabled, you must type or paste the Security Descriptor Definition Language (SDDL) string that corresponds to the group accounts for the computers to which this policy applies. The format of the SDDL string to enter in the text box for a single group is:

O:DAG:DAD:(A;;RCGW;;;SID)

in which *SID* is the Security Identifier (SID) of a group account. To obtain the SID of a group account, use the Getsid.exe tool from [Windows Server 2003 Resource Kit Tools](#). Getsid.exe is typically used to compare the SIDs of two accounts on different domain controllers, but you can also use it to obtain the SID of a specified user or group account.

To obtain a SID for a group account, use the following syntax:

```
getsid \\domain_controller group_account \\domain_controller group_account
```

in which *domain_controller* is the computer name of a domain controller and *group_account* is the group account name.

Here is an example for a domain controller named EXAMPLE2 for the example.com domain:

```
C: \>getsid \\example2 IPSecComputers \\example2 IPSecComputers
```

```
The SID for account EXAMPLE\IPSecComputers matches account EXAMPLE\IPSecComputers
The SID for account EXAMPLE\IPSecComputers is S-1-5-21-3575094098-3669797271-991787341-1127
The SID for account EXAMPLE\IPSecComputers is S-1-5-21-3575094098-3669797271-991787341-1127
```

Therefore, the SID for the IPSecComputers group account is S-1-5-21-3575094098-3669797271-991787341-1127.

For this example, the entry in the **Windows Firewall: Allow authenticated IPSec bypass** setting to specify that the IPSec-secured traffic that is received from computers that are members of the IPSecComputers group is not processed by the Windows Firewall is the following:

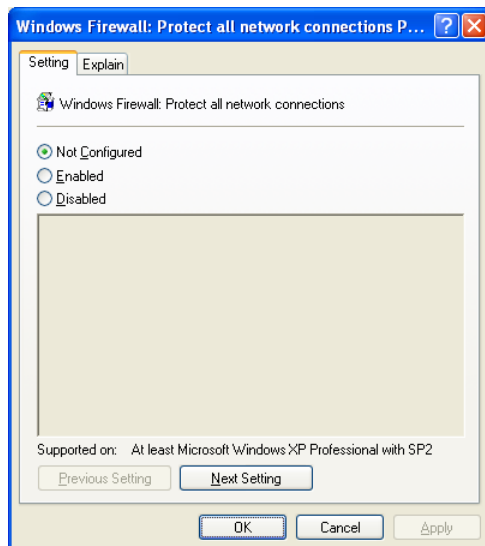
```
O:DAG:DAD:(A;;RCGW;;;S-1-5-21-3575094098-3669797271-991787341-1127)
```

If you have more than one group, then the syntax for the SDDL string is:

```
O:DAG:DAD:(A;;RCGW;;;SID1) (A;;RCGW;;;SID2) (A;;RCGW;;;SID3)...
```

Windows Firewall: Protect All Network Connections

The **Windows Firewall: Protect all network connections** setting allows you to specify the operating mode of Windows Firewall, and is shown in the following figure.



You can select the following:

- Not Configured (default)

No change to the status of Windows Firewall is made. Local administrators may enable or disable Windows Firewall locally, such as from the **General** tab of the Windows Firewall component in Control

Panel.. The Windows Firewall runs unless you enable the **Prohibit use of Internet Connection Firewall on your DNS domain network** Group Policy setting.

- Enabled

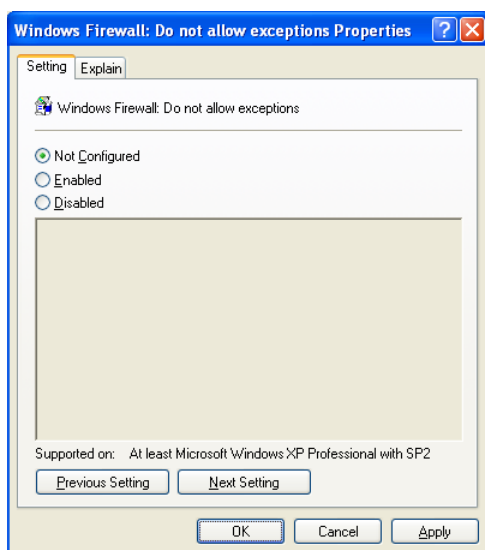
Windows Firewall is enabled to protect all network connections and local administrators cannot enable or disable Windows Firewall locally. The **Prohibit use of Internet Connection Firewall on your DNS domain network** Group Policy setting is ignored.

- Disabled

Disables Windows Firewall. Local administrators cannot enable the Windows Firewall.

Windows Firewall: Do Not Allow Exceptions

The **Windows Firewall: Do not allow exceptions** setting is used to discard all incoming unsolicited traffic, including excepted traffic, and is shown in the following figure.



You can select the following:

- Not Configured (default)

Local administrators can enable or disable the operational mode in which no exceptions are allowed, such as from the **General** tab of the Windows Firewall component in Control Panel.

- Enabled

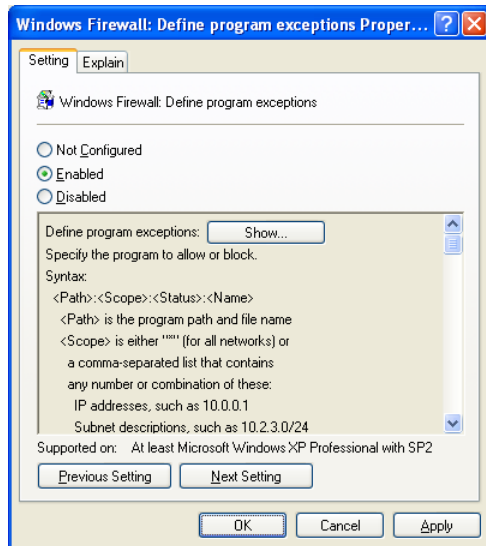
Excepted traffic is not allowed. You should also enable the **Windows Firewall: Protect all network connections** setting. Otherwise, local administrators can thwart the **Windows Firewall: Do not allow exceptions** setting by disabling the Windows Firewall locally. Enabling this setting does not affect other Windows Firewall local or Group Policy settings, which are restored when you set this setting to Not Configured or Disabled.

- Disabled

Local administrators cannot enable the operational mode in which no exceptions are allowed.

Windows Firewall: Define Program Exceptions

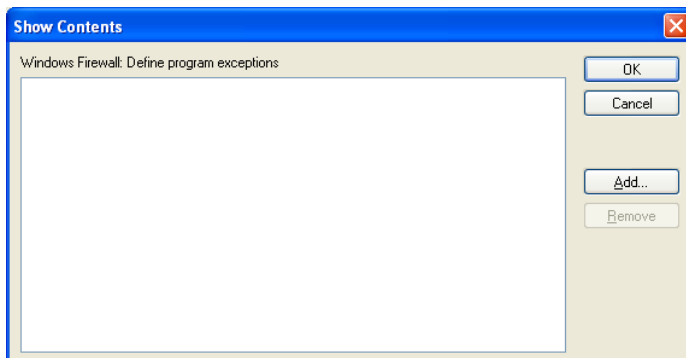
The **Windows Firewall: Define program exceptions** setting allows you to configure excepted traffic by specifying the program's file name, and is shown in the following figure.



You can select the following:

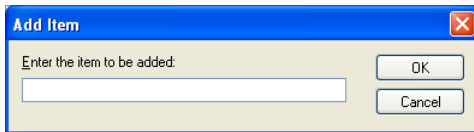
- **Not Configured (default)**
No excepted traffic is configured. Local administrators can specify allowed programs locally, such as from the **Exceptions** tab of the Windows Firewall component in Control Panel, unless the **Windows Firewall: Allow local program exceptions** setting is set to **Disabled**.
- **Enabled**
The configured program exceptions are excepted traffic. All locally configured program exceptions are ignored, including settings pre-defined through setup files, as described in Appendix E and Appendix F.
- **Disabled**
No excepted traffic is configured. The program exceptions list defined by Group Policy is deleted and the one defined by local administrators is ignored, unless you enable the **Windows Firewall: Allow local program exceptions** policy setting.

To define the list of allowed programs, click **Enabled**, and then click **Show**. The **Show Contents** dialog box is displayed. An example is shown in the following figure.



From **Show Contents**, you can add or remove an allowed program. You cannot edit an existing allowed program. To change an existing allowed program, remove it, and then add with the correct parameters.

To add a new allowed program, click **Add**. An example is shown in the following figure.



In **Add Item**, type the parameters for an allowed program using the following syntax:

ProgramPath:Scope:Enabled|Disabled:ApplicationName

- *ProgramPath*

Type the path and file name of the application as it is installed on the computers running Windows XP with SP2. You can use environment variables such as %ProgramFiles% when specifying the program path.

- *Scope*

The *Scope* parameter specifies the addresses from which the traffic is allowed. Type * to specify traffic originating from any source IPv4 address or a comma separated list of sources. The sources can be **LocalSubnet** to specify traffic originating from a directly reachable IPv4 address or one or more IPv4 addresses or IPv4 address ranges separated by commas. IPv4 address ranges typically correspond to subnets. For IPv4 addresses, type the IPv4 address in dotted decimal notation. For IPv4 address ranges, you can specify the range using a dotted decimal subnet mask or a prefix length. When you use a dotted decimal subnet mask, you can specify the range as an IPv4 network ID (such as 10.47.81.0/255.255.255.0) or by using an IPv4 address within the range (such as 10.47.81.231/255.255.255.0). When you use a network prefix length, you can specify the range as an IPv4 network ID (such as 10.47.81.0/24) or by using an IPv4 address within the range (such as 10.47.81.231/24). The following is an example list of sources:

Local Subnet, 10. 91. 12. 56, 10. 7. 14. 9/255. 255. 255. 0, 10. 116. 45. 0/255. 255. 255. 0, 172. 16. 31. 11/24, 172. 16. 111. 0/24

IPv6 traffic supports the * and **LocalSubnet** scopes.

Note If you have any spaces between the entries in the list of sources or any other invalid characters, the scope is ignored and the setting behaves as if it were disabled. Please double-check your scope syntax before saving changes.

Host names, DNS names, or DNS suffixes are not supported.

- **Enabled|Disabled**

This is the Status parameter. Type **Enabled** to allow incoming unsolicited traffic to this application. Type **Disabled** to prevent the program from being allowed in the exceptions list. This does not prevent excepted programs from running or receiving solicited incoming traffic if the ports are opened elsewhere or by another application.

- *ApplicationName*

Type a friendly name for the program. This becomes the name of the program in the list of allowed programs in the Windows Firewall settings of the computers running Windows XP with SP2.

The following is an example of an allowed program entry:

```
%ProgramFiles%\ExampleAppFolder\Example.exe*:Enabled:Example Program
```

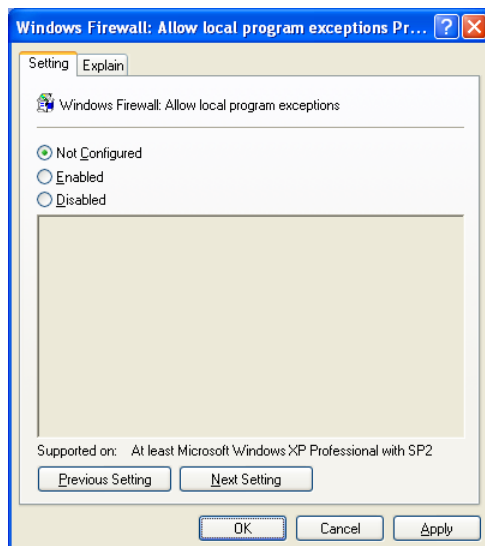
If you type an invalid program definition string, Windows Firewall adds it to the list without checking for errors. This allows you to add programs that you have not installed yet.

It is possible to create multiple entries for the same program with conflicting Scope or Status parameters. If entries have conflicting Scope parameters, any system specified by any entry can send messages to this program. If the Status parameter of a definition string is set to Disabled, Windows Firewall prohibits incoming messages to this program. If entries have different Status values, then any definition with the Status set to Disabled overrides all definitions with the Status set to Enabled, and the program does not receive the messages. Therefore, if you set the Status to Disabled, you can prevent local administrators from enabling the program.

Windows Firewall opens ports for the program only when the program is running and listening for incoming traffic. If the program is not running, or is running but not listening for those messages, Windows Firewall does not open its ports.

Windows Firewall: Allow Local Program Exceptions

The **Windows Firewall: Allow local program exceptions** setting allows you to specify whether local administrators are allowed to configure their own program exceptions, and is shown in the following figure.



You can select the following:

- Not Configured (default)

If the **Windows Firewall: Define program exceptions** setting is set to Not Configured, local administrators can add program exceptions locally, such as from the **Exceptions** tab of the Windows Firewall component in Control Panel.

- Enabled

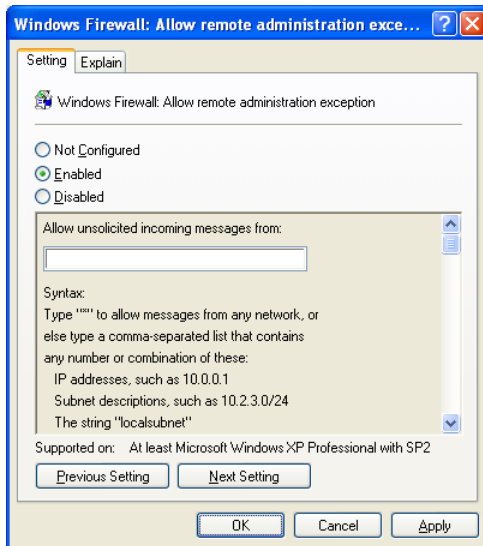
Local administrators can add program exceptions.

- Disabled

Local administrators cannot add program exceptions.

Windows Firewall: Allow Remote Administration Exception

The **Windows Firewall: Allow remote administration exception** setting allows you to specify whether computers running Windows XP with SP2 can be remotely administered by applications that use TCP ports 135 and 445 (such as MMC and WMI), and is shown in the following figure.



Services that use these ports to communicate are using remote procedure calls (RPC) and Distributed Component Object Model (DCOM) to access remote hosts. In effect, Windows Firewall adds Svchost.exe and Lsass.exe to the program exceptions list and allows those services to open additional, dynamically assigned ports, typically in the range of 1024 to 1034. Windows Firewall also allows incoming ICMP Echo messages (also known as the ICMP Echo Request messages).

You can select the following:

- Not Configured (default)

Remote administration is not allowed.

- Enabled

Windows Firewall allows the computer to receive the unsolicited incoming messages associated with remote administration. In **Allow unsolicited incoming messages from**, type * to specify traffic originating from any source IPv4 address or a comma-separated list of sources. The sources can be **LocalSubnet** to specify traffic originating from a directly reachable IPv4 address or one or more IPv4 addresses or IPv4 address ranges separated by commas. IPv4 address ranges typically correspond to subnets. For IPv4 addresses, type the IPv4 address in dotted decimal notation. For IPv4 address ranges, you can specify the range using a dotted decimal subnet mask or a prefix length. When you use a dotted decimal subnet mask, you can specify the range as an IPv4 network ID (such as 10.47.81.0/255.255.255.0) or by using an IPv4 address within the range (such as 10.47.81.231/255.255.255.0). When you use a network prefix length, you can specify the range as an

IPv4 network ID (such as 10.47.81.0/24) or by using an IPv4 address within the range (such as 10.47.81.231/24). The following is an example list of sources:

Local Subnet, 10. 91. 12. 56, 10. 7. 14. 9/255. 255. 255. 0, 10. 116. 45. 0/255. 255. 255. 0, 172. 16. 31. 11/24, 172. 16. 111. 0/24

IPv6 traffic supports the * and **LocalSubnet** scopes.

Note If you have any spaces between the entries in the list of sources or any other invalid characters, the scope is ignored and the setting behaves as if it were disabled. Please double-check your scope syntax before saving changes.

Host names, DNS names, or DNS suffixes are not supported.

- Disabled

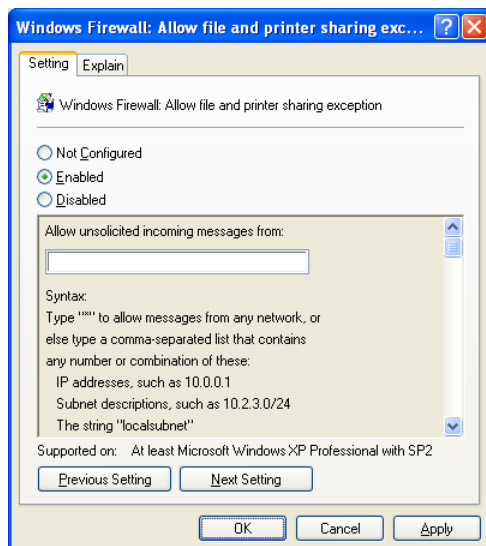
Remote administration is not allowed. Windows Firewall blocks port 135 and does not open 445. Also, in effect, it adds SVCHOST.EXE and LSASS.EXE to the program exceptions list with the Status of Disabled. Because disabling this policy setting does not block TCP port 445, it does not conflict with the **Windows Firewall: Allow file and printer sharing exception** setting. This does not prevent these programs from running or their corresponding ports from being opened.

Malicious users and programs often attempt to attack networks and computers using RPC and DCOM traffic. We recommend that you contact the manufacturers of your critical programs to determine if they require RPC and DCOM communication. If they do not, then do not enable this setting.

Note If you only want to open a subset of the ports that this setting opens, leave this setting set to Not Configured and use the **Windows Firewall: Define port exceptions** setting to selectively open ports.

Windows Firewall: Allow File and Print Sharing Exception

The **Windows Firewall: Allow file and printer sharing exception** setting specifies whether the ports for file and printer sharing are open, and is shown in the following figure.



You can select the following:

- Not Configured (default)

The ports for file and printer sharing are not opened. The shared files and printers on the computer will not be available from other computers. However, local administrators can configure the pre-defined File and Printer Sharing exception, such as from the **Exceptions** tab of the Windows Firewall component in Control Panel.

- Enabled

The following ports for file and printer sharing are opened:

- UDP 137
- UDP 138
- TCP 139
- TCP 445

When you enable the pre-defined File and Printer Sharing exception, Windows Firewall also allows incoming ICMP Echo messages.

In **Allow unsolicited incoming messages from**, type * to specify file and printer sharing traffic originating from any source IPv4 address or a comma-separated list of sources. The sources can be **LocalSubnet** to specify traffic originating from a directly reachable IPv4 address or one or more IPv4 addresses or IPv4 address ranges separated by commas. IPv4 address ranges typically correspond to subnets. For IPv4 addresses, type the IPv4 address in dotted decimal notation. For IPv4 address ranges, you can specify the range using a dotted decimal subnet mask or a prefix length. When you use a dotted decimal subnet mask, you can specify the range as an IPv4 network ID (such as 10.47.81.0/255.255.255.0) or by using an IPv4 address within the range (such as 10.47.81.231/255.255.255.0). When you use a network prefix length, you can specify the range as an IPv4 network ID (such as 10.47.81.0/24) or by using an IPv4 address within the range (such as 10.47.81.231/24). The following is an example list of sources:

Local Subnet, 10. 91. 12. 56, 10. 7. 14. 9/255. 255. 255. 0, 10. 116. 45. 0/255. 255. 255. 0, 172. 16. 31. 11/24, 172. 16. 111. 0/24

IPv6 traffic supports the * and **LocalSubnet** scopes.

Note If you have any spaces between the entries in the list of sources or any other invalid characters, the scope is ignored and the setting behaves as if it were disabled. Please double-check your scope syntax before saving changes.

Host names, DNS names, or DNS suffixes are not supported.

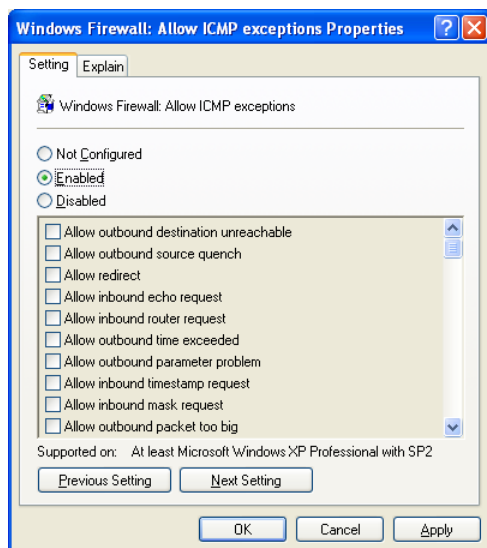
- Disabled

The ports for file and printer sharing are not opened and local administrators cannot configure the pre-defined File and Printer Sharing exception. The shared files and printers on the computer will not be available from other computers. Selecting Disabled does not prevent these ports from being used by other applications.

Note If you only want to open a subset of the ports that this setting opens, leave this setting set to Not Configured and use the **Windows Firewall: Define port exceptions** setting to selectively open ports.

Windows Firewall: Allow ICMP Exceptions

The **Windows Firewall: Allow ICMP exceptions** setting allows you to configure specific types of ICMP messages as excepted traffic, and is shown in the following figure.



You can select the following:

- Not Configured (default)

Local administrators can define ICMP exceptions, such as from the **Advanced** tab of the Windows Firewall component in Control Panel.

- Enabled

The specified unsolicited incoming ICMP traffic is allowed. When you select Enabled, you must also specify the specific types of ICMP messages that are allowed. Selecting Enabled overrides the local ICMP settings of Windows Firewall.

- Disabled

No unsolicited incoming ICMP traffic is allowed. Local administrators cannot define ICMP exceptions.

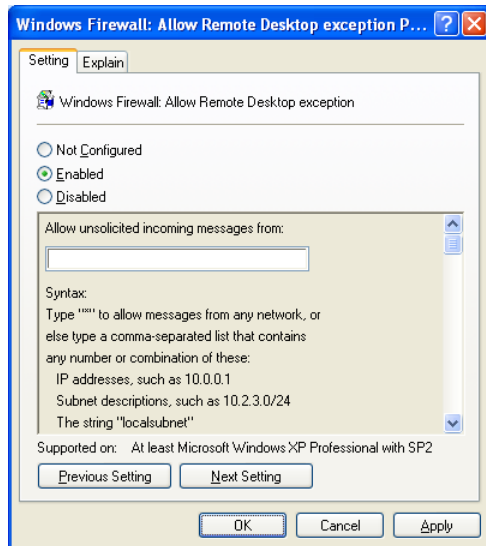
If you do not enable this setting and select **Allow inbound echo request**, tools that use the ICMP Echo message (also known as the ICMP Echo Request message) such as Ping or Tracert will not work. If you are running network management software uses ICMP Destination Unreachable messages, also select **Allow outbound destination unreachable**.

If any policy setting opens TCP port 445, Windows Firewall automatically allows incoming ICMP Echo messages, even if the **Windows Firewall: Allow ICMP exceptions** setting is disabled. Policy settings that can open TCP port 445 include **Windows Firewall: Allow file and printer sharing exception**, **Windows Firewall: Allow remote administration exception**, and **Windows Firewall: Define port exceptions**.

Other Windows Firewall policy settings affect only incoming messages, but several of the options of the **Windows Firewall: Allow ICMP exceptions** setting affect outgoing communication.

Windows Firewall: Allow Remote Desktop Exception

The **Windows Firewall: Allow Remote Desktop exception** setting allows you to specify whether Remote Desktop connections are allowed, and is shown in the following figure.



You can select the following:

- Not Configured (default)

Remote Desktop connections are not allowed. However, local administrators can configure the pre-defined Remote Desktop exception, such as from the **Exceptions** tab of the Windows Firewall component in Control Panel.

- Enabled

Remote Desktop connections are allowed. TCP port 3389 is opened.

In **Allow unsolicited incoming messages from**, type * to specify Remote Desktop traffic originating from any source IPv4 address or a comma separated list of sources. The sources can be **LocalSubnet** to specify traffic originating from a directly reachable IPv4 address or one or more IPv4 addresses or IPv4 address ranges separated by commas. IPv4 address ranges typically correspond to subnets. For IPv4 addresses, type the IPv4 address in dotted decimal notation. For IPv4 address ranges, you can specify the range using a dotted decimal subnet mask or a prefix length. When you use a dotted decimal subnet mask, you can specify the range as an IPv4 network ID (such as 10.47.81.0/255.255.255.0) or by using an IPv4 address within the range (such as 10.47.81.231/255.255.255.0). When you use a network prefix length, you can specify the range as an IPv4 network ID (such as 10.47.81.0/24) or by using an IPv4 address within the range (such as 10.47.81.231/24). The following is an example list of sources:

LocalSubnet, 10. 91. 12. 56, 10. 7. 14. 9/255. 255. 255. 0, 10. 116. 45. 0/255. 255. 255. 0, 172. 16. 31. 11/24, 172. 16. 111. 0/24

IPv6 traffic supports the * and **LocalSubnet** scopes.

Note If you have any spaces between the entries in the list of sources or any other invalid characters, the scope is ignored and the setting behaves as if it were disabled. Please double-check your scope syntax before saving changes.

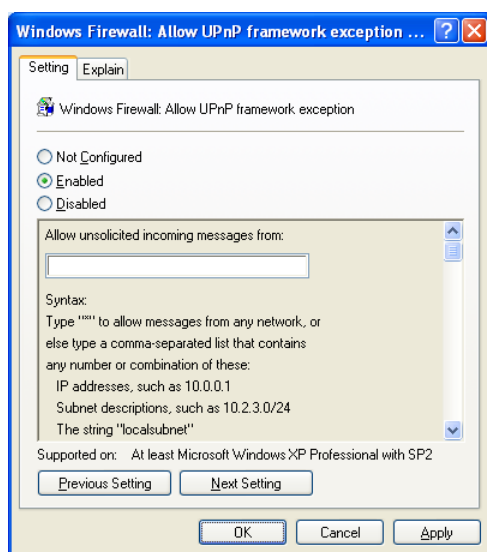
Host names, DNS names, or DNS suffixes are not supported.

- Disabled

Remote Desktop connections are not allowed. Local administrators cannot configure the pre-defined Remote Desktop exception.

Windows Firewall: Allow UPnP Framework Exception

The **Windows Firewall: Allow UPnP framework exception** setting specifies whether the ports for UPnP traffic are open, and is shown in the following figure.



You can select the following:

- Not Configured (default)

The ports for UPnP traffic are not opened, which prevents the computer from receiving UPnP messages. However, local administrators can configure the pre-defined UPnP Framework exception, such as from the **Exceptions** tab of the Windows Firewall component in Control Panel.

- Enabled

The following ports for UPnP traffic are opened:

- UDP 1900
- TCP 2869

In **Allow unsolicited incoming messages from**, type * to specify UPnP traffic originating from any source IPv4 address or a comma separated list of sources. The sources can be **LocalSubnet** to specify traffic originating from a directly reachable IPv4 address or one or more IPv4 addresses or IPv4 address ranges separated by commas. IPv4 address ranges typically correspond to subnets. For IPv4 addresses, type the IPv4 address in dotted decimal notation. For IPv4 address ranges, you can specify

the range using a dotted decimal subnet mask or a prefix length. When you use a dotted decimal subnet mask, you can specify the range as an IPv4 network ID (such as 10.47.81.0/255.255.255.0) or by using an IPv4 address within the range (such as 10.47.81.231/255.255.255.0). When you use a network prefix length, you can specify the range as an IPv4 network ID (such as 10.47.81.0/24) or by using an IPv4 address within the range (such as 10.47.81.231/24). The following is an example list of sources:

Local Subnet, 10. 91. 12. 56, 10. 7. 14. 9/255. 255. 255. 0, 10. 116. 45. 0/255. 255. 255. 0, 172. 16. 31. 11/24, 172. 16. 111. 0/24

IPv6 traffic supports the * and **LocalSubnet** scopes.

Note If you have any spaces between the entries in the list of sources or any other invalid characters, the scope is ignored and the setting behaves as if it were disabled. Please double-check your scope syntax before saving changes.

Host names, DNS names, or DNS suffixes are not supported.

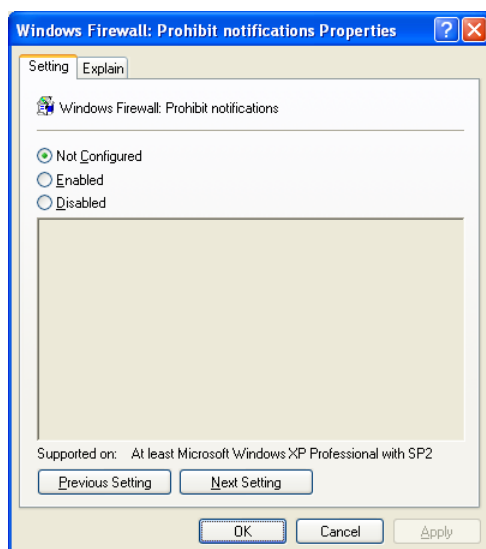
- Disabled

The ports for UPnP traffic are not opened, which prevents the computer from receiving unsolicited incoming UPnP messages. Local administrators cannot configure the pre-defined UPnP Framework exception.

Note If you only want to open a subset of the ports that this setting opens, leave this setting set to Not Configured and use the **Windows Firewall: Define port exceptions** setting to selectively open ports.

Windows Firewall: Prohibit Notifications

The **Windows Firewall: Prohibit notifications** setting specifies whether the Windows Firewall displays notification messages when applications listen on a port, and is shown in the following figure.



You can select the following:

- Not Configured (default)

The notification messages are displayed. However, local administrators can configure notification behavior, such as the **Notify when Windows Firewall blocks a program** option from the **Exceptions** tab of the Windows Firewall component in Control Panel.

- Enabled

The notification messages are not displayed.

- Disabled

The notification messages are displayed. Local administrators cannot configure notification behavior.

When most applications request an open port, Windows Firewall adds the program to the program exceptions list with the default status value of Disabled. If you enable this policy setting, notifications are not displayed and the status value for the program exception remains Disabled until manually changed.

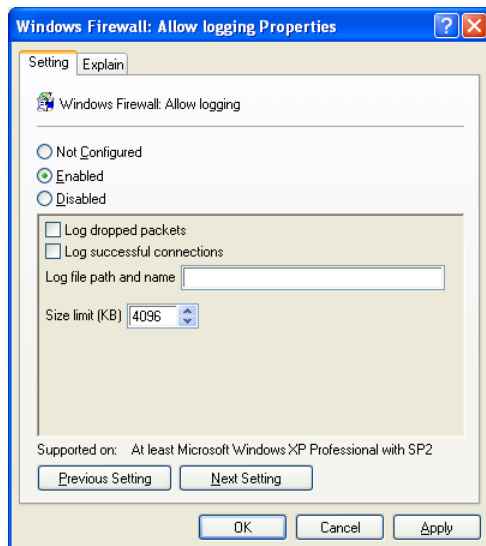
If you disable or do not configure this policy setting, Windows Firewall displays notification messages.

If the user is not a local administrator, the message informs them that they might need to contact a network administrator, which can alert the network administrator about possible malicious programs on the network.

If the user is a local administrator, and either you have enabled the **Windows Firewall: Allow local program exceptions** setting or you have not configured the **Windows Firewall: Define program exceptions** setting, then the notification message allows the user to specify whether to enable the application. If you disable the **Windows Firewall: Define program exceptions** setting, then the user will not be notified unless enabled locally.

Windows Firewall: Allow Logging

The **Windows Firewall: Allow logging** setting specifies whether the Windows Firewall logs activity information to a log file, and is shown in the following figure.



You can select the following:

- Not Configured (default)

Logging is not enabled.

- Enabled

Logging is enabled with the specified log file settings.

- Not Configured (default)

Logging is not enabled. Local administrators cannot enable logging, such as from the **Advanced** tab of the Windows Firewall component in Control Panel.

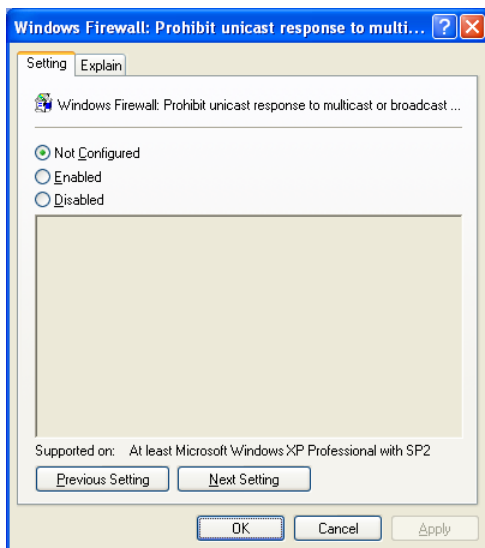
If enabled, you must provide the name, location, and maximum size of the log file (up to a maximum size of 32767 KB). When the log file becomes full, it is archived and a new file is created. The location can contain environment variables, such as %SystemRoot%. You can also separately specify whether you want to log the following:

- Dropped packets, which correspond to incoming unsolicited traffic that was not excepted.
- Successful connections, which correspond to successful incoming and outgoing connections.

There is no option to log incoming packets (solicited or unsolicited) that were not dropped.

Windows Firewall: Prohibit Unicast Response to Multicast or Broadcast Requests

The **Windows Firewall: Prohibit unicast response to multicast or broadcast requests** setting specifies whether unicast response message received in response to a multicast or broadcast message that was sent by the computer is dropped, and is shown in the following figure.



You can select the following:

- Not Configured (default) or Disabled

The received unicast response is accepted (not dropped) if received within 3 seconds. The difference between the Not Configured and Disabled settings is based on Group Policy inheritance rules.

- Enabled

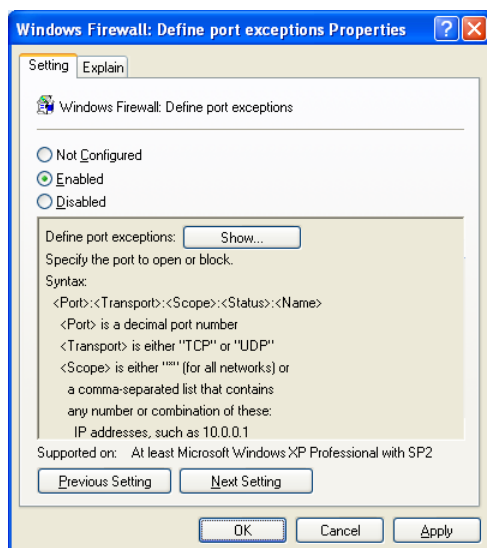
The unicast response to a multicast or broadcast packet sent by the computer is dropped.

This setting has no effect if the unicast message is a response to a DHCP broadcast message sent by the computer. Windows Firewall always permits DHCP unicast responses. However, this policy setting can interfere with the unique NetBIOS name conflict detection process, in which a broadcast-based NetBIOS message is sent to register a NetBIOS unique name. If another computer on the network is using that same

name, there is a name conflict and the current name owner sends a unicast NetBIOS Negative Name Registration Reply message. If the Windows Firewall drops this message, then the computer continues to use the duplicate name. If the computers are using Windows Internet Name Service (WINS), then the duplicate name is detected via the WINS server.

Windows Firewall: Define Port Exceptions

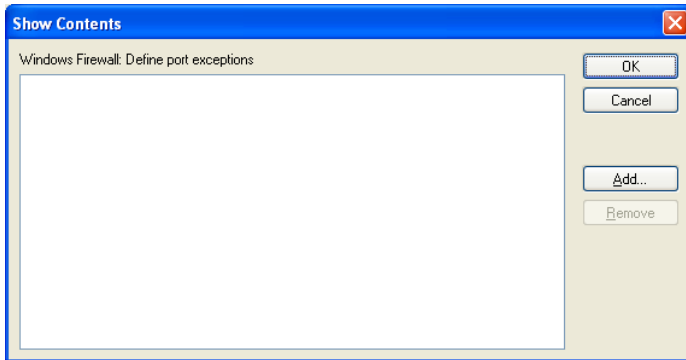
The **Windows Firewall: Define port exceptions** setting allows you to specify excepted traffic in terms of TCP and UDP ports, and is shown in the following figure.



You can select the following:

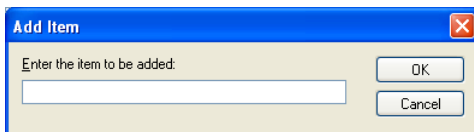
- **Not Configured** (default)
No excepted traffic is configured. Local administrators can specify open ports locally, such as from the **Exceptions** tab of the Windows Firewall component in Control Panel.
- **Enabled**
The configured ports are excepted traffic. Locally configured port exceptions are ignored, including settings pre-defined through setup files, as described in Appendix E and Appendix F.
- **Disabled**
No excepted traffic is configured. Local administrators cannot specify open ports locally, unless the **Windows Firewall: Allow local port exceptions** setting is set to Enabled.

To define the list of open ports, click **Enabled**, and then click **Show**. The **Show Contents** dialog box is displayed, as shown in the following figure.



From **Show Contents**, you can add or remove an open port. You cannot edit an existing open port. To change an open port, remove it, and then add it with the correct parameters.

To add a new open port, click **Add**. An example is shown in the following figure.



In **Add Item**, type the parameters for an open port using the following syntax:

Port#:TCP|UDP:Scope:Enabled|Disabled:PortName

- *Port#*

Type the port number for the TCP or UDP Port.

- **TCP|UDP**

This is the Port Type parameter. Type **TCP** to specify a TCP port. Type **UDP** to specify a UDP port.

- *Scope*

The *Scope* parameter specifies the addresses from which the traffic is allowed. Type * to specify traffic originating from any source IPv4 address or a comma separated list of sources. The sources can be **LocalSubnet** to specify traffic originating from a directly reachable IPv4 address or one or more IPv4 addresses or IPv4 address ranges separated by commas. IPv4 address ranges typically correspond to subnets. For IPv4 addresses, type the IPv4 address in dotted decimal notation. For IPv4 address ranges, you can specify the range using a dotted decimal subnet mask or a prefix length. When you use a dotted decimal subnet mask, you can specify the range as an IPv4 network ID (such as 10.47.81.0/255.255.255.0) or by using an IPv4 address within the range (such as 10.47.81.231/255.255.255.0). When you use a network prefix length, you can specify the range as an IPv4 network ID (such as 10.47.81.0/24) or by using an IPv4 address within the range (such as 10.47.81.231/24). The following is an example list of sources:

Local Subnet, 10. 91. 12. 56, 10. 7. 14. 9/255. 255. 255. 0, 10. 116. 45. 0/255. 255. 255. 0, 172. 16. 31. 11/24, 172. 16. 111. 0/24

IPv6 traffic supports the * and **LocalSubnet** scopes.

Notes If you have any spaces between the entries in the list of sources or any other invalid characters, the scope is ignored and the setting behaves as if it were disabled. Please double-check your scope syntax before saving changes.

Host names, DNS names, or DNS suffixes are not supported.

- **Enabled|Disabled**

This is the Status parameter. Type **Enabled** to allow incoming unsolicited traffic to this port. Type **Disabled** to prevent the port from being allowed in the exceptions list.

- *PortName*

Type a friendly name for the traffic or program that uses the port. This becomes the name of the port in the list of open ports in the Windows Firewall settings of the computers running Windows XP with SP2.

The following is an example of a valid port entry:

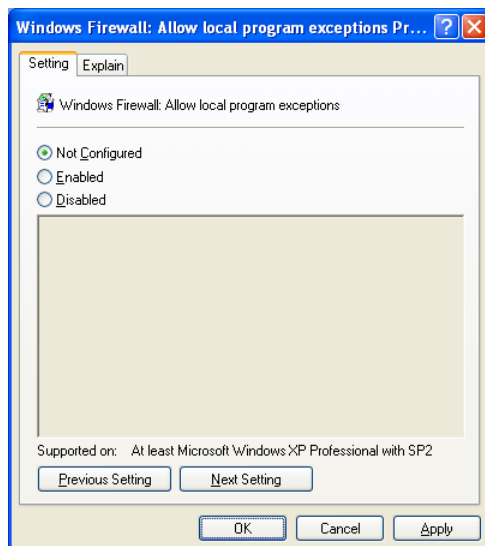
```
23:TCP:*.Enabled:Telnet
```

Note You can add the same application multiple times to the Open Ports list. An entry to enable an open port takes precedence over an entry to disable it.

For resources that describe what applications or protocols use which ports, see Appendix G.

Windows Firewall: Allow Local Port Exceptions

The **Windows Firewall: Allow local port exceptions** setting allows you to specify whether local administrators are allowed to configure their own port exceptions, and is shown in the following figure.



You can select the following:

- Not Configured (default)

Local administrators cannot add port exceptions setting unless the **Windows Firewall: Define port exceptions** setting is set to Not Configured. If the **Windows Firewall: Define port exceptions** setting is set to Enabled or Disabled, local administrators cannot define a local port exceptions list.

- Enabled
Local administrators can add port exceptions.
- Disabled
Local administrators cannot add port exceptions.

Appendix B: Netsh Command Syntax for the Netsh Firewall Context

The following Netsh commands can be used in scripts or at the command line to configure Windows Firewall for IPv4 and IPv6 traffic when executed from the **netsh firewall** context:

- add allowedprogram
- set allowedprogram
- delete allowedprogram
- set icmpsetting
- set multicastbroadcastresponse
- set notifications
- set logging
- set opmode
- add portopening
- set portopening
- delete portopening
- set service
- show commands
- reset

The following sections describe each command and its syntax.

add allowedprogram

Used to add a program-based exception.

Syntax:

```
add allowedprogram
```

```
[ program = ] path
[ name = ] name
[ [ mode = ] ENABLE|DI SABLE
  [ scope = ] ALL|SUBNET|CUSTOM
  [ addresses = ] addresses
  [ profile = ] CURRENT|DOMAIN|STANDARD|ALL ]
```

Adds firewall allowed program configuration.

Parameters:

program - Program path and file name.

name - Program name.

mode - Program mode (optional).

ENABLE - Allow through firewall (default).

DISABLE - Do not allow through firewall.

scope - Program scope (optional).

ALL - Allow all traffic through firewall (default).

SUBNET - Allow only local network (subnet) traffic through firewall.
 CUSTOM - Allow only specified traffic through firewall.

addresses - Custom scope addresses (optional).

profile - Configuration profile (optional).

CURRENT - Current profile (default).
 DOMAIN - Domain profile.
 STANDARD - Standard profile.
 ALL - All profiles.

Remarks: 'scope' must be 'CUSTOM' to specify 'addresses'.

Examples:

```
add allowedprogram C:\MyApp\MyApp.exe MyApp ENABLE
add allowedprogram C:\MyApp\MyApp.exe MyApp DISABLE
add allowedprogram C:\MyApp\MyApp.exe MyApp ENABLE CUSTOM
    157.60.0.1, 172.16.0.0/16, 10.0.0.0/255.0.0.0, Local Subnet
add allowedprogram program = C:\MyApp\MyApp.exe name = MyApp mode = ENABLE
add allowedprogram program = C:\MyApp\MyApp.exe name = MyApp mode = DISABLE
add allowedprogram program = C:\MyApp\MyApp.exe name = MyApp mode = ENABLE
    scope = CUSTOM 157.60.0.1, 172.16.0.0/16, 10.0.0.0/255.0.0.0, Local Subnet
```

set allowedprogram

Used to modify the settings of an existing program-based exception.

Syntax:

set allowedprogram

```
[ program = ] path
[ [ name = ] name
  [ mode = ] ENABLE|DISABLE
  [ scope = ] ALL|SUBNET|CUSTOM
  [ addresses = ] addresses
  [ profile = ] CURRENT|DOMAIN|STANDARD|ALL ]
```

Sets firewall allowed program configuration.

Parameters:

program - Program path and file name.

name - Program name (optional).

mode - Program mode (optional).

ENABLE - Allow through firewall (default).
 DISABLE - Do not allow through firewall.

scope - Program scope (optional).

ALL - Allow all traffic through firewall (default).
 SUBNET - Allow only local network (subnet) traffic through firewall.
 CUSTOM - Allow only specified traffic through firewall.

addresses - Custom scope addresses (optional).

profile - Configuration profile (optional).

CURRENT - Current profile (default).
 DOMAIN - Domain profile.
 STANDARD - Standard profile.
 ALL - All profiles.

Remarks: 'scope' must be 'CUSTOM' to specify 'addresses'.

Examples:

```

set allowedprogram C:\MyApp\MyApp.exe MyApp ENABLE
set allowedprogram C:\MyApp\MyApp.exe MyApp DISABLE
set allowedprogram C:\MyApp\MyApp.exe MyApp ENABLE CUSTOM
    157.60.0.1, 172.16.0.0/16, 10.0.0.0/255.0.0.0, Local Subnet
set allowedprogram program = C:\MyApp\MyApp.exe name = MyApp mode = ENABLE
set allowedprogram program = C:\MyApp\MyApp.exe name = MyApp mode = DISABLE
set allowedprogram program = C:\MyApp\MyApp.exe name = MyApp mode = ENABLE
    scope = CUSTOM 157.60.0.1, 172.16.0.0/16, 10.0.0.0/255.0.0.0, Local Subnet

```

delete allowedprogram

Used to delete an existing program-based exception.

Syntax:

```
delete allowedprogram
```

```

[ program = ] path
[ [ profile = ] CURRENT|DOMAIN|STANDARD|ALL ]

```

Deletes firewall allowed program configuration.

Parameters:

program - Program path and file name.

profile - Configuration profile (optional).

- CURRENT - Current profile (default).
- DOMAIN - Domain profile.
- STANDARD - Standard profile.
- ALL - All profiles.

Examples:

```

delete allowedprogram C:\MyApp\MyApp.exe
delete allowedprogram program = C:\MyApp\MyApp.exe

```

set icmpsetting

Used to specify excepted ICMP traffic.

Syntax:

```
set icmpsetting
```

```

[ type = ] 2-5|8-9|11-13|17|ALL
[ [ mode = ] ENABLE|DISABLE
  [ profile = ] CURRENT|DOMAIN|STANDARD|ALL
  [ interface = ] name ]

```

Sets firewall ICMP configuration.

Parameters:

type - ICMP type.

- 2 - Allow outbound packet too big.
- 3 - Allow outbound destination unreachable.
- 4 - Allow outbound source quench.
- 5 - Allow redirect.
- 8 - Allow inbound echo request.
- 9 - Allow inbound router request.
- 11 - Allow outbound time exceeded.

12 - Allow outbound parameter problem.
 13 - Allow inbound timestamp request.
 17 - Allow inbound mask request.
 ALL - All types.

mode - ICMP mode (optional).
 ENABLE - Allow through firewall (default).
 DISABLE - Do not allow through firewall.

profile - Configuration profile (optional).
 CURRENT - Current profile (default).
 DOMAIN - Domain profile.
 STANDARD - Standard profile.
 ALL - All profiles.

interface - Interface name (optional).

Remarks: 'profile' and 'interface' may not be specified together.
 'type' 2 and 'interface' may not be specified together.

Examples:

```
set icmpsetting 8
set icmpsetting 8 ENABLE
set icmpsetting ALL DISABLE
set icmpsetting type = 8
set icmpsetting type = 8 mode = ENABLE
set icmpsetting type = ALL mode = DISABLE
```

set multicastbroadcastresponse

Used to specify the unicast response to a multicast or broadcast request behavior.

Syntax:

```
set multicastbroadcastresponse
```

```
[ mode = ] ENABLE|DISABLE
[ [ profile = ] CURRENT|DOMAIN|STANDARD|ALL ]
```

Sets firewall multicast/broadcast response configuration.

Parameters:

mode - Multicast/broadcast response mode.
 ENABLE - Allow responses to multicast/broadcast traffic through the firewall.
 DISABLE - Do not allow responses to multicast/broadcast traffic through the firewall.

profile - Configuration profile (optional).
 CURRENT - Current profile (default).
 DOMAIN - Domain profile.
 STANDARD - Standard profile.
 ALL - All profiles.

Examples:

```
set multicastbroadcastresponse ENABLE
set multicastbroadcastresponse DISABLE
set multicastbroadcastresponse mode = ENABLE
set multicastbroadcastresponse mode = DISABLE
```

set notifications

Used to specify the notification behavior.

Syntax:

```
set notifications
```

```
[ mode = ] ENABLE|DISABLE
[ [ profile = ] CURRENT|DOMAIN|STANDARD|ALL ]
```

Sets firewall notification configuration.

Parameters:

mode - Notification mode.

ENABLE - Allow pop-up notifications from firewall.

DISABLE - Do not allow pop-up notifications from firewall.

profile - Configuration profile (optional).

CURRENT - Current profile (default).

DOMAIN - Domain profile.

STANDARD - Standard profile.

ALL - All profiles.

Examples:

```
set notifications ENABLE
```

```
set notifications DISABLE
```

```
set notifications mode = ENABLE
```

```
set notifications mode = DISABLE
```

set logging

Used to specify logging options.

Syntax:

```
set logging
```

```
[ [ filelocation = ] path
  [ maxfilesize = ] 1-32767
  [ droppedpackets = ] ENABLE|DISABLE
  [ connections = ] ENABLE|DISABLE ]
```

Sets firewall logging configuration.

Parameters:

filelocation - Log path and file name (optional).

maxfilesize - Maximum log file size in kilobytes (optional).

droppedpackets - Dropped packet log mode (optional).

ENABLE - Log in firewall.

DISABLE - Do not log in firewall.

connections - Successful connection log mode (optional).

ENABLE - Log in firewall.

DISABLE - Do not log in firewall.

Remarks: At least one parameter must be specified.

Examples:

```
set logging %windir%\pfirewall.log 4096
```

```
set logging %windir%\pfirewall.log 4096 ENABLE
```

```
set logging filelocation = %windir%\pfirewall.log maxfilesize = 4096
set logging filelocation = %windir%\pfirewall.log maxfilesize = 4096
droppedpackets = ENABLE
```

set opmode

Used to specify the operating mode of Windows Firewall either globally or for a specific connection (interface).

Syntax:

```
set opmode
  [ mode = ] ENABLE|DISABLE
  [ [ exceptions = ] ENABLE|DISABLE
    [ profile = ] CURRENT|DOMAIN|STANDARD|ALL
    [ interface = ] name ]
```

Sets firewall operational configuration.

Parameters:

mode - Operational mode.

ENABLE - Enable firewall.
DISABLE - Disable firewall.

exceptions - Exception mode (optional).

ENABLE - Allow through firewall (default).
DISABLE - Do not allow through firewall.

profile - Configuration profile (optional).

CURRENT - Current profile (default).
DOMAIN - Domain profile.
STANDARD - Standard profile.
ALL - All profiles.

interface - Interface name (optional).

Remarks: 'profile' and 'interface' may not be specified together.
'exceptions' and 'interface' may not be specified together.

Examples:

```
set opmode ENABLE
set opmode ENABLE DISABLE
set opmode mode = ENABLE
set opmode mode = ENABLE exceptions = DISABLE
```

add portopening

Used to create a port-based exception.

Syntax:

```
add portopening
  [ protocol = ] TCP|UDP|ALL
  [ port = ] 1-65535
  [ name = ] name
  [ [ mode = ] ENABLE|DISABLE
    [ scope = ] ALL|SUBNET|CUSTOM
    [ addresses = ] addresses
    [ profile = ] CURRENT|DOMAIN|STANDARD|ALL
    [ interface = ] name ]
```

Adds firewall port configuration.

Parameters:

protocol - Port protocol.

TCP - Transmission Control Protocol (TCP).
 UDP - User Datagram Protocol (UDP).
 ALL - All protocols.

port - Port number.

name - Port name.

mode - Port mode (optional).
 ENABLE - Allow through firewall (default).
 DISABLE - Do not allow through firewall.

scope - Port scope (optional).
 ALL - Allow all traffic through firewall (default).
 SUBNET - Allow only local network (subnet) traffic through firewall.
 CUSTOM - Allow only specified traffic through firewall.

addresses - Custom scope addresses (optional).

profile - Configuration profile (optional).
 CURRENT - Current profile (default).
 DOMAIN - Domain profile.
 STANDARD - Standard profile.
 ALL - All profiles.

interface - Interface name (optional).

Remarks: 'profile' and 'interface' may not be specified together.
 'scope' and 'interface' may not be specified together.
 'scope' must be 'CUSTOM' to specify 'addresses'.

Examples:

```
add portopening TCP 80 MyWebPort
add portopening UDP 500 IKE ENABLE ALL
add portopening ALL 53 DNS ENABLE CUSTOM
    157. 60. 0. 1, 172. 16. 0. 0/16, 10. 0. 0. 0/255. 0. 0. 0, Local Subnet
add portopening protocol = TCP port = 80 name = MyWebPort
add portopening protocol = UDP port = 500 name = IKE mode = ENABLE scope = ALL
add portopening protocol = ALL port = 53 name = DNS mode = ENABLE
    scope = CUSTOM addresses =
    157. 60. 0. 1, 172. 16. 0. 0/16, 10. 0. 0. 0/255. 0. 0. 0, Local Subnet
```

set portopening

Used to modify the settings of an existing port-based exception.

Syntax:

```
set portopening
  [ protocol = ] TCP|UDP|ALL
  [ port = ] 1-65535
  [ [ name = ] name
  [ mode = ] ENABLE|DISABLE
  [ scope = ] ALL|SUBNET|CUSTOM
  [ addresses = ] addresses
  [ profile = ] CURRENT|DOMAIN|STANDARD|ALL
  [ interface = ] name ]
```

Sets firewall port configuration.

Parameters:

protocol - Port protocol.
 TCP - Transmission Control Protocol (TCP).
 UDP - User Datagram Protocol (UDP).

ALL - All protocols.

port - Port number.

name - Port name (optional).

mode - Port mode (optional).

ENABLE - Allow through firewall (default).

DISABLE - Do not allow through firewall.

scope - Port scope (optional).

ALL - Allow all traffic through firewall (default).

SUBNET - Allow only local network (subnet) traffic through firewall.

CUSTOM - Allow only specified traffic through firewall.

addresses - Custom scope addresses (optional).

profile - Configuration profile (optional).

CURRENT - Current profile (default).

DOMAIN - Domain profile.

STANDARD - Standard profile.

ALL - All profiles.

interface - Interface name (optional).

Remarks: 'profile' and 'interface' may not be specified together.

'scope' and 'interface' may not be specified together.

'scope' must be 'CUSTOM' to specify 'addresses'.

Examples:

```
set portopening TCP 80 MyWebPort
```

```
set portopening UDP 500 IKE ENABLE ALL
```

```
set portopening ALL 53 DNS ENABLE CUSTOM
```

```
157. 60. 0. 1, 172. 16. 0. 0/16, 10. 0. 0. 0/255. 0. 0. 0, Local Subnet
```

```
set portopening protocol = TCP port = 80 name = MyWebPort
```

```
set portopening protocol = UDP port = 500 name = IKE mode = ENABLE scope = ALL
```

```
set portopening protocol = ALL port = 53 name = DNS mode = ENABLE
```

```
scope = CUSTOM addresses =
```

```
157. 60. 0. 1, 172. 16. 0. 0/16, 10. 0. 0. 0/255. 0. 0. 0, Local Subnet
```

delete portopening

Used to delete an existing port-based exception.

Syntax:

```
delete portopening
```

```
[ protocol = ] TCP|UDP|ALL
```

```
[ port = ] 1-65535
```

```
[ [ profile = ] CURRENT|DOMAIN|STANDARD|ALL
```

```
[ interface = ] name ]
```

Deletes firewall port configuration.

Parameters:

protocol - Port protocol.

TCP - Transmission Control Protocol (TCP).

UDP - User Datagram Protocol (UDP).

ALL - All protocols.

port - Port number.

profile - Configuration profile (optional).

CURRENT - Current profile (default).
 DOMAIN - Domain profile.
 STANDARD - Standard profile.
 ALL - All profiles.

interface - Interface name (optional).

Remarks: 'profile' and 'interface' may not be specified together.

Examples:

```
delete portopening TCP 80
delete portopening UDP 500
delete portopening protocol = TCP port = 80
delete portopening protocol = UDP port = 500
```

set service

Used to enable or disable the pre-defined file and printer sharing, remote administration, remote desktop, and UPnP exceptions.

Syntax:

set service

```
[ type = ] FILEANDPRINT|REMOTEDADMIN|REMOTEDESKTOP|UPNP|ALL
[ [ mode = ] ENABLE|DISABLE
  [ scope = ] ALL|SUBNET|CUSTOM
  [ addresses = ] addresses
  [ profile = ] CURRENT|DOMAIN|STANDARD|ALL ]
```

Sets firewall service configuration.

Parameters:

type - Service type.

FILEANDPRINT - File and printer sharing.
 REMOTEDADMIN - Remote administration.
 REMOTEDESKTOP - Remote assistance and remote desktop.
 UPNP - UPnP framework.
 ALL - All types.

mode - Service mode (optional).

ENABLE - Allow through firewall (default).
 DISABLE - Do not allow through firewall.

scope - Service scope (optional).

ALL - Allow all traffic through firewall (default).
 SUBNET - Allow only local network (subnet) traffic through firewall.
 CUSTOM - Allow only specified traffic through firewall.

addresses - Custom scope addresses (optional).

profile - Configuration profile (optional).

CURRENT - Current profile (default).
 DOMAIN - Domain profile.
 STANDARD - Standard profile.
 ALL - All profiles.

Remarks: 'scope' ignored if 'mode' is DISABLE.
 'scope' must be 'CUSTOM' to specify 'addresses'.

Examples:

```
set service FILEANDPRINT
set service REMOTEDADMIN ENABLE SUBNET
```

```
set service REMOTEDESKTOP ENABLE CUSTOM
    157.60.0.1, 172.16.0.0/16, 10.0.0.0/255.0.0.0, Local Subnet

set service type = FILEANDPRINT

set service type = REMOTEADMIN mode = ENABLE scope = SUBNET

set service type = REMOTEDESKTOP mode = ENABLE scope = CUSTOM
    addresses = 157.60.0.1, 172.16.0.0/16, 10.0.0.0/255.0.0.0, Local Subnet
```

show commands

The following show commands are used to display the current configuration:

- **show allowedprogram** Displays the excepted programs.
- **show config** Displays the local configuration information.
- **show currentprofile** Displays the current profile.
- **show icmpsetting** Displays the ICMP settings.
- **show logging** Displays the logging settings.
- **show multicastbroadcastresponse** Displays multicast/broadcast response settings.
- **show notifications** Displays the current settings for notifications.
- **show opmode** Displays the operational mode.
- **show portopening** Displays the excepted ports.
- **show service** Displays the services.
- **show state** Displays the current state information.

For additional information about the **show config** and **show state** commands, see [Troubleshooting Internet Connection Firewall on Microsoft Windows XP](#).

reset

Used to reset the configuration of Windows Firewall to default settings. There are no command line options for the **reset** command.

Appendix C: Deploying Windows Firewall Settings in a Windows NT 4.0 Domain

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 computers running Windows XP that are members of a Windows NT 4.0 domain, 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 a Windows NT 4.0 domain controller.

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](http://www.microsoft.com/downloads/details.aspx?FamilyID=d67c7085-4bff-4056-8e7e-3d583214e728&DisplayLang=en) 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**.
7. If you have an existing System Policy file, click **File**, and then click **Open Policy**. In the **Open Policy File** dialog box, select the **Ntconfig.pol** file that is currently being used as your System Policy file.
If you do not have an existing System Policy file, click **File**, and then click **New Policy**.
8. From the **System Policy Editor**, double-click **Default Computer**.
9. In the **Default Computer Properties** dialog box, open **Windows Firewall** and configure the appropriate Windows Firewall settings.
10. Click **OK**.
11. If you have an existing System Policy file, click **File** and then click **Save**.
If you did not have an existing System Policy file, click **File**, click **Save As**, and then save the file with the name Ntconfig.pol.
12. Distribute the modified or new Ntconfig.pol file to the Netlogon shares of all of your Windows NT 4.0 domain controllers.

Appendix D: Allowing Remote Assistance Support

You must perform the following changes to Group Policy settings to fully enable both Solicited (an invitation is sent from the novice computer) and Offer-based Remote Assistance connections for a computer running Windows XP with SP2 or Windows XP 64-bit Service Pack 1.

Enabling Solicited Remote Assistance

If the **Windows Firewall: Allow local program exceptions** setting is set to Not Configured (default) or Enabled, then no additional configuration is necessary.

If the **Windows Firewall: Allow local program exceptions** setting is set to Disabled, or you have already enabled the **Windows Firewall: Define program exceptions** setting, then you must add the following program exceptions:

- %WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exe:*:Enabled:Remote Assistance – Windows Messenger and Voice
- %WINDIR%\SYSTEM32\Sessmgr.exe:*:Enabled:Remote Assistance

Note For computers running Windows Server 2003 with SP1, do not add the exception for Sessmgr.exe. Instead, enable the **Windows Firewall: Allow Remote Desktop Exception** setting.

Enabling Offer-based Remote Assistance

Add the following entry to the **Windows Firewall: Define port exceptions** setting:

- 135:TCP:*:Enabled:Offer Remote Assistance

Add the following entries to the **Windows Firewall: Define program exceptions** setting:

- %WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe:*:Enabled:Offer Remote Assistance
- %WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exe:*:Enabled:Remote Assistance – Windows Messenger and Voice
- %WINDIR%\SYSTEM32\Sessmgr.exe:*:Enabled:Remote Assistance

Note For computers running Windows Server 2003 with SP1, do not add the exception for Sessmgr.exe. Instead, enable the **Windows Firewall: Allow Remote Desktop Exception** setting.

Note By opening TCP port 135, you are also allowing Remote Procedure Call (RPC) traffic.

Appendix E: Example of Using the Unattend.txt File

You can use the Unattend.txt file to implement custom Windows Firewall settings when performing an unattended installation of Windows XP SP2 from a central file share that contains all of the Windows XP SP2 files.

The sections of the Unattend.txt file for Windows Firewall configuration consist of the following:

- [WindowsFirewall]

A required section that defines which profiles to use and Windows Firewall log file settings.
- [WindowsFirewall.profile_name]

The Domain profile section, [WindowsFirewall.Domain], contains settings for when a computer is connected to a network that contains domain controllers for the domain of which the computer is a member. The Standard profile, [WindowsFirewall.Standard], contains settings for when a computer is not connected to a network that contains domain controllers for the domain of which the computer is a member.

The [WindowsFirewall.profile_name] section is a user-defined section that is referenced by the [WindowsFirewall] section to make changes to Windows Firewall's default configuration, including programs, services, ports, and ICMP settings.
- WindowsFirewall.program_name]

A user-defined section that adds a program to the Windows Firewall exceptions list.
- WindowsFirewall.service_name]

A user-defined section that adds a pre-defined service to the Windows Firewall exceptions list (such as file and print sharing, UPnP framework, remote desktop service, and remote administration service).
- WindowsFirewall.portopening_name]

A user-defined section that adds a port to the Windows Firewall exceptions list.
- [WindowsFirewall.icmpsetting_name]

A user-defined section that adds ICMP message types to the Windows Firewall exceptions list.

Here is an example Unattend.txt:

```
[WindowsFirewall]
Profiles=WindowsFirewall.Standard
LogFile = %WINDIR%\Pfirewall.log
LogSize = 4096
LogDroppedPackets = 1
LogConnections = 1

[WindowsFirewall.Standard]
Type = 3
Mode = 1
Exceptions = 1
Notifications = 1
MulticastBroadcastResponse = 1
AllowedPrograms = WindowsFirewall.RemoteAssistance
Services = WindowsFirewall.RemoteDesktop
PortOpenings = WindowsFirewall.WebService
IcmpSettings = WindowsFirewall.EchoRequest
```

```
[WindowsFirewall.RemoteAssistance]
Program = %WINDIR%\System32\Sessmgr.exe
Name = "Remote Assistance"
Mode = 1
Scope = 2
Addresses = 192.168.0.5, Local Subnet
```

```
[WindowsFirewall.RemoteDesktop]
Type = 2
Mode = 1
Scope = 2
Addresses = 192.168.0.5, Local Subnet
```

```
[WindowsFirewall.WebService]
Protocol = 6
Port = 80
Name = Web Server (TCP 80)
Mode = 1
Scope = 2
Addresses = 192.168.0.5, Local Subnet
```

```
[WindowsFirewall.EchoRequest]
Type = 8
Mode = 1
```

As another example, the following sections in the Unattend.txt file disable the use of Windows Firewall because another third party host firewall is being used:

```
[WindowsFirewall]
Profiles = WindowsFirewall.TurnOffFirewall
```

```
[WindowsFirewall.TurnOffFirewall]
Mode = 0
```

For more information, including the full syntax for commands and additional examples, see the Help topics in the [Windows Firewall] section of the Unattend.txt file in the Ref.chm Help file. You can obtain this Help file by running Setup.exe from the Support\Tools folder of the Windows XP SP2 CD. The Ref.chm file is stored in the Deploy.cab file in this same folder. To order the Windows XP SP2 CD, see [Order Windows XP Service Pack 2 on CD](#).

Appendix F: Example of Using the Netfw.inf File

You can use the Netfw.inf file to implement custom Windows Firewall settings when performing an interactive installation of Windows XP SP2 from a central file share that contains all of the Windows XP SP2 files.

The default contents of the Netfw.inf file are the following:

```
[version]
Signature       = "SWindows NTS"
DriverVer      =07/01/2001, 5. 1. 2600. 2132

[DefaultInstall]
AddReg=ICF.AddReg.DomainProfile
AddReg=ICF.AddReg.StandardProfile

[ICF.AddReg.DomainProfile]
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\AuthorizedApplications\List", "%windir%\system32\sessmgr.exe", 0x00000000, "%windir%\system32\sessmgr.exe: *: enabled:@xpsp2res.dll, -22019"

[ICF.AddReg.StandardProfile]
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List", "%windir%\system32\sessmgr.exe", 0x00000000, "%windir%\system32\sessmgr.exe: *: enabled:@xpsp2res.dll, -22019"
```

The first two sections of Netfw.inf contain versioning and configuration information and do not need to be modified. The sections that are significant for modifying the default configuration for Windows Firewall are the following:

- **ICF.AddReg.DomainProfile** – Defines changes to Windows Firewall's default configuration when a computer is connected to a network that contains domain controllers for the domain of which the computer is a member.
- **ICF.AddReg.StandardProfile** – Defines changes to Windows Firewall's default configuration when a computer is not connected to a network that contains domain controllers for the domain of which the computer is a member. If a computer is not a member of a domain, Windows Firewall uses the configuration stored in the standard profile.

For example, to modify the default Netfw.inf file to contain a setting to disable the use of Windows Firewall for the domain profile because another host firewall is being used, you would add the following line to the **ICF.AddReg.DomainProfile** section:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile", "EnableFirewall", 0x00010001, 0
```

For more information about using the Netfw.inf file, see [Using the Windows Firewall INF File in Microsoft Windows XP Service Pack 2](#).

Appendix G: Port Numbers for Microsoft Applications and Services

Consult the following resources for information about TCP and UDP port numbers for Microsoft applications and services:

- [Frequently Asked Questions about the Systems Management Server Client](#)
- [How to enable ports on Windows XP SP2 for Analysis Services and SQL Server 7.0 OLAP Services](#)
- [How to configure Windows XP Service Pack 2 \(SP2\) for use with SQL Server](#)
- [Programs Require Manual Port Configurations with Internet Connection Firewall](#)
- [XCCC: Setting TCP/IP Ports for Exchange and Outlook Client Connections Through a Firewall](#)
- [XADM: Setting TCP/IP Port Numbers for Internet Firewalls](#)
- [How to Play Internet Games Through a Firewall or Proxy Server in Windows XP](#)
- [INF: TCP Ports Used by OLAP Services when Connecting Through a Firewall](#)
- [INF: TCP Ports Needed for Communication to SQL Server Through a Firewall](#)
- [XCCC: TCP/IP Ports Used by Microsoft Mobile Information Server](#)
- [TCP and UDP Port Assignments](#)
- [How to Open Ports in the Windows XP Internet Connection Firewall](#)

For additional articles, search on "Windows Firewall" in the [Microsoft Knowledge Base](#).

Appendix H: Windows Firewall in Windows Server 2003 Service Pack 1

Windows Server 2003 Service Pack 1 (SP1) also includes Windows Firewall, which works the same way as Windows Firewall in Windows XP SP2. However, because the purpose of a server computer is to accept incoming unsolicited traffic, Windows Firewall for Windows Server 2003 SP1 is disabled by default.

The exception to this behavior is the following: for a new installation of Windows Server 2003 that already includes SP1 (known as a slipstream installation), Windows Firewall is enabled by default for the duration of the Security Out-of-Box Experience, a portion of the initial setup of the server computer in which the latest security fixes are downloaded and installed from Windows Update. After the Security Out-of-Box Experience is complete, Windows Firewall is disabled. If you do not want the Security Out-of-Box Experience, you can use the Unattend.txt file or Group Policy to configure Windows Firewall settings. The Security Out-of-Box Experience does not occur if there are configured firewall settings.

You can enable Windows Firewall on a computer running Windows Server 2003 with SP1 manually using the Windows Firewall component of Control Panel, through Group Policy settings as described in this article, or you can use the new Security Configuration Wizard in Windows Server 2003 SP1. The Security Configuration Wizard is the recommended method to enable and configure Windows Firewall and other security settings on computers running Windows Server 2003 with SP1.

If you enable Windows Firewall interactively after the server computer is up and running, you should restart the server computer. This assures that Windows Firewall can add entries to its exceptions table for the ports opened by programs that correspond to enabled program-based exceptions. Windows Firewall cannot determine the ports that have been opened by a program if they were opened before the Windows Firewall was started. Various messages for Windows Firewall have been updated in Windows Server 2003 SP1 to remind the computer user to restart the system if Windows Firewall is enabled interactively.

For more information about Windows Firewall in Windows Server 2003 SP1, see the [Windows Server 2003 Windows Firewall \(WF\) TechCenter](#).

Summary

Windows XP SP2 contains the new Windows Firewall, which replaces ICF in Windows XP with SP1 and Windows XP with no service packs installed. Because Windows XP SP2 enables Windows Firewall by default on all connections, communications can be affected if the Windows XP with SP2-based computer is managed or is acting as a server, a listener, or a peer. You can deploy Windows Firewall settings in an organization intranet for computers running Windows XP with SP2 using the new Windows Firewall Computer Configuration Group Policy settings, the Unattend.txt file, the Netfw.inf file, a Netsh script, or a custom configuration program.

Related Links

See the following resources for further information:

- [Troubleshooting Windows Firewall in Microsoft Windows XP Service Pack 2](http://www.microsoft.com/downloads/details.aspx?FamilyID=b3d01193-ad93-492f-b74b-97c2fc44e08b&displaylang=en) at <http://www.microsoft.com/downloads/details.aspx?FamilyID=b3d01193-ad93-492f-b74b-97c2fc44e08b&displaylang=en>
- [Manually Configuring Windows Firewall in Windows XP Service Pack 2](http://www.microsoft.com/technet/community/columns/cableguy/cg0204.mspx) at <http://www.microsoft.com/technet/community/columns/cableguy/cg0204.mspx>
- [Using the Windows Firewall INF File in Microsoft Windows XP Service Pack 2](http://www.microsoft.com/downloads/details.aspx?FamilyID=cb307a1d-2f97-4e63-a581-bf25685b4c43&displaylang=en) at <http://www.microsoft.com/downloads/details.aspx?FamilyID=cb307a1d-2f97-4e63-a581-bf25685b4c43&displaylang=en>
- [Network Determination Behavior for Network-Related Group Policy Settings](http://www.microsoft.com/technet/community/columns/cableguy/cg0504.mspx) at <http://www.microsoft.com/technet/community/columns/cableguy/cg0504.mspx>
- [Windows XP Service Pack 2 Resources for IT Professionals](http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/winxpsp2.mspx) at <http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/winxpsp2.mspx>

For the latest information about Windows XP, see the [Windows XP Web site](http://www.microsoft.com/windowsxp) at <http://www.microsoft.com/windowsxp>.