Security

How to Configure Windows Firewall on a Single Computer

Introduction

Windows Firewall is a new feature of Microsoft® Windows® XP Service Pack 2 (SP2) that is turned on by default. It monitors and restricts the information that travels between your computer and a network such as the Internet. Windows Firewall helps to provide a line of defense against someone who might try to access your computer over a network without your permission. It also helps to block malicious software and worms and provides a means to log security events.

Windows Firewall helps to protect your computer by blocking unsolicited traffic. Unsolicited traffic is any attempt to communicate with your computer over a network connection that was not specifically requested by programs running on your computer. Therefore programs such as Microsoft® Internet Explorer or Outlook® Express will continue to operate successfully with Windows Firewall enabled.

This document describes how to configure Windows Firewall on a single computer if the recommended default settings do not meet your requirements. For example, you might need to adjust settings if you use a program that needs an open connection to the Internet, or if you connect your mobile computer to a public network in a hotel or airport. This document focuses on:

- How to configure Windows Firewall General Settings
- How to configure Windows Firewall Exceptions
- How to configure Windows Firewall Advanced settings

  IMPORTANT: All of the step-by-step instructions included in this document use the Start menu that appears by default when you install Windows XP. If you have modified your Start menu, the procedures might differ slightly.

Before You Begin

This document provides guidance to configure the Windows Firewall feature of Windows XP SP2. It focuses on the configuration of Windows Firewall on a single computer in a small business environment.

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

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

Configuring Windows Firewall General Settings

The Windows Firewall general settings allow you to configure these options:

- **On (recommended)**. This is the default setting (with Don't allow exceptions not selected).
    - **Don't allow exceptions**. When this check box is selected, the firewall is placed into On With No Exceptions mode which blocks all unsolicited requests to connect to your computer. This includes requests to programs or services that you select on the Exceptions tab. Use the Don't allow exceptions setting when you need maximum protection for your computer, such as when you connect to a public network in a hotel or airport, or when a vulnerability is discovered and either you have not had time to download a hotfix for your computer or a hotfix is unavailable.

      After you have installed the latest operating system service packs and software updates, you can restore normal Internet functionality by returning the operational mode to On with Don't allow exceptions cleared.

- **Off (not recommended)**. Turning off Windows Firewall might make your computer more vulnerable to damage from viruses, worms, or intruders.

To modify the recommended Windows Firewall default general settings, perform these tasks:

- Open Windows Security Center
- Open Windows Firewall
- Configure Windows Firewall On with No Exceptions mode
- Disable Windows Firewall
- Verify Windows Firewall General settings are applied

  Note: The steps to disable Windows Firewall are listed here but should only be performed by advanced users for computer administration purposes, or if your computer is protected by another hardware or software firewall.

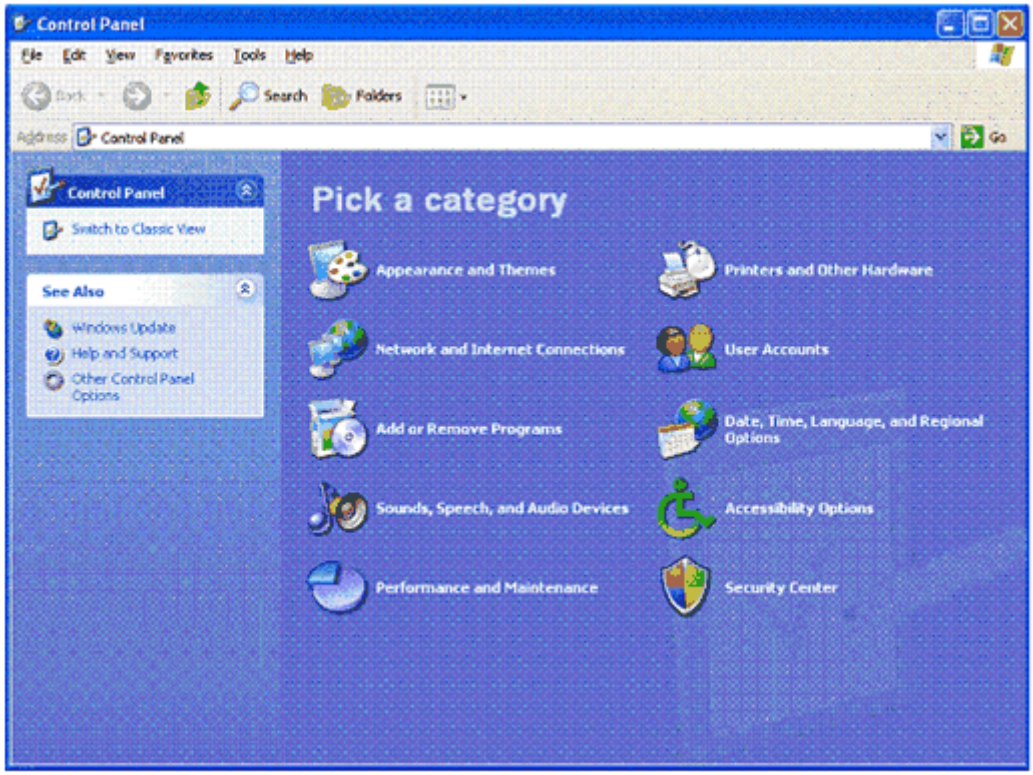
Requirements to perform this task

- Credentials: You must be logged on as a member of the local Administrators group.

Open Windows Security Center

To open Windows Security Center

1. From the Windows XP SP2 desktop, click **Start**, and then click **Control Panel**.

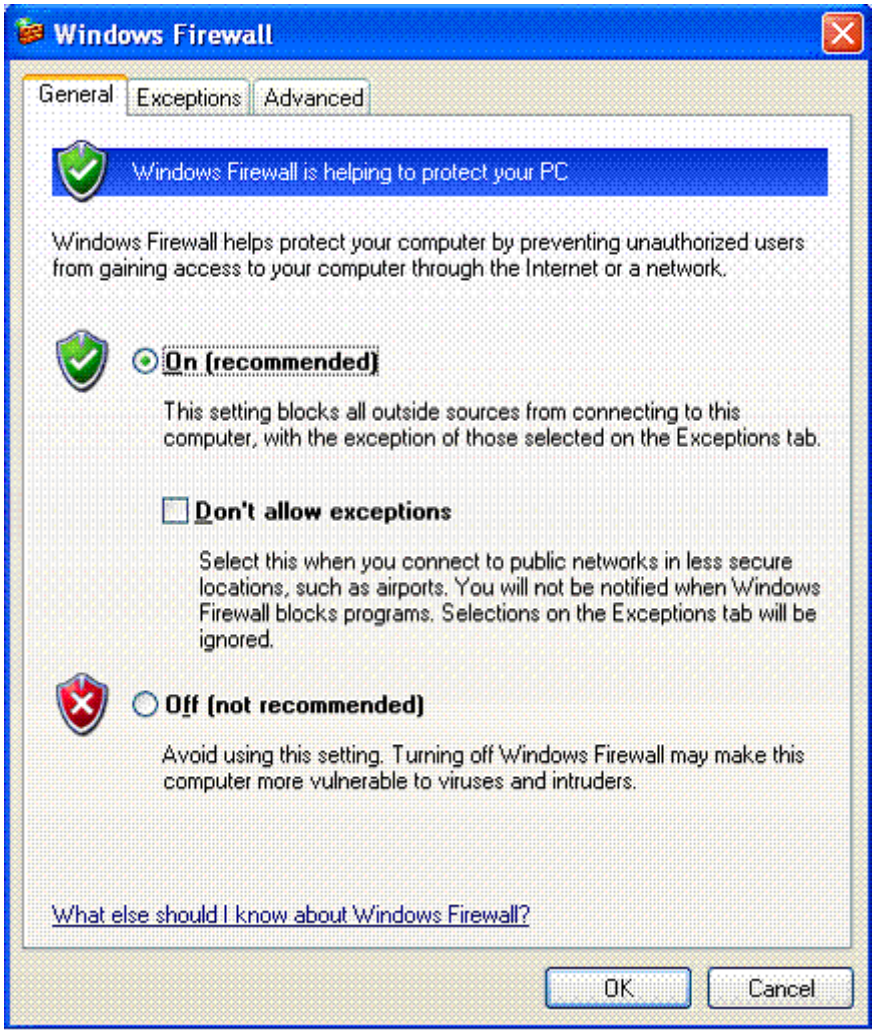


2. In Control Panel, click **Security Center**.

Open Windows Firewall

To open Windows Firewall

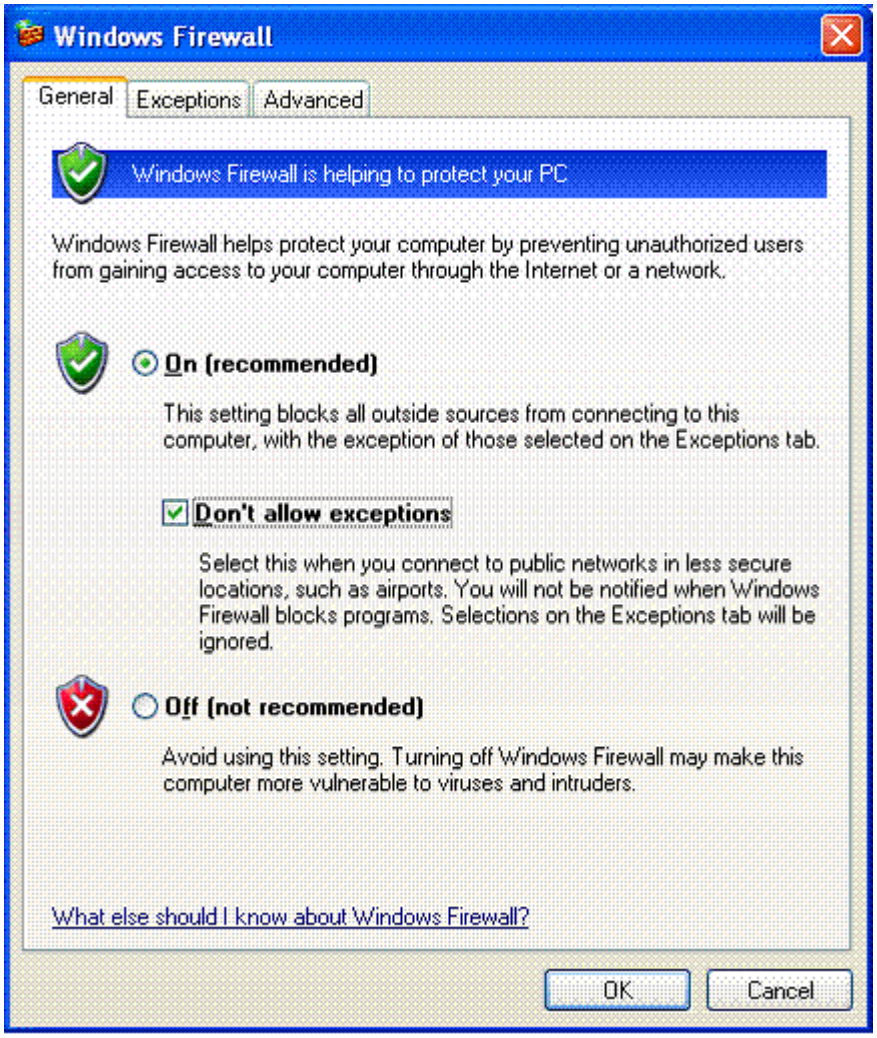
1. In **Windows Security Center**, under **Manage security settings for**, click **Windows Firewall**.



Configure Windows Firewall On With No Exceptions

To configure Windows Firewall On with no exceptions mode

1. In the **Windows Firewall** dialog box, select the **Don't allow exceptions** check box.



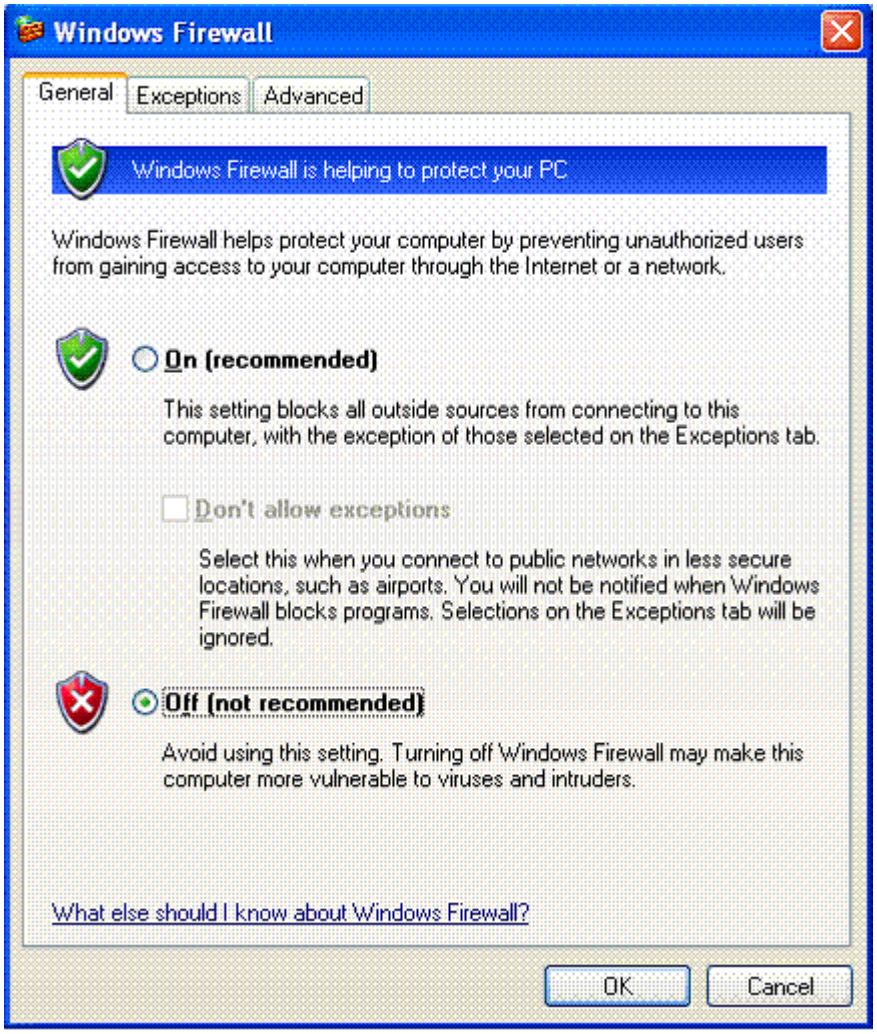
2. Click **OK**.

Disable Windows Firewall

WARNING: Disabling Windows Firewall will expose your computer to the Internet, if no other firewall exists. The setting discussed in this section should only be used by advanced users for computer administration purposes, or if your computer is protected by another firewall.

To disable Windows Firewall

1. In **Windows Security Center** under **Manage security settings for**, click **Windows Firewall**.
2. In the **Windows Firewall** dialog box, click **Off (not recommended)**.



3. Click **OK**, then close **Security Center**, and then close **Control Panel**.

Verifying Windows Firewall General Settings Are Applied

When you verify Windows Firewall settings, some tabs and options in the Windows Firewall dialog box might be unavailable depending on your configuration.

To verify Windows Firewall General settings are applied

1. From the Windows XP SP2 desktop, click **Start**, and then click **Control Panel**.
2. Under **Pick a category**, click **Security Center**.
3. Under **Manage security settings for**, click **Windows Firewall**.
4. Click the **General** tab and verify that your configuration is applied to Windows Firewall, and then click **OK**.

Configuring Windows Firewall Exceptions

Because Windows Firewall restricts communication between your computer and the Internet, you might have to adjust settings for some programs that require an open connection to the Internet. For any program on the Windows Firewall exceptions list, Windows opens the necessary connection automatically, regardless of where the application is run from.

Note: The firewall designates that the connection is only open while the program is waiting to receive the connection. All other times the port is closed.

The firewall designates that the port is only open while the program is waiting to receive the connection. All other times the port is closed and your computer is secure from unsolicited requests.

To help minimize your security risk, if you must allow exceptions:

- Only allow an exception when you really need it.
- Never allow an exception for a program that you don't recognize.
- Remove an exception as soon as you no longer need it.

To enable Windows Firewall Exceptions, you must perform these tasks:

- Configure notifications
- Add Exceptions for Programs
- Add Exceptions for Ports
- Edit Exceptions
- Verify Windows Firewall Exceptions settings are applied

Requirements to perform this task

- Credentials: You must be logged on as a member of the local Administrators group.

Configure Notifications

By default, Windows Firewall displays a notification dialog box, similar to the one that appears in Figure 6, whenever it blocks a program.

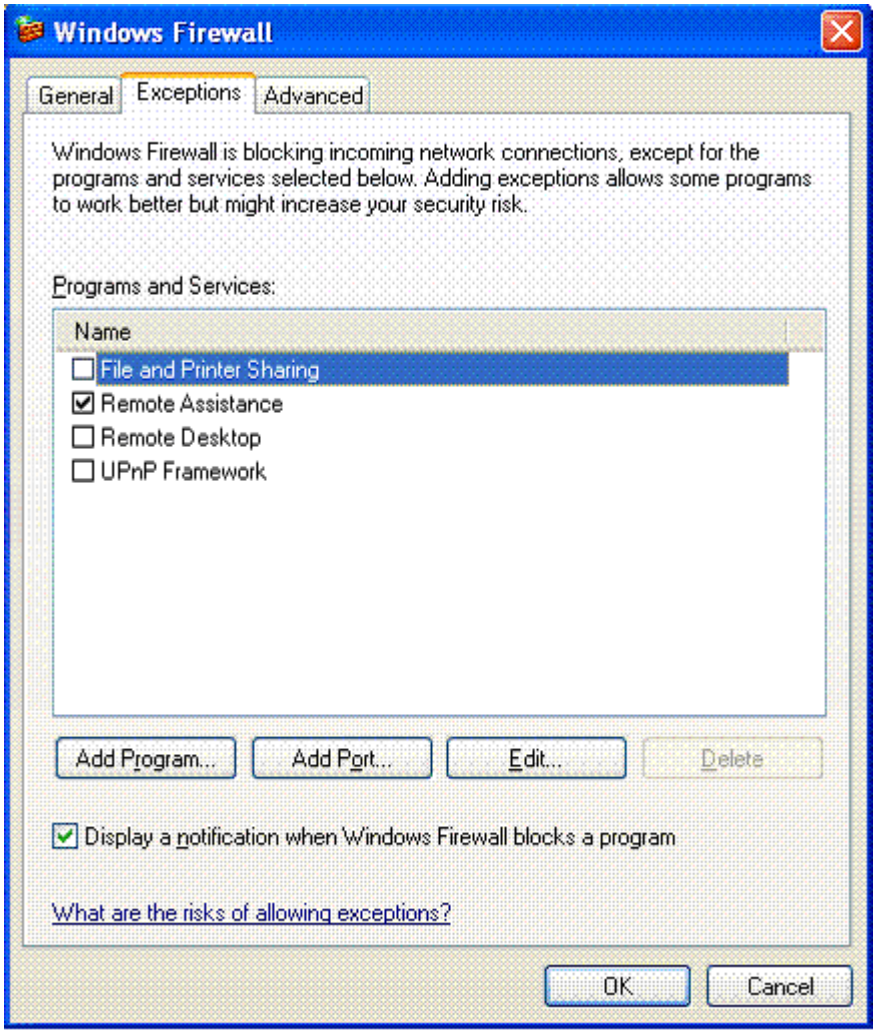
The dialog indicates which program has been blocked and allows you to choose whether to allow this program. The options available are:

- **Keep Blocking**. Use this option so the program won't connect without your permission.
- **Unblock**. Use this option to place the program in the Windows Firewall exceptions list.
- **Ask me later**. Use this option if you do not know whether to block or to unblock the program. This option keeps the program blocked for greater security. This message appears again the next time that this program is blocked.

Complete these steps if you choose not to receive any notifications.

To configure notifications

1. In **Security Center**, under **Manage security settings for**, click **Windows Firewall**.
2. On the **Exceptions** tab, either clear or select **Display a notification when Windows Firewall blocks a program**.



3. Click **OK**.

Configure Exceptions for Programs

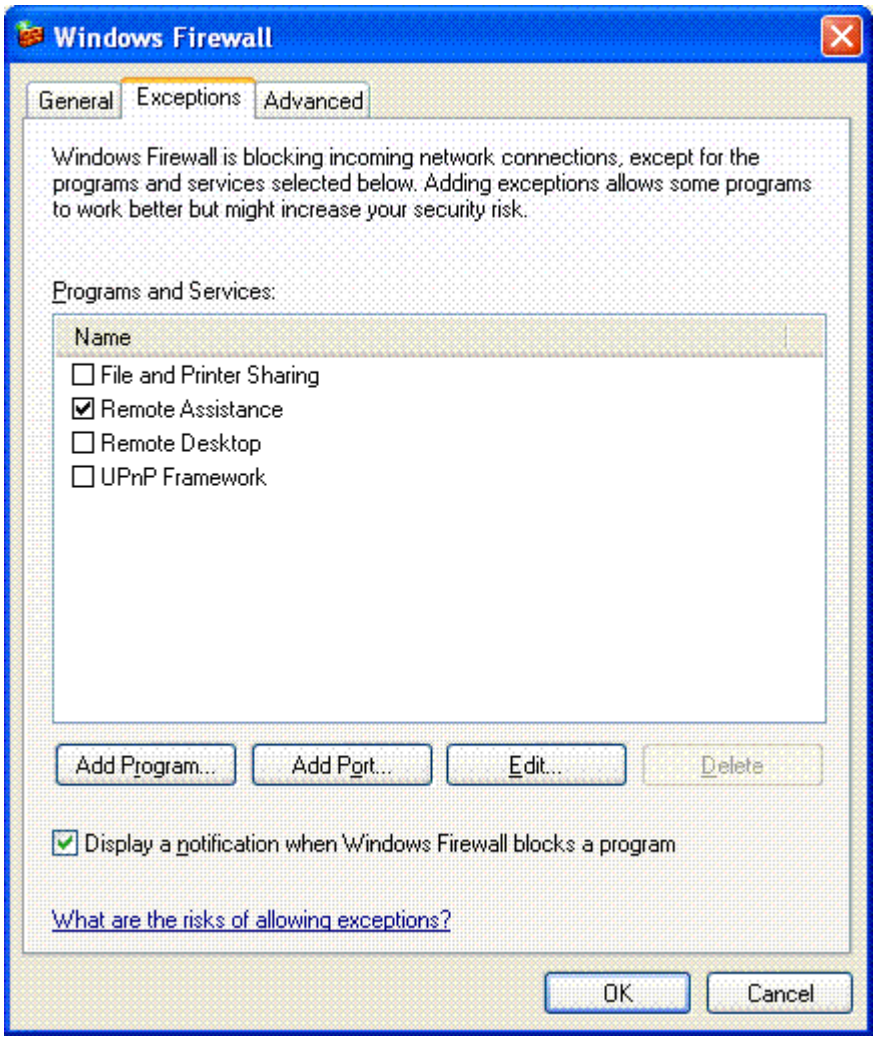
You can configure exceptions to the default firewall setting, to allow unsolicited requests to connect to a program on your computer. You can also be more specific about where the request is allowed to initiate from by changing its scope.

A scope is an optional configuration that enables you to specify which computers can use the excepted program on your computer. For home and small office networks, Microsoft recommends that you set the scope to the local network only where you can do this. If you set the scope to the local network only, computers on the same network can connect to the program on the computer. However, traffic that originates from a remote computer is not allowed.

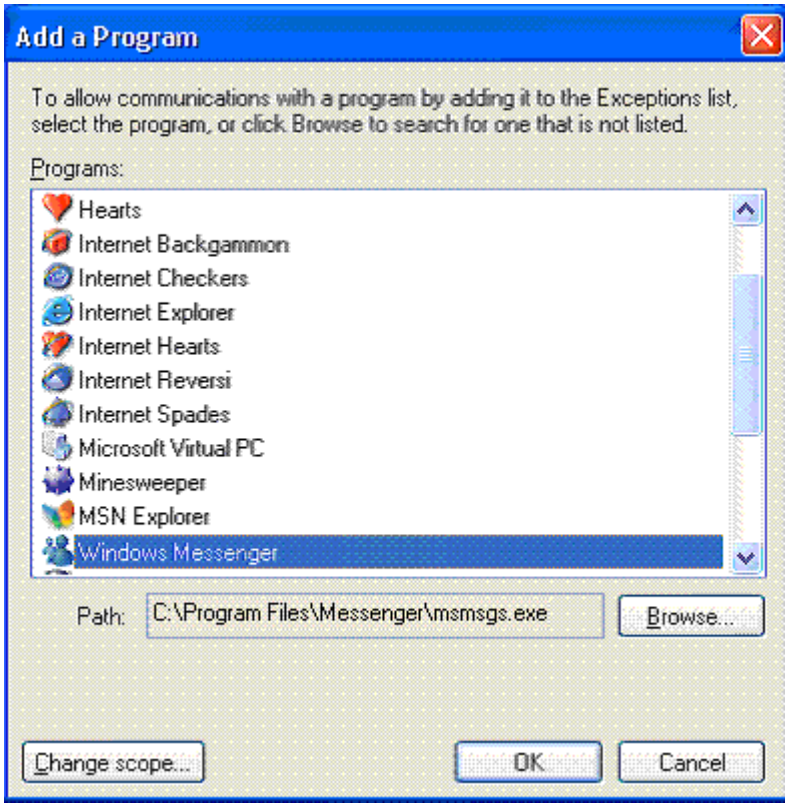
If the program that you want to allow an exception for is not listed on the Exceptions tab, you can search for it in the list of programs on your computer and then add it.

To configure Windows Firewall Program Exceptions

1. In the **Windows Firewall** dialog box, click the **Exceptions** tab.



2. Under **Programs and Services**, select the check box for the program or service that you want to allow, and then click **OK**.
3. If the program or service that you want to allow is not listed, click **Add Program**.

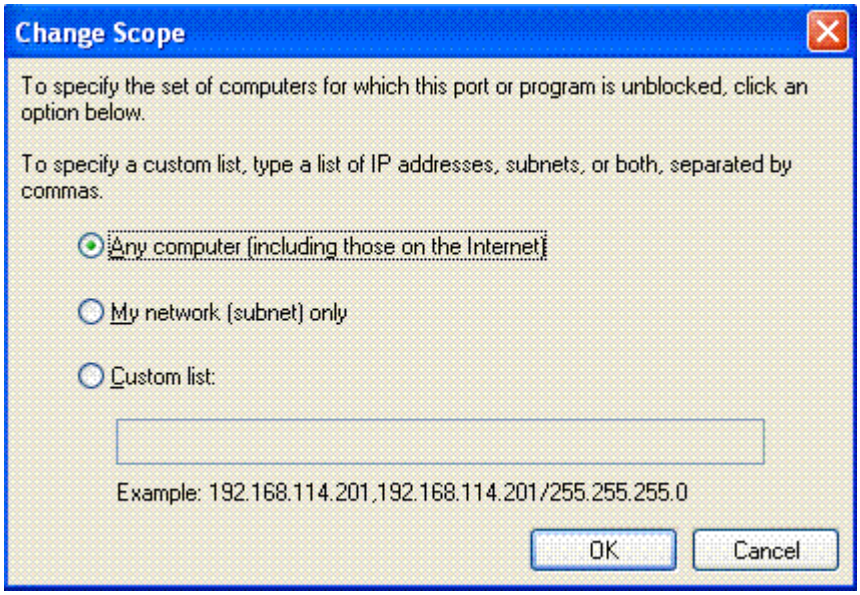


4. From the list, scroll to the program that you want to add, select it, and then click **OK**.

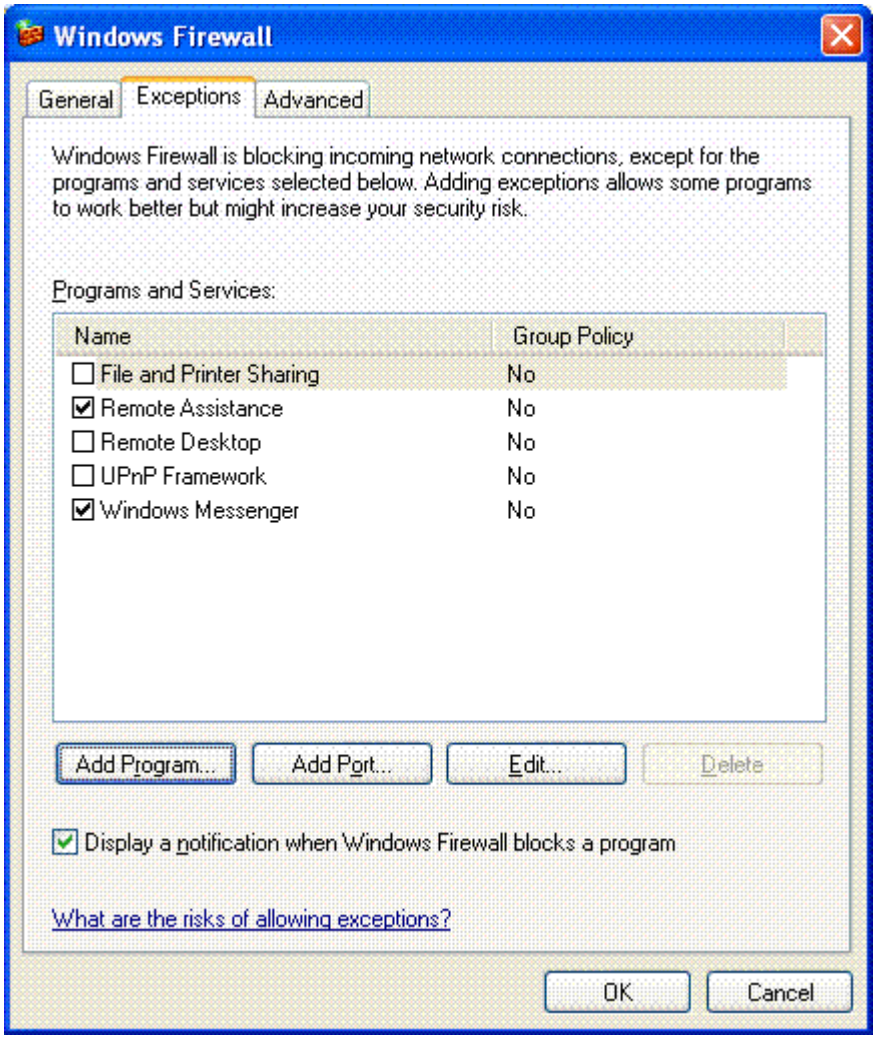
   Note: If the program that you wish to add is not listed in the Add a Program box, click **Browse**. For the steps to browse to a program, skip to step 8 in this procedure.

5. Click **Change scope**.

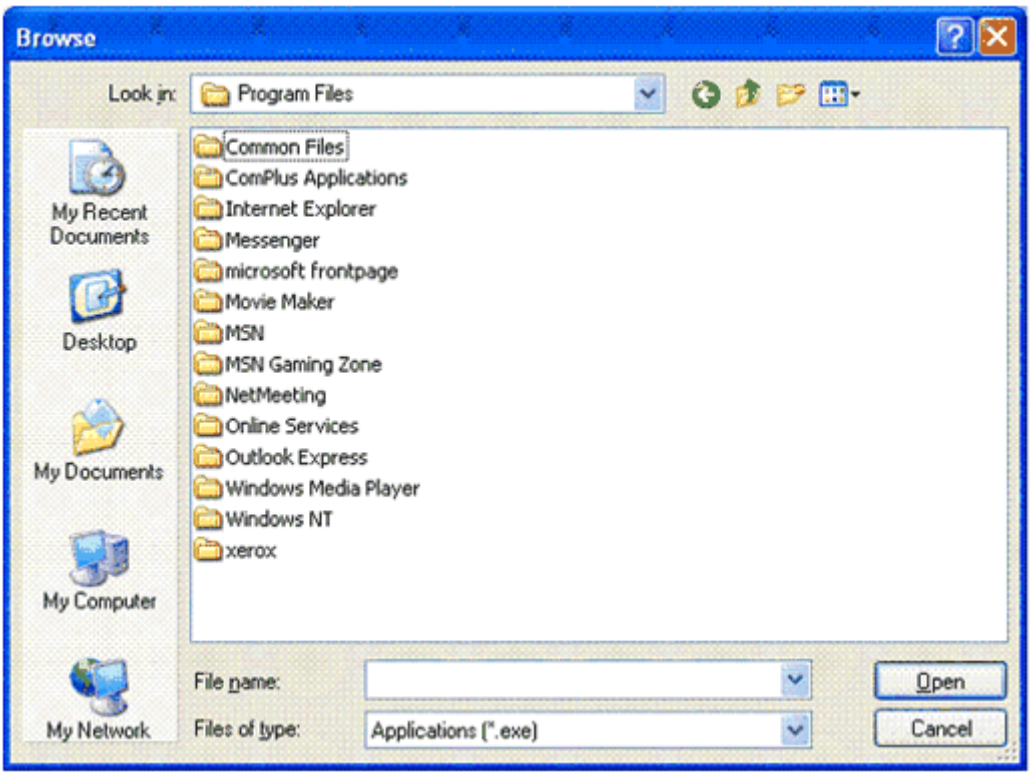
   Note: Change scope is an optional configuration that enables you to specify which computers can use the excepted program on your computer. If you do not need to set a scope, you can skip to step 7.



6. Specify the set of computers for which this program is unblocked, and then click **OK**.

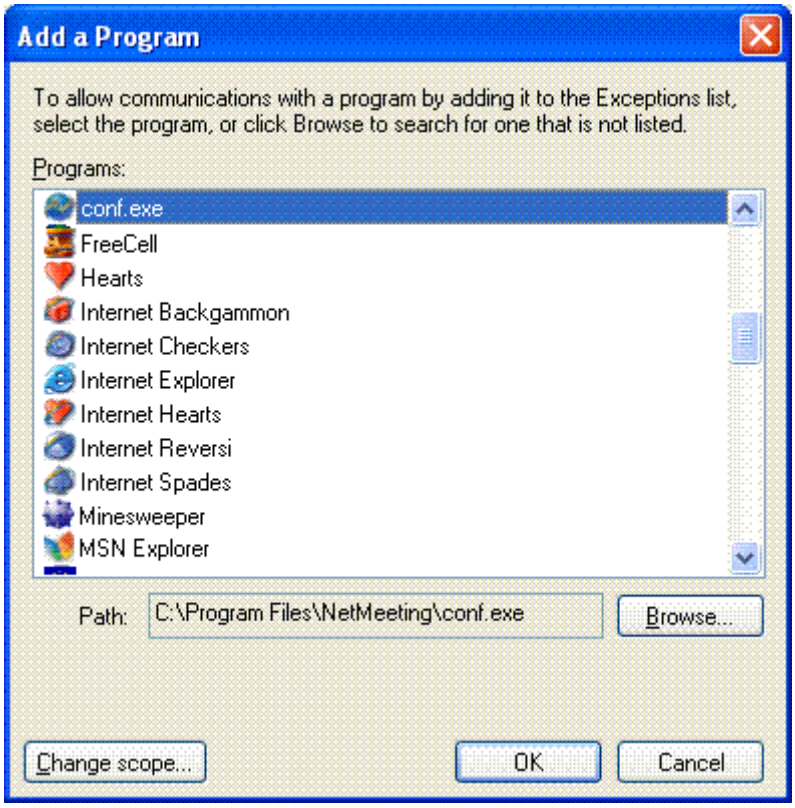


7. Click **OK**.
8. If the program that you want to allow is not listed in the **Add a Program** dialog box, click **Add Program** and then click **Browse**.

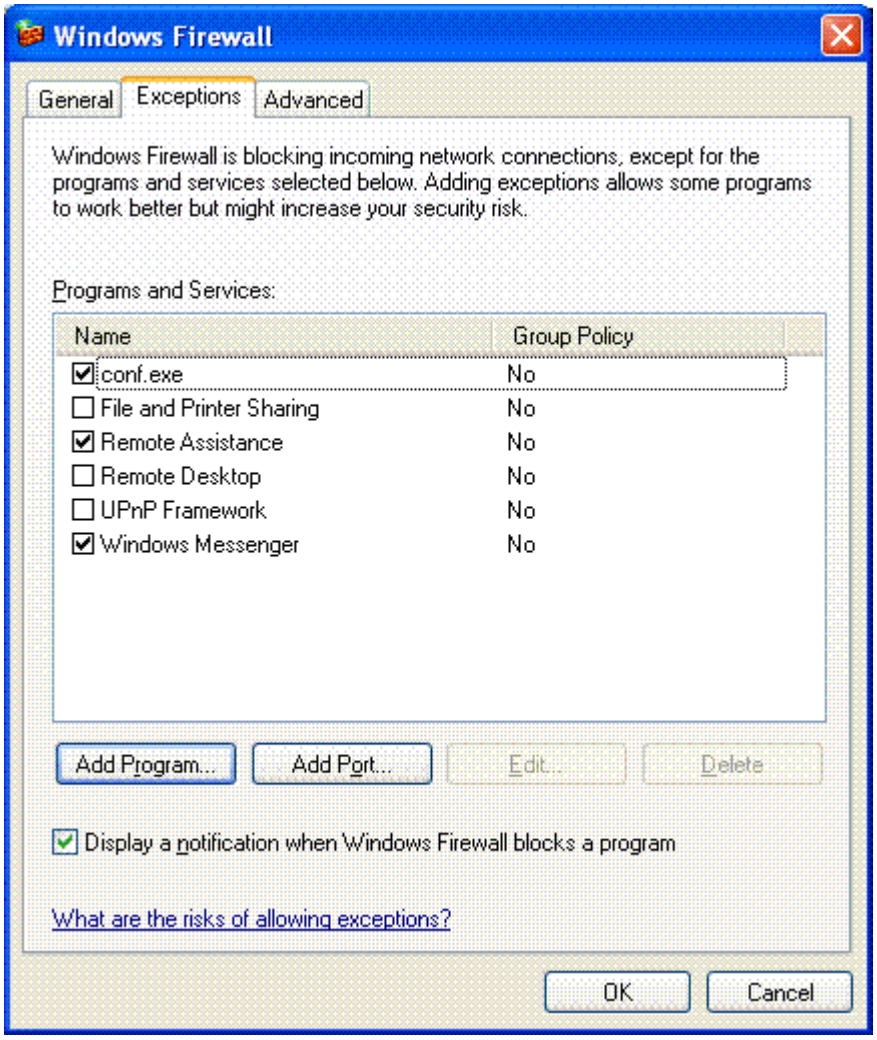


Programs are usually stored in the Program Files folder on your computer.

9. Browse to the program that you want to add, select it and then click **Open**.



10. Click **OK**. The program will now appear in the **Add a Program** dialog box, under **Programs**.



11. Click **OK**.

Configure Exceptions for Ports

You can configure exceptions to the default Windows Firewall settings, to allow unsolicited requests to connect to a port. You can also be more specific about where the request is allowed to initiate by defining scopes.

A port is like a small door in the firewall that allows communications to pass through. You must specify the exact port number to open but remember to close it again as soon as you have finished using it or else it will remain open indefinitely.

A scope is an optional configuration that enables you to specify which computers can use the excepted port on your computer. For home and small office networks, Microsoft recommends that you set the scope to the local network only where you can do this. If you set the scope to the local network only, computers on the same network can connect

to the port on the computer. However, traffic that originates from a remote computer is not allowed.

It is better to add a program than it is to open a port because:

- You can do it easily.
- You do not have to know which port number to use.
- The firewall designates that the port is only open while the program waits to receive the connection. All other times the port is closed and your computer is secure from unsolicited requests. However, when a user opens a port manually, that port remains open even while the program is not using it.

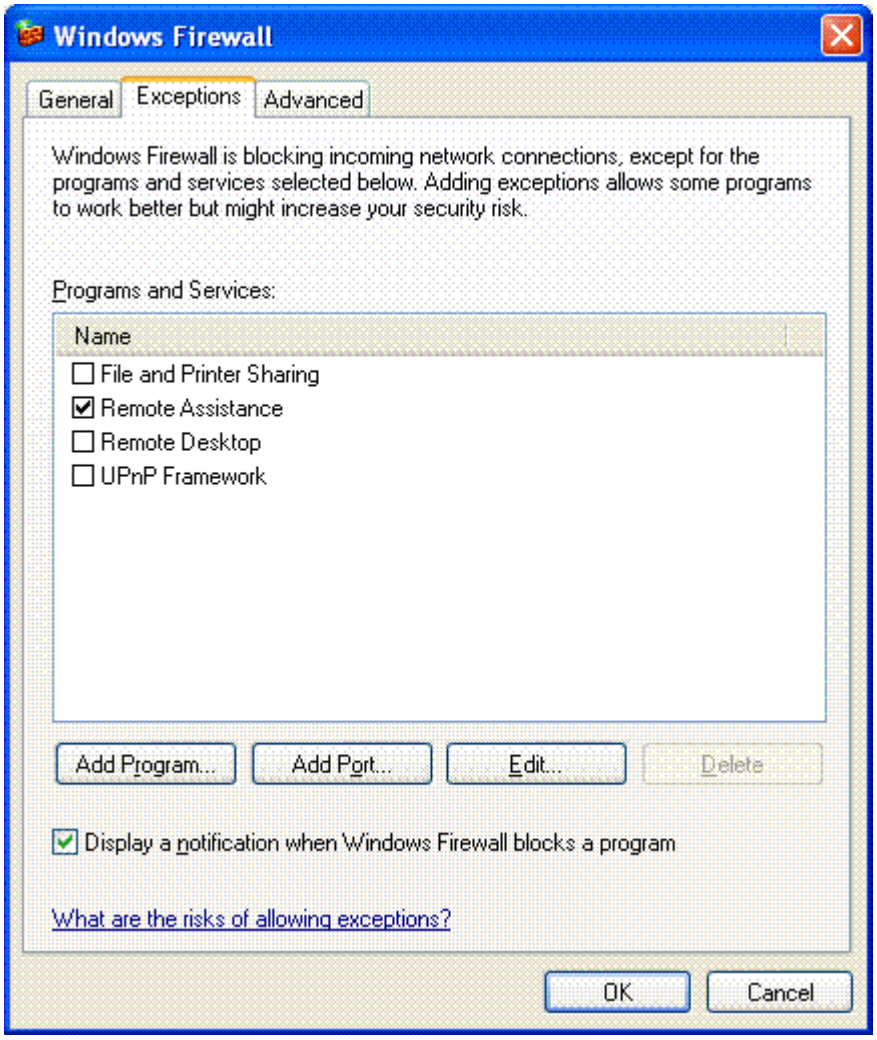
Only advanced users should open ports for, and configure the scope of, individual connections. This restriction minimizes opportunities for intruders to connect to a computer or network.

Note: For more information about ports, see the following:

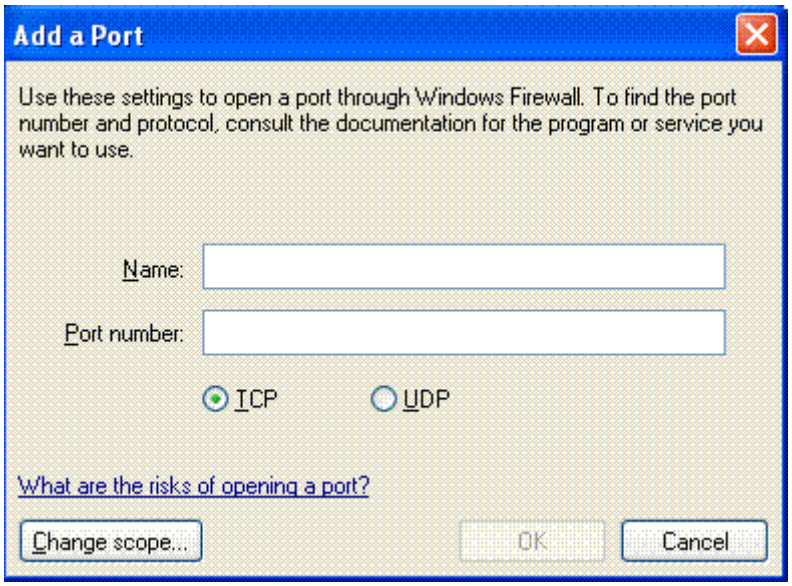
- Microsoft Knowledge Base article 842242 on the Microsoft Help and Support Web site at: http://go.microsoft.com/fwlink/?linkid=36364

To configure Windows Firewall Port Exceptions

1. In the **Windows Firewall** dialog box, click the **Exceptions** tab.

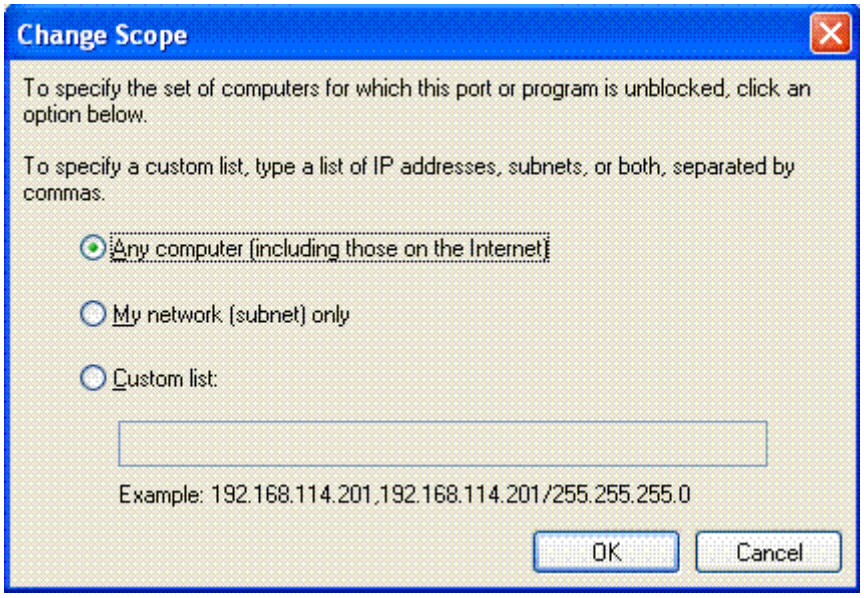


2. Click **Add Port**.



3. Type a name for the port you want to allow, type the port number, then indicate whether this is a TCP or UDP port by clicking **TCP** or **UDP**.
4. Click **Change scope**.

   Note: Change scope is an optional configuration that enables you to specify which computers can use the excepted program on your computer. If you do not need to set a scope, you can skip to step 6.



5. Specify the set of computers for which this port is unblocked, and then click **OK**.
6. Click **OK**.

Edit Exceptions

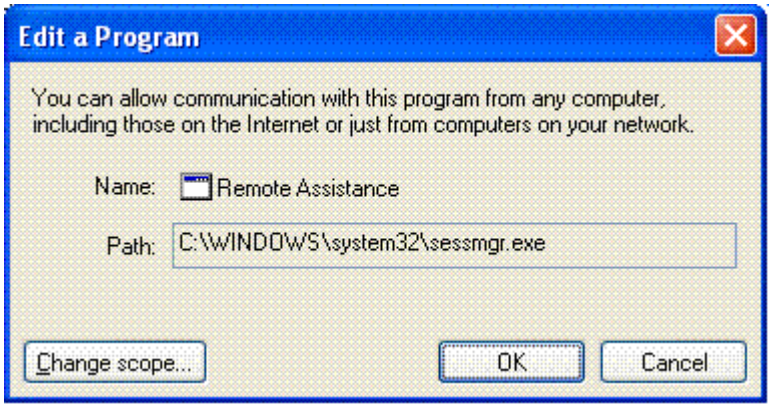
You can edit any program or port exceptions on the Windows Firewall Exceptions tab.

To edit exceptions

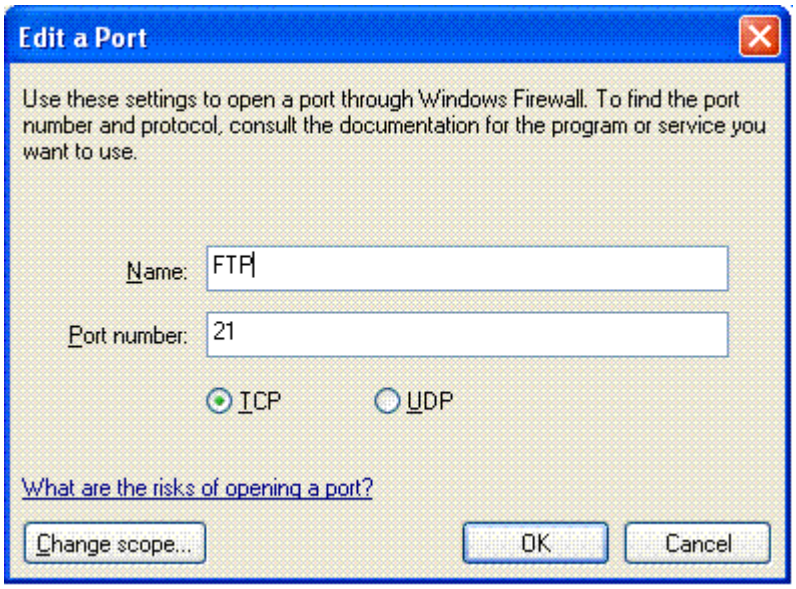
1. In the **Windows Firewall** dialog box, click the **Exceptions** tab.
2. Under **Programs or Services**, select a program, a port, or a service exception and then click **Edit**.

   If you chose to edit a program, in the **Edit a Program** dialog box, click **Change scope**, select the options that you require and then click **OK** twice.

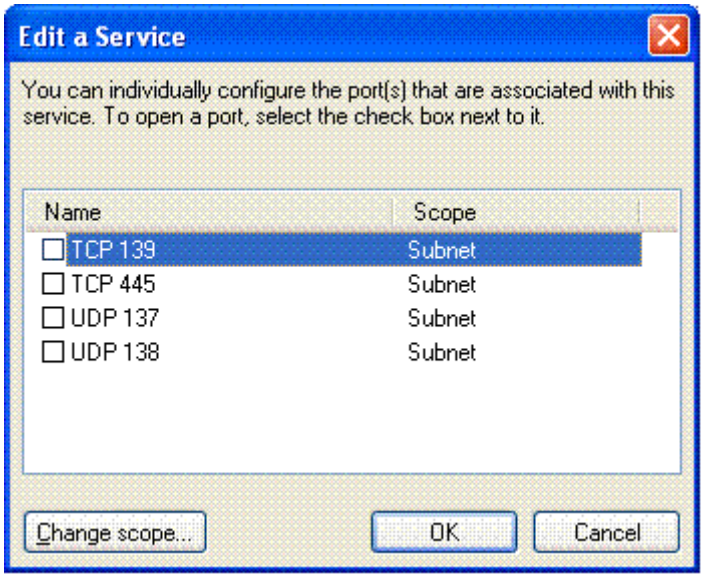
   Note: Change scope is an optional configuration that enables you to specify which computers can use the excepted program on your computer.



If you select a port in the **Edit a Port** dialog box make the necessary edits and then click **OK**.



If you select a service in the **Edit a Service** dialog box select any ports associated with the service that you wish to open and then click **OK**.



Verifying Windows Firewall Exceptions Settings Are Applied

When you verify Windows Firewall settings, some tabs and options in the Windows Firewall dialog box might be unavailable depending on your configuration.

To verify Windows Firewall Exceptions settings are applied

1. From the Windows XP SP2 desktop, click **Start**, and then click **Control Panel**.
2. Under **Pick a category**, click **Security Center**.
3. Under **Manage security settings for**, click **Windows Firewall**.
4. Click the **Exceptions** tab and verify that your configuration is applied to Windows Firewall.

Configuring Windows Firewall Advanced Settings

On the Advanced tab in Windows Firewall there are several settings that you can configure. These settings are divided into four sections:

- **Network Connection Settings**. Advanced users modify these to define Windows Firewall settings for individual hardware connections that are available on a computer. For example, you could configure Windows Firewall to block connections only if they were attempted by a device attached to a USB port, and allow connections via your network card. The standard configuration on a standalone computer is for the Firewall to have the same settings for every hardware connection available.
- **Security Logging**. Advanced users can create a record of successful connections and unsuccessful connection attempts across Windows Firewall. When you choose to log unsuccessful attempts, information is collected about each connection attempt that is detected and blocked by Windows Firewall.

When you choose to log successful connections, information is collected about each successful connection that travels across the firewall. Together these create a log of all the transactions going into and out of the computers environment.

- **ICMP**. Advanced users can select which parts of Internet Control Message Protocol (ICMP) can be used through Windows Firewall. To configure these settings requires in-depth knowledge of ICMP mechanisms. Incorrect configuration of ICMP can seriously affect your computers security.
- **Default Settings**. Users with Administrator rights can use this option to restore Windows Firewall settings to their original defaults settings.

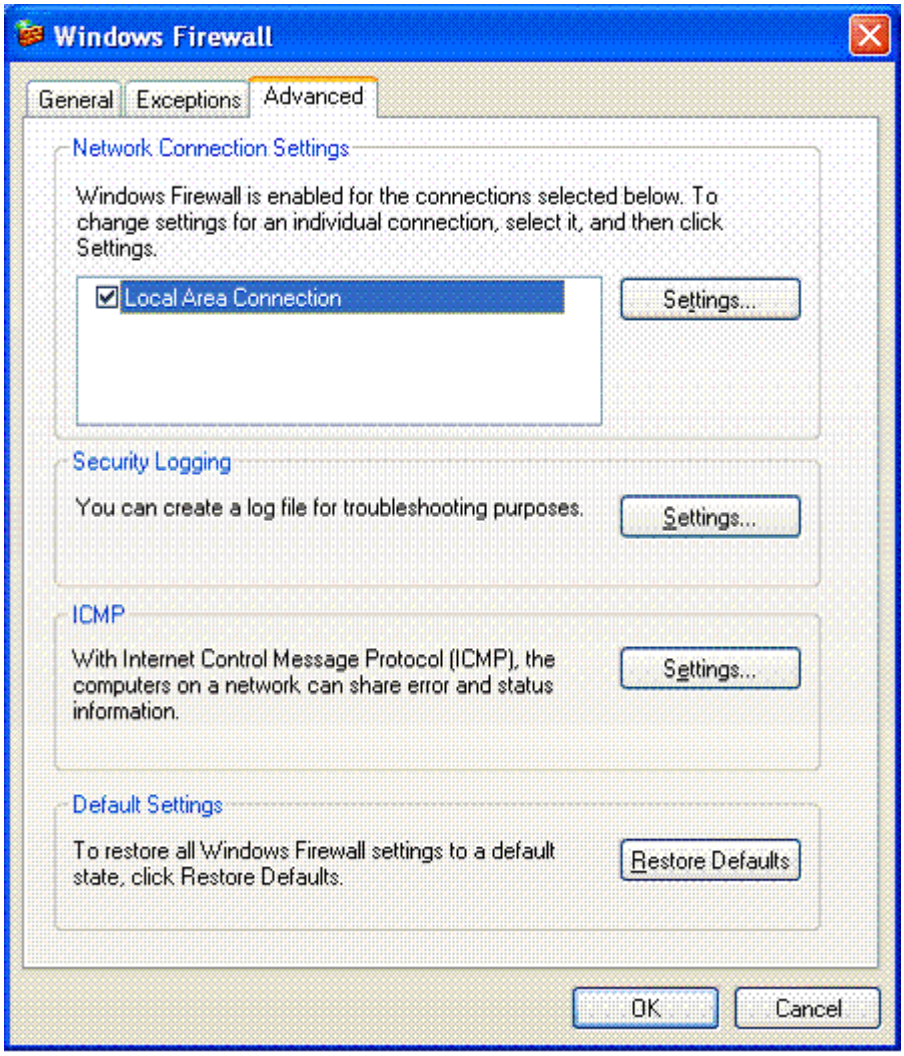
Requirements to perform this task

- Credentials: You must log on as a member of the local Administrators group and have Windows Firewall open.

Open Windows Firewall Advanced Settings

To open the Windows Firewall Advanced Settings

1. In the **Windows Firewall** dialog box, click the **Advanced** tab.



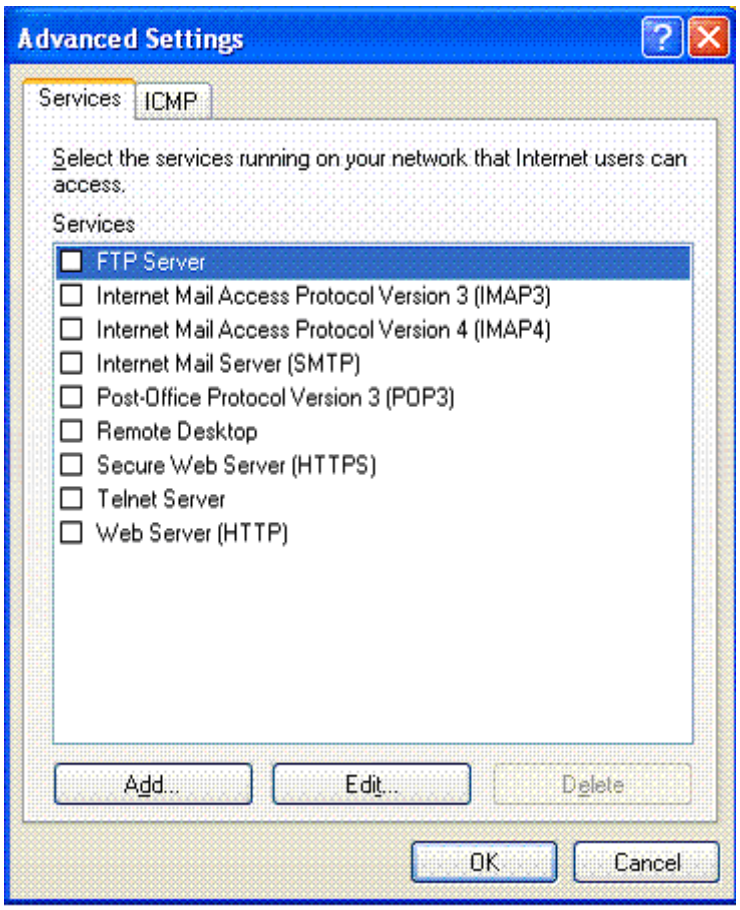
Configure Network Connection Settings

The default configuration for Windows Firewall is enabled for all connections. You can change this for individual connections, and you can set a different configuration for each connection.

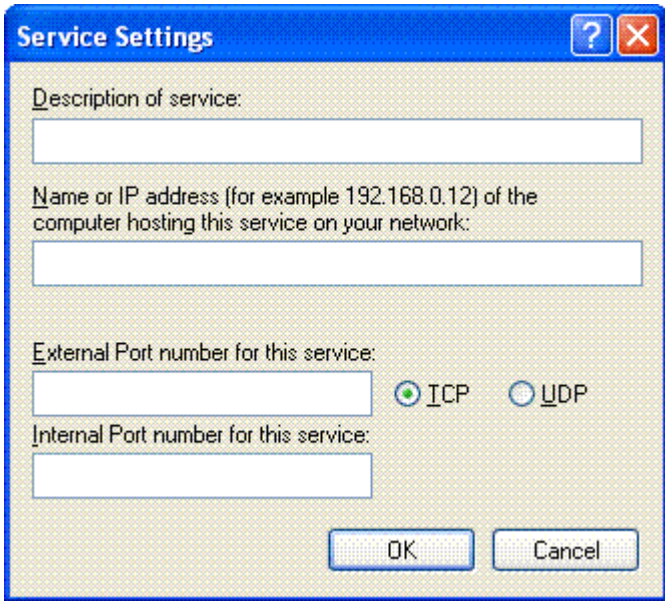
For example, you might wish to disable email on your Internet connection, but allow email on your Local Area Connection.

To use Network Connection settings

1. In **Windows Firewall**, on the **Advanced** tab, under **Network Connection Settings**, clear all connections that you do not require Windows Firewall to protect.
2. Click to select the particular connection that you wish to change from the default firewall settings, and then click **Settings**.



3. Select or deselect the particular service that you wish to enable or disable for this connection.
4. If the service you wish to enable for this connection is not displayed, click **Add**.



5. Type the specific connection details into each of the fields for the service that you wish to enable, and then click **OK**.

   Note: For each service, you must supply a description for the service, the name or IP Address of the computer that hosts the service, and the TCP or UDP internal and external ports used by the service.

Configure Security Logging Settings

Windows Firewall can keep a log of successful connections that go through the firewall and any connections that are blocked.

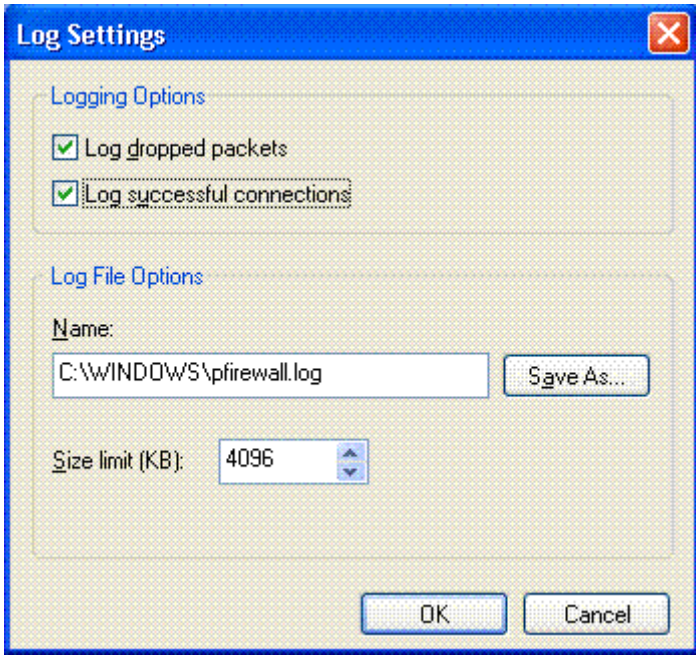
When you choose to log dropped packets, information is collected about each attempt to cross the firewall that is detected and blocked. When you choose to log successful connections, information is collected about each successful connection that travels across the firewall. For example, when your computer successfully connects to a Web site using a Web browser, that connection is recorded in the log.

The security log has two sections:

- **Header**. This displays information about the version of the security log and the fields that are available to enter information into.
- **Body**. This is the complete report of all of the information gathered and recorded about the traffic across, or attempts to cross the firewall. The body of the security log is a dynamic list, which displays new data entries at the bottom of the log.

To configure Security Logging settings

1. In **Windows Firewall**, on the **Advanced** tab, under **Security Logging**, click **Settings**.



2. In the **Log Settings** dialog box, click **Log dropped packets**, to record all the connection attempts rejected by your firewall, and **Log successful connections**, to record all the connection attempts allowed by your firewall.
3. Type a path and name for your log, (pfirewall.log is the default).

   Note: You must ensure that you specify a secure location for your log to prevent any deliberate or accidental modification.

4. Configure a size limit, such as 4096KB, to ensure that your log does not grow to an unmanageable size, and then click **OK**.

   Note: When your log reaches the size limit, it is renamed by having .old added to the end of the log name. A new log file is created with the original log name and logging continues.

Configure ICMP Settings

The ICMP is used in networks to diagnose many network problems. For example, the ping utility uses ICMP echo request and response messages to test connectivity between computers.

Note: For more information about ICMP, see the following:

- "Internet Control Message Protocol (ICMP)" on the Microsoft Windows XP Web site at http://go.microsoft.com/fwlink/?linkid=35499

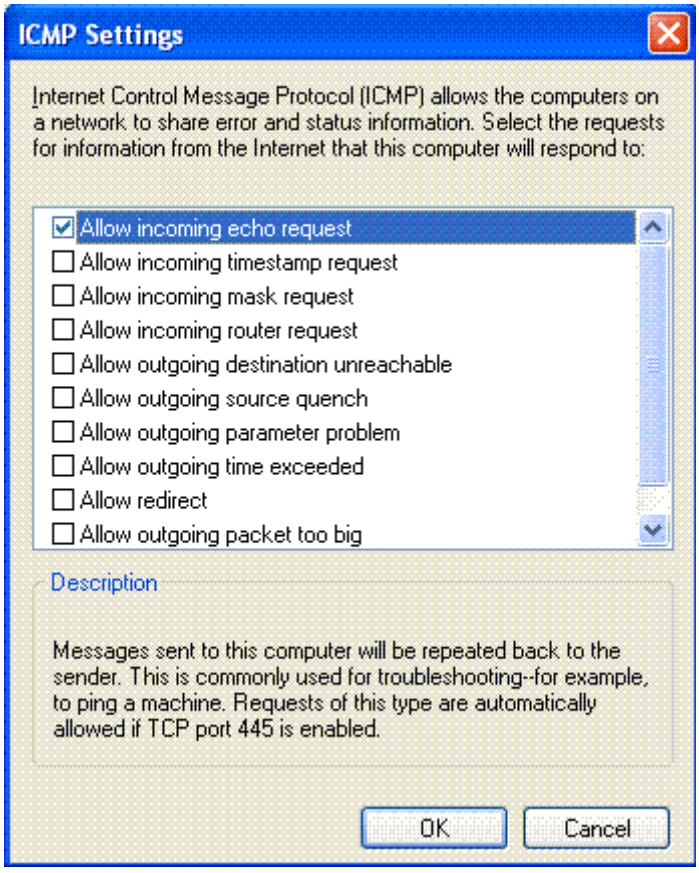
Windows XP SP2 is not capable of discovering whether the ICMP packets are being used for a genuine test or are being used for malicious purposes. This is another reason not to change these settings unless you are an advanced user.

With the ICMP settings in Windows Firewall, you can choose which control messages your computer responds to.

Note: When you enable File and Printer Sharing on your Exceptions tab, the Allow incoming echo request option is also enabled.

To configure ICMP options

1. In **Windows Firewall** on the **Advanced** tab, under **ICMP**, click **Settings**.



2. Select the appropriate requests that you want your computer to respond to and then click **OK**.

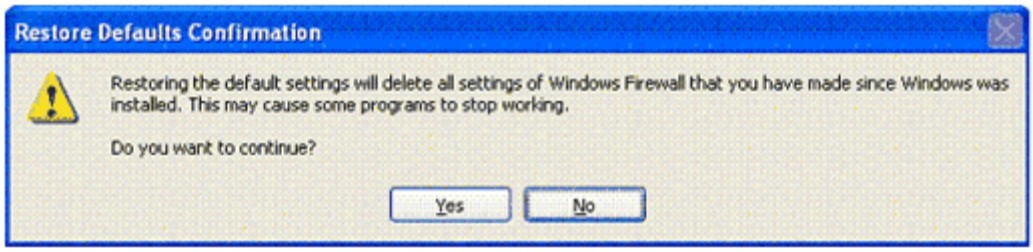
Restore Windows Firewall Default Settings

This is a configuration option that allows you to restore all of the Windows Firewall settings to their original defaults. This is important because Windows Firewall might

have been configured to allow incoming connections, either through adding applications or ports to the Windows Firewall exception list, that are no longer necessary.

To use Restore Defaults

1. In **Windows Firewall**, on the **Advanced** tab, in the **Default Settings** section, click **Restore Defaults**.



2. In the **Restore Defaults Confirmation** dialog box, click **Yes**.
3. Click **OK** to close Windows Firewall settings.

Verifying Windows Firewall Advanced Settings Are Applied

When you verify Windows Firewall settings, some tabs and options in the Windows Firewall dialog box might be unavailable depending on your configuration.

To verify Windows Firewall settings are applied

1. From the Windows XP SP2, click **Start**, and then click **Control Panel**.
2. Under **Pick a category**, click **Security Center**.
3. Under **Manage security settings for**, click **Windows Firewall**.
4. Click the **Advanced** tab and verify that your configuration is applied to Windows Firewall.

Related Information

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

- "Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2" on the Microsoft Download Center Web site at http://go.microsoft.com/fwlink/?linkid=35303
- "The Cable Guy - February 2004 - Manually Configuring Windows Firewall in Windows XP Service Pack 2" on the Microsoft TechNet Web site at http://go.microsoft.com/fwlink/?linkid=35304
- "Understanding Windows Firewall" on the Microsoft Windows XP Web site at http://go.microsoft.com/fwlink/?linkid=35305

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

- "Windows XP Security Guide v2 updated for Service Pack 2" on the Microsoft Download Center Web site at http://go.microsoft.com/fwlink/?linkid=35309
- "Windows XP Security Guide Appendix A: Additional Guidance for Windows XP Service Pack 2" on the Microsoft TechNet Web site at http://go.microsoft.com/fwlink/?linkid=35465

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

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

Send feedback to Microsoft