Search

Troubleshooting Windows Firewall settings in Windows XP Service Pack 2 for advanced users

Article ID : 875357
Last Review : November 29, 2007
Revision : 2.1

Notice

This article is intended for advanced computer users. If you are not comfortable with advanced troubleshooting, you might want to ask someone for help or contact support. For information about how to do this, visit the following Microsoft Web site:

http://support.microsoft.com/contactus/ (http://support.microsoft.com/contactus/)

On This Page

SUMMARY

Windows XP Service Pack 2 (SP2) includes Microsoft Windows Firewall, the updated firewall software that replaces Internet Connection Firewall (ICF). If Microsoft Windows Firewall is blocking a port that is used by a service or by a program, you can configure the Windows Firewall to create an exception. Windows Firewall may be blocking a program or a service if the following conditions are true:

- *Programs do not respond to a client's request.*
- *Client programs do not receive data from the server.*

A Windows Firewall Security Alert may notify you that Windows Firewall is blocking a particular program. When this scenario occurs, you may unblock the program by selecting Unblock this program in the Security Alert dialog box. To help determine which programs and ports are being blocked, you can configure Windows Firewall to log dropped packets. With Windows Firewall Netsh Helper, you can configure Windows Firewall and Windows Firewall logging at the command prompt. Program compatibility may not always be the issue. Group Policy settings can also prevent

programs from running. Windows XP Service Pack 2 (SP2) includes several utilities that you can use to troubleshoot Windows Firewall issues.

INTRODUCTION

The best way to resolve firewall blocking issues is to modify programs to work with stateful filtering firewalls. If you cannot modify a program, you can configure the Windows Firewall to add exceptions for specific ports and programs. This article discusses the failure symptoms that relate to the default configuration of the Windows XP Service Pack 2 firewall, how to configure exceptions for ports and for programs, and how to perform some troubleshoot methods for firewall settings.

MORE INFORMATION

Failures that are related to the default firewall configuration appear in two ways. Client programs may not receive data from a server. Server programs that are running on a Windows XP-based computer may not respond to client requests.
If a program is being blocked, you may receive the following Windows Firewall Security Alert:

For information about these symptoms and advanced troubleshooting steps to resolve them, see the "Advanced troubleshooting" section.

Configuring Windows Firewall by using the Windows Firewall Security Alert

To unblock the program, click Unblock in the Security Alert dialog box.

Configuring Windows Firewall by using the Windows Security Center

Adding a program exception

When you add a program to the exception list, you enable the firewall to open ranges of ports that could change every time the program is run. To add a program exception, follow these steps:

1. Use an administrator account to log on.
2. Click Start, click Run, type wscui.cpl, and then click OK.
3. In Windows Security Center, click Windows Firewall.
4. On the Exceptions tab, click Add Program.

5. In the list of programs, click the name of the program that you want to add, and then click OK. If the name of your program is not in the list of programs, click Browse to locate the program, and then click OK. Note If you do not know where the program is located, contact the program vendor to determine the program location.

   For information about how to contact your program vendor, click the appropriate article number in the following list to view the article in the Microsoft Knowledge Base:

   65416 (http://support.microsoft.com/kb/65416/) Hardware and software vendor contact information, A-K

   60781 (http://support.microsoft.com/kb/60781/) Hardware and software vendor contact information, L-P

   60782 (http://support.microsoft.com/kb/60782/) Hardware and software vendor contact information, Q-Z

6. Click OK.
7. Test the program to verify that the firewall settings are correct.

If you are still experiencing problems, you might want to ask someone for help or contact support. For information about how to do this, visit the following Microsoft Web site:

http://support.microsoft.com/contactus (http://support.microsoft.com/contactus)

Advanced troubleshooting

This section is intended for advanced computer users. If you are not comfortable with advanced troubleshooting, you might want to ask someone for help or contact support. For information about how to do this, visit the following Microsoft Web site:

http://support.microsoft.com/contactus (http://support.microsoft.com/contactus/)

Recognizing failure symptoms

Failures that are related to the default firewall configuration appear in two ways:

- Client programs may not receive data from a server. For example, the following client programs may not receive data:
  - An FTP client
  - Multimedia streaming software
  - New mail notifications in some e-mail programs
- Server programs that are running on a Windows XP-based computer may not respond to client requests. For example, the following server programs may not respond:
  - A Web server program, such as Internet Information Services (IIS)
  - Remote Desktop
  - File sharing

  Notes
  - Failures in network programs are not limited to firewall issues. These failures may be caused by RPC or DCOM security changes. Therefore, you have to determine whether the failure is accompanied by a Windows Firewall Security Alert that indicates that a program is being blocked.

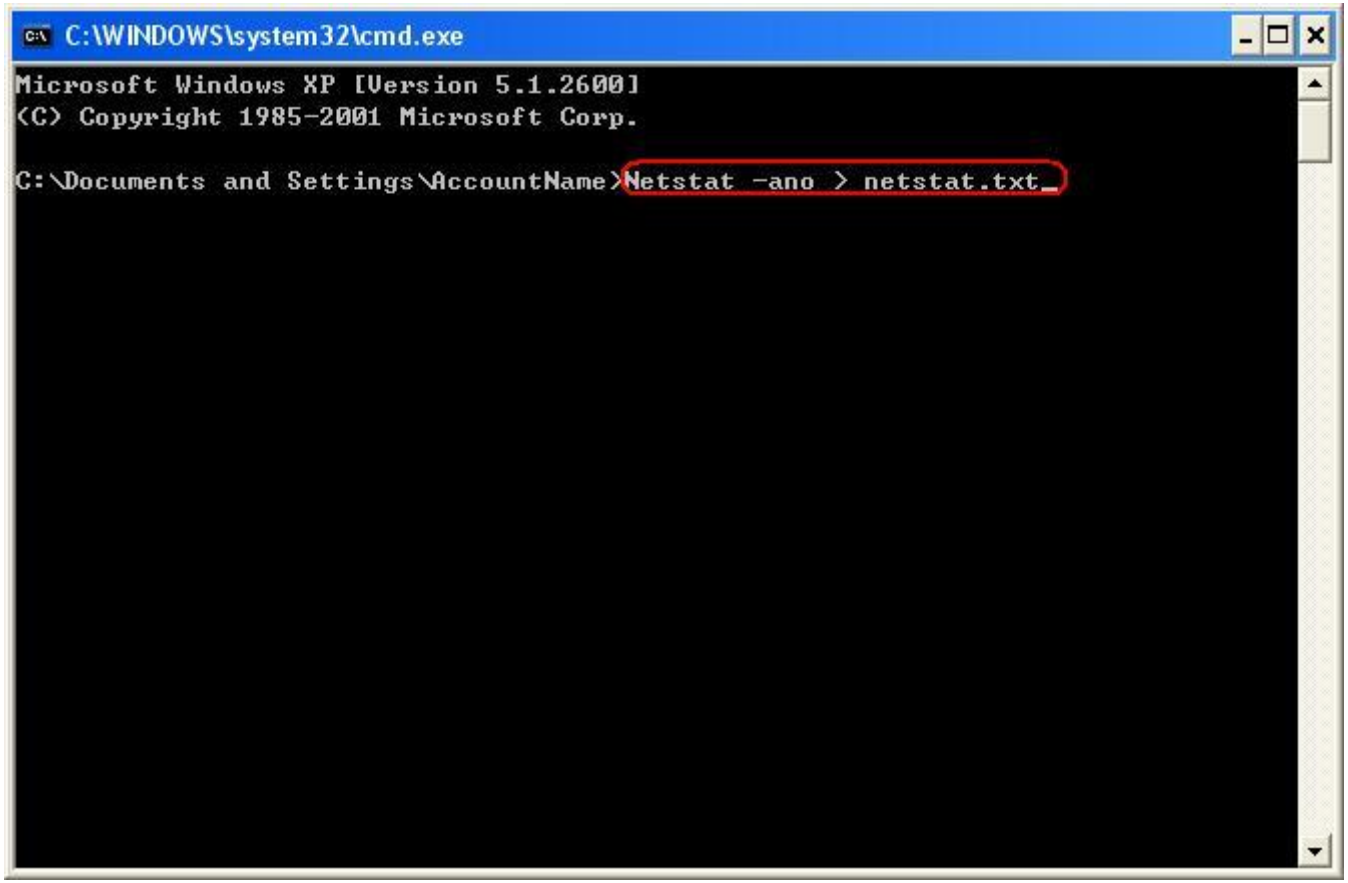
- Service failures are not accompanied by a Windows Firewall Security Alert because services are not typically associated with a user logon session. If the failure is service-related, configure the firewall as discussed in the "Configuring Windows Firewall by using the Windows Security Center" section.

Adding a port exception

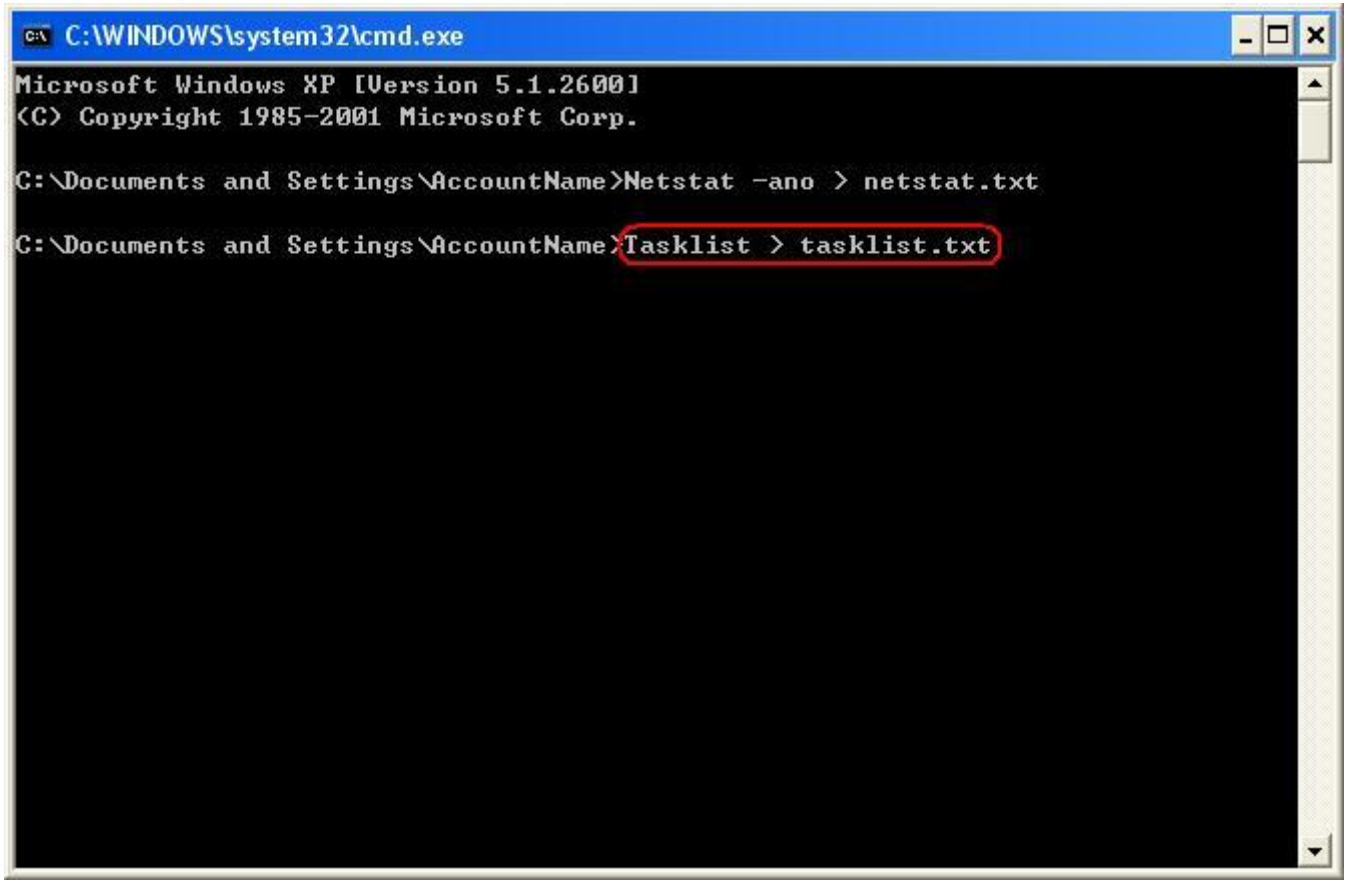
If you do not resolve this issue by adding a program to the exception list, you can add ports manually. To do this, you must first identify the ports that are used by the program. A reliable way to determine port usage is to contact the program vendor. If you cannot contact a vendor, or if a port list is not available, you can use the Netstat.exe tool to identify the ports in use.

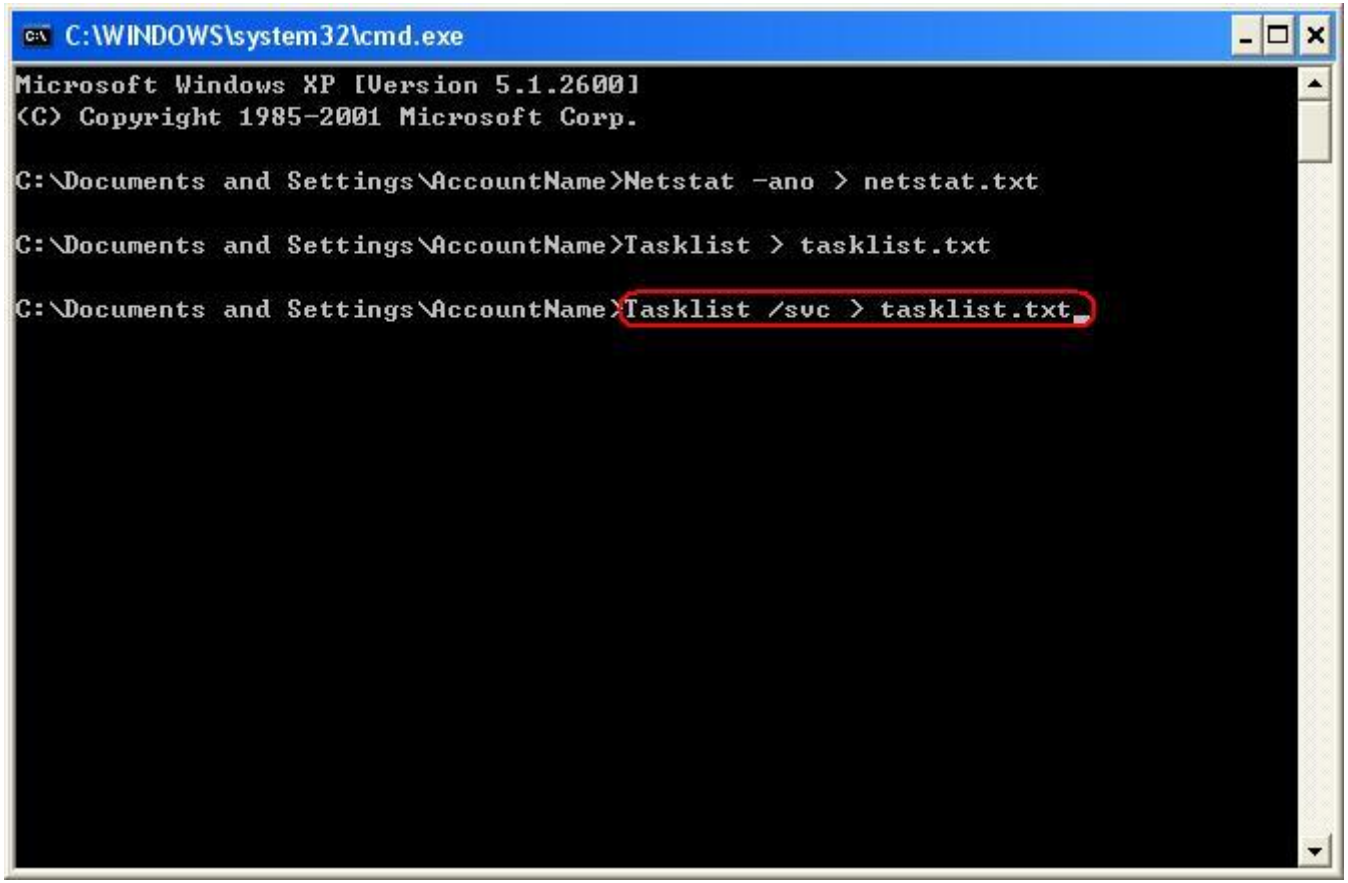
Identifying the ports

1. Start the program and try to use its network features. For example, with a multimedia program, try to start an audio stream. With a Web server, try to start the service.
2. Click Start, click Run, type cmd, and then click OK.
3. At the command prompt, type netstat –ano > netstat.txt, and then press ENTER. This command creates the Netstat.txt file. This file lists all the listening ports.

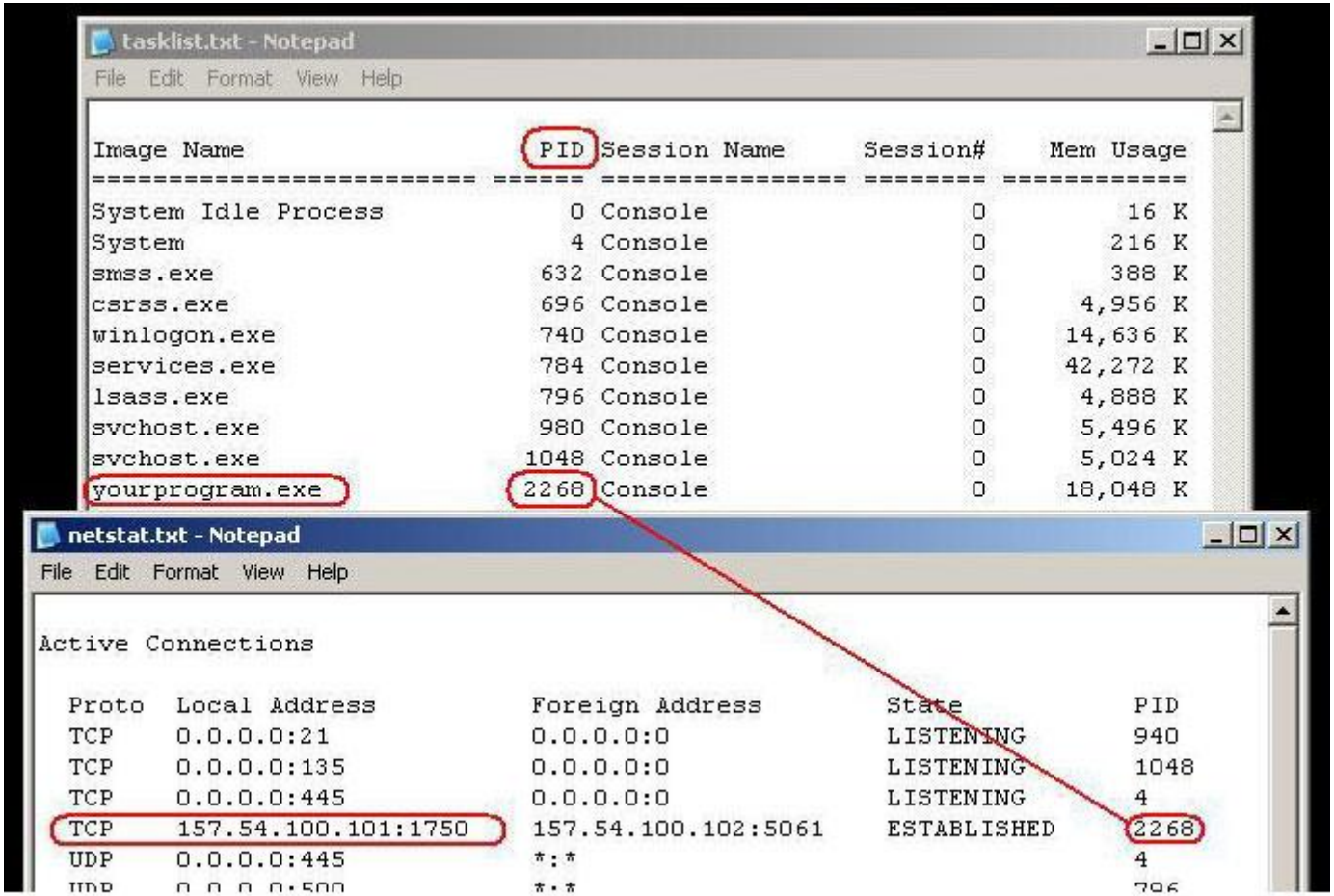


4. At the command prompt, type tasklist > tasklist.txt, and then press ENTER. If the program in question runs as a service, type tasklist /svc > tasklist.txt instead of tasklist > tasklist.txt so that the services that are loaded in each process are listed.


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\AccountName>Netstat -ano > netstat.txt
C:\Documents and Settings\AccountName>Tasklist > tasklist.txt



5. Open the Tasklist.txt file, and then locate the program that you are troubleshooting. Write down the Process Identifier for the process, and then open the Netstat.txt file. Note any entries that are associated with that Process Identifier and the protocol that is used.



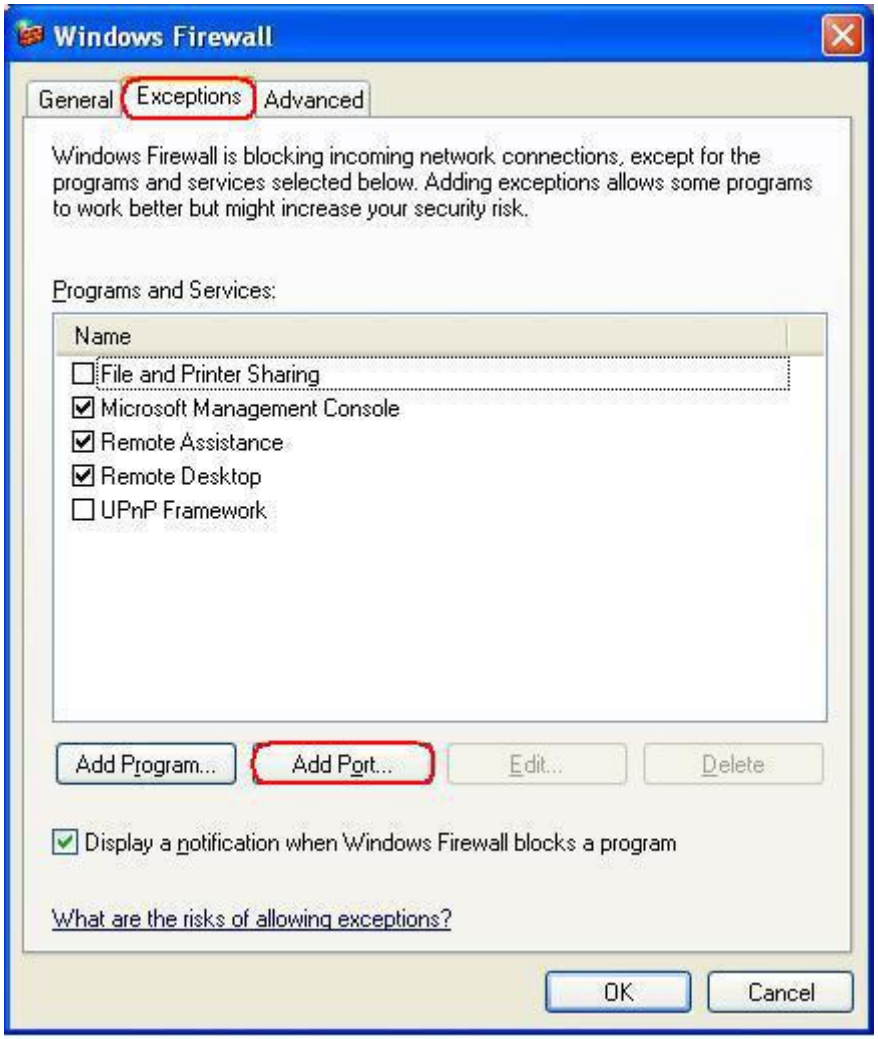
The program with process identifier (PID) 2268 is using port 1750 on the local computer.

If the port numbers for the process are less than 1024, the port numbers will probably not change. If the numbers that are used are greater than or equal to 1024, the program may use a range of ports. Therefore, you may not be able to resolve the issue by opening individual ports.

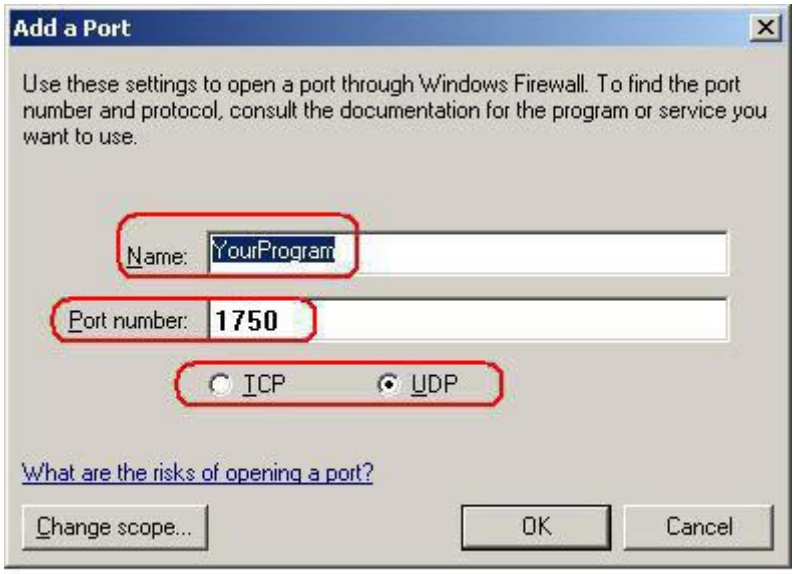
Adding the port exception

1. Click Start, click Run, type wscui.cpl, and then click OK.
2. In Windows Security Center, click Windows Firewall.

3. Click the Exceptions tab, and then click Add Port to display the Add a Port dialog box.

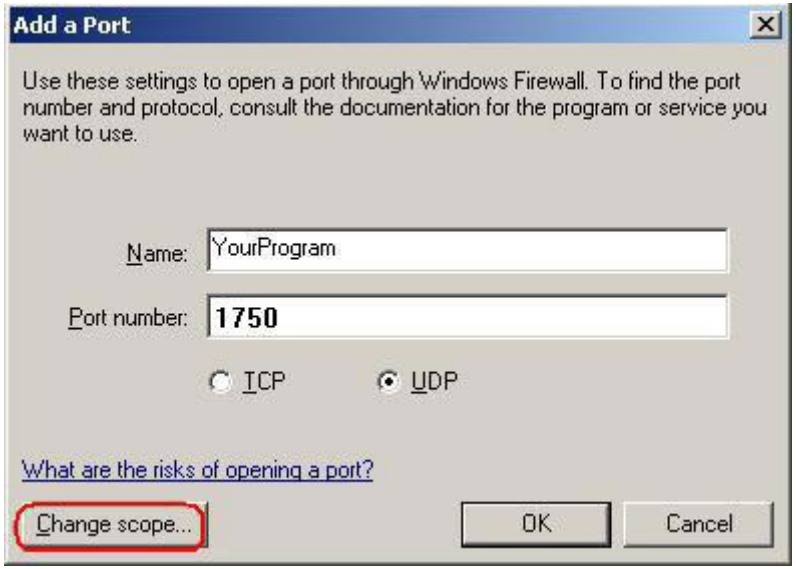


4. Type a descriptive name for the port exception and the port number that your program uses, and then select either the TCP or UDP protocol.

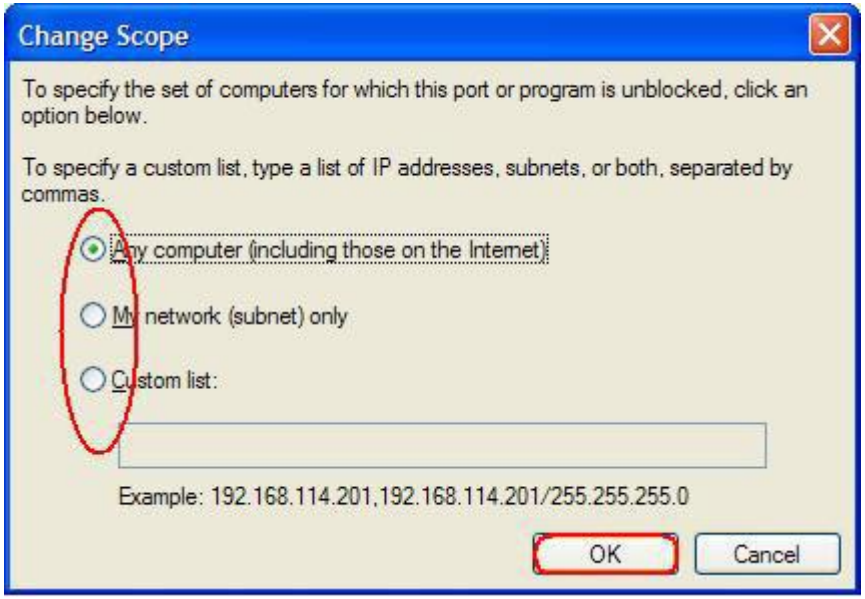


After you finish this step, the **Add a Port** dialog box will appear as shown here.

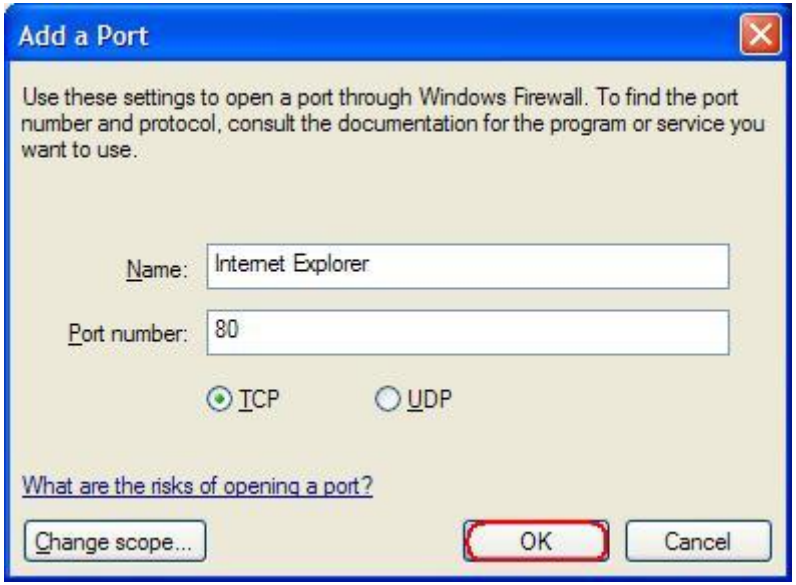
5. Click Change Scope.



6. View or set the scope for the port exception, and then click OK.



7. Click OK to close the Add a Port dialog box.



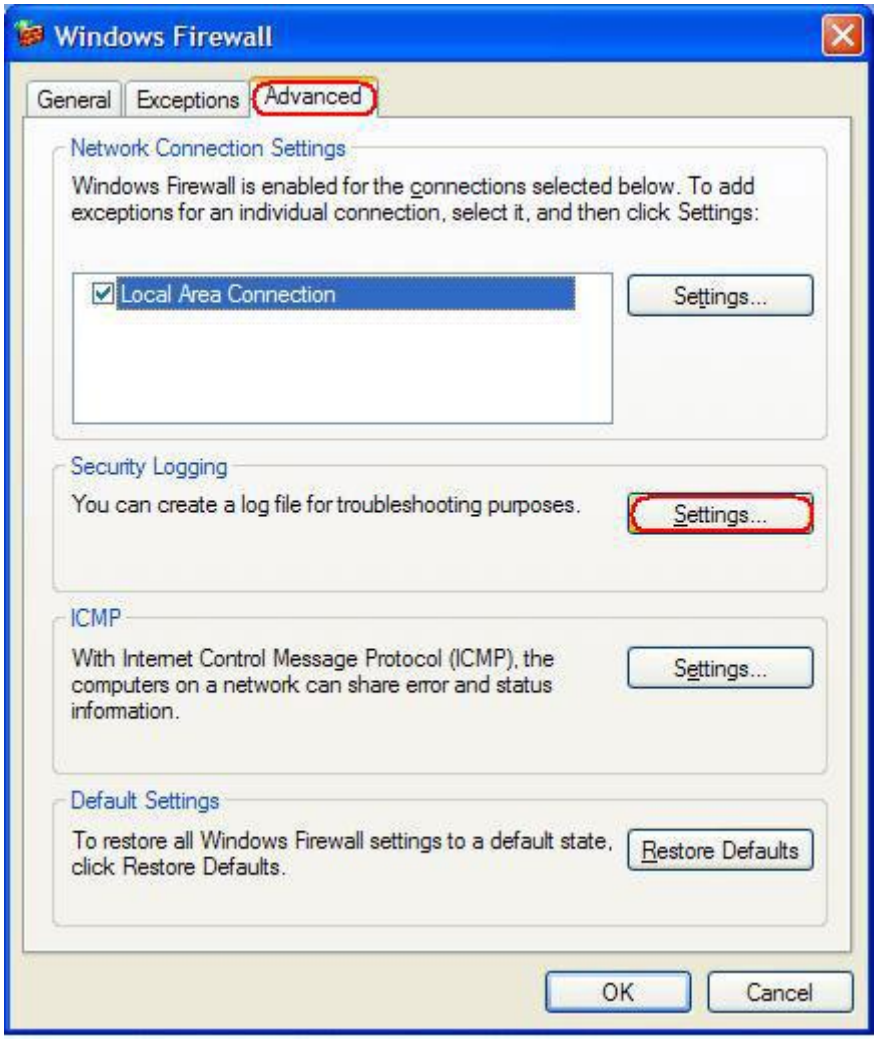
8. To verify that the port settings are correct for your program, test the program.

Using Logging

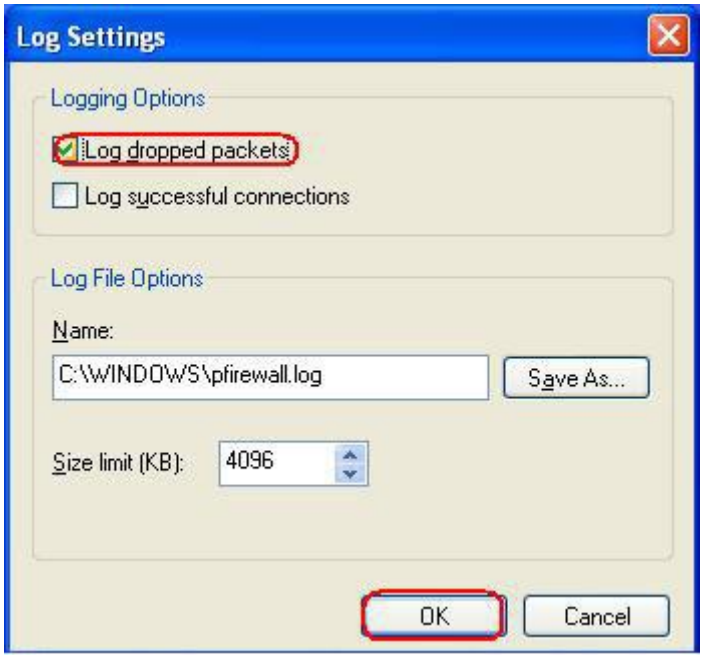
You can enable logging to help identify the source of inbound traffic and to provide details on what traffic is being blocked. %Windir%\pfirewall.log is the default log file. To enable logging, follow these steps:

1. Click Start, click Run, type firewall.cpl, and then click OK.
2. Click the Advanced tab.

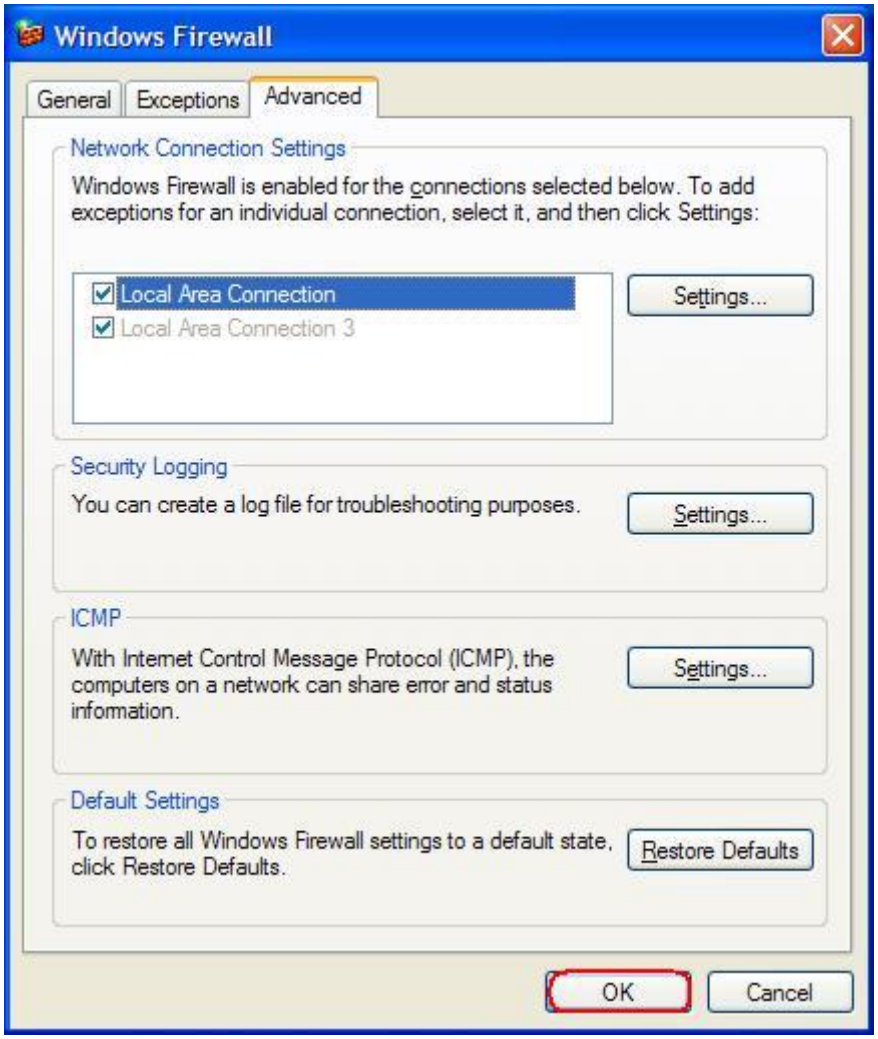
3. In the Security Logging area, click Settings.



4. Click to select the Log dropped packets check box, and then click OK.


Log Settings
Logging Options
Log dropped packets
Log successful connections
Log File Options
Name:
C:\WINDOWS\pfirewall.log
Save As...
Size limit (KB):
4096
OK
Cancel

5. Click OK.



Note Outbound successes are not logged. Outbound traffic that is not blocked is not logged.

Interpreting the log file

The following log information is collected for each packet that is logged:

Fields	Description	Example

Date	Displays the year, month, and day that the recorded transaction occurred. Dates are recorded in the format YYYY-MM-DD, where YYYY is the year, MM is the month, and DD is the day.	2001-01-27
Time	Displays the hour, minute, and seconds when the recorded transaction occurred. Times are recorded in the format: HH:MM:SS, where HH is the hour in 24-hour format, MM is the number of minutes, and SS is the number of seconds.	21:36:59
Action	Indicates the operation that was observed by the firewall. The options available to the firewall are OPEN, CLOSE, DROP, and INFO-EVENTS-LOST. An INFO-EVENTS-LOST action indicates the number of events that occurred but that were not recorded in the log.	OPEN
Protocol	Displays the protocol that was used for the communication. A protocol entry can also be a number for packets that are not using TCP, UDP, or ICMP.	TCP
src-ip	Displays the source IP address, or the IP address of the computer, that is trying to establish communications.	192.168.0.1
dst-ip	Displays the destination IP address of a communication try.	192.168.0.1
src-port	Displays the source port number of the sending computer. A src-port entry is recorded in the form of a whole number, between 1 and 65,535. Only TCP and UDP display a valid src-port entry. All other protocols display a src-port entry of -.	4039
dst-port	Displays the port number of the destination computer. A dst-port entry is recorded in the form of a whole number, between 1 and 65,535. Only TCP and UDP display a valid dst-port entry. All other protocols display a dst-port entry of -.	53
size	Displays the packet size in bytes.	60
tcpflags	Displays the TCP control flags that are found in the TCP header of an IP packet: • Ack acknowledgement field significant • Fin No more data from sender • Psh Push function • Rst Reset the connection • Syn Synchronize sequence numbers • Urg Urgent Pointer field significant Flags are written as uppercase letters.	AFP
tcpsyn	Displays the TCP sequence number in the packet.	1315819770
tcpack	Displays the TCP acknowledgement number in the packet.	0
tcpwin	Displays the TCP window size in bytes in the packet.	64240
icmptype	Displays a number that represents the Type field of the ICMP message.	8
icmpcode	Displays a number that represents the Code field of the ICMP message.	0
info	Displays an information entry that depends on the type of action that occurred. For example, an INFO-EVENTS-LOST action creates an entry for the number of events that occurred but were not recorded in the log from the time of the last	23

occurrence of this event type.

Note The hyphen (-) is used for fields where no information is available for an entry.

Using command-line support

Windows Firewall Netsh Helper was added to Windows XP in the Microsoft Advanced Networking Pack. This command-line helper previously applied to IPv6 Windows Firewall. With Windows XP Service Pack 2, the helper now includes support for configuring IPv4.

With Netsh Helper, you can now:

- Configure the default state of Windows Firewall. (Options include Off, On, and On with no exceptions.)
- Configure the ports that must be open.
- Configure the ports to enable global access or to restrict access to the local subnet.
- Set ports to be open on all interfaces or only on a specific interface.
- Configure the logging options.
- Configure the Internet Control Message Protocol (ICMP) handling options.
- Add or remove programs from the exceptions list.

These configuration options apply to both IPv4 Windows Firewall and IPv6 Windows Firewall except where specific functionality does not exist in the Windows Firewall version.

Gathering diagnostic data

Windows Firewall configuration and status information can be retrieved at the command line by using the Netsh.exe tool. This tool adds IPv4 firewall support to the following Netsh context:

```
netsh firewall
```

To use this context, type netsh firewall at a command prompt, and then use additional Netsh commands as needed. The following commands are useful for gathering firewall status and configuration information:

- Netsh firewall show state
- Netsh firewall show config

Compare the output from these commands with the output from the netstat –ano command to identify the programs that may have listening ports open and that do not have corresponding exceptions in the firewall configuration. Supported data gathering and configuration commands are listed in the following tables.

Note Settings can be modified only by an administrator.

Data Gathering

Command	Description
show allowedprogram	Displays the allowed programs.

show config	Displays the detailed local configuration information.
show currentprofile	Displays the current profile.
show icmpsetting	Displays the ICMP settings.
show logging	Displays the logging settings.
show opmode	Displays the operational mode.
show portopening	Displays the excepted ports.
show service	Displays the services.
show state	Displays the current state information.
show notifications	Displays the current settings for notifications.

Configuration

Command	Description
add allowedprogram	Used to add excepted traffic by specifying the program's file name.
set allowedprogram	Used to modify the settings of an existing allowed program.
delete allowedprogram	Used to delete an existing allowed program.
set icmpsetting	Used to specify allowed ICMP traffic.
set logging	Used to specify logging options for Windows Firewall either globally or for a specific connection (interface).
set opmode	Used to specify the operating mode of Windows Firewall either globally or for a specific connection (interface).
add portopening	Used to add excepted traffic by specifying a TCP or UDP port.
set portopening	Used to modify the settings of an existing open TCP or UDP port.
delete portopening	Used to delete an existing open TCP or UDP port.
set service	Used to enable or drop RPC and DCOM traffic, file and printer sharing, and UPnP traffic.
set notifications	Used to specify whether notifications to the user when programs try to open ports are enabled.
reset	Resets firewall configuration to default. This provides the same functionality as the Restore Defaults button in the Windows Firewall interface.

Troubleshooting the firewall

Along with program compatibility issues, the Windows Firewall may experience other problems. Follow these steps to diagnose problems:

1. To verify that TCP/IP is functioning correctly, use the ping command to test the loopback address (127.0.0.1) and the assigned IP address.
2. Verify the configuration in the user interface to determine whether the firewall has been unintentionally set to Off or On with No Exceptions.
3. Use the netsh commands for Status and Configuration information to look for unintended settings that could be interfering with expected behavior.
4. Determine the status of the Windows Firewall/Internet Connection Sharing service by typing the following at a command prompt:

   sc query sharedaccess

   (The short name of this service is SharedAccess.) Troubleshoot service startup based on the Win32 exit code if this service does not start.
5. Determine the status of the Ipnat.sys firewall driver by typing the following at a command prompt:

   sc query ipnat

   This command also returns the Win32 exit code from the last start try. If the driver is not starting, use troubleshooting steps that would apply to any other driver.
6. If the driver and service are both running, and no related errors exist in the event logs, use the Restore Defaults option on the Advanced tab of Windows Firewall properties to eliminate any potential problem configuration.
7. If the issue is still not resolved, look for policy settings that might produce the unexpected behavior. To do this, type GPResult /v > gpresult.txt at the command prompt, and then examine the resulting text file for configured policies that are related to the firewall.

Configuring Windows Firewall Group Policy

Contact your network administrator to determine if a Group Policy setting prevents programs and scenarios from running in a corporate environment.

Windows Firewall Group Policy settings are located in the following Group Policy Object Editor snap-in paths:

- Computer Configuration/Administrative Templates/Network/Network Connections/Windows Firewall
- Computer Configuration/Administrative Templates/Network/Network Connections/Windows Firewall/ Domain Profile
- Computer Configuration/Administrative Templates/Network/Network Connections/Windows Firewall/ Standard Profile

From these locations, you can configure the following Group Policy settings:

- Windows Firewall: Allow authenticated Internet Protocol security (IPsec) bypass
- 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 Universal Plug and Plan (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

For more information about Windows Firewall Group Policy settings, download the following white paper:

Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2
(http://download.microsoft.com/download/6/8/a/68a81446-cd73-4a61-8665-8a67781ac4e8/wf_xpsp2.doc)

REFERENCES

843090 (http://support.microsoft.com/kb/843090/) Description of the Windows Firewall feature in Windows XP Service Pack 2

892199 (http://support.microsoft.com/kb/892199/) Certain Administrative Templates from the Windows XP Security Guide may prevent you from starting the Windows Firewall service in Windows XP Service Pack 2

920074 (http://support.microsoft.com/kb/920074/) You cannot start the Windows Firewall service in Windows XP SP2

886257 (http://support.microsoft.com/kb/886257/) How Windows Firewall affects the UPnP framework in Windows XP Service Pack 2

If these articles do not help you resolve the problem or if you experience symptoms that differ from those that are described in this article, search the Microsoft Knowledge Base for more information. To search the Microsoft Knowledge Base, visit the following Microsoft Web site:

http://support.microsoft.com (http://support.microsoft.com/)

Then, type the text of the error message that you receive, or type a description of the problem in the Search Support (KB) field.

APPLIES TO

- Microsoft Windows XP Professional
- Microsoft Windows XP Home Edition

Keywords: kbresolve kbgraphxlink kbnomt kbscreenshot kbtshoot kbhowtomaster KB875357