Security checklist for Windows 7

Use this checklist to make sure you're taking advantage of all the ways that Windows can help keep your computer as secure and safe as possible.

Action Center

Use Action Center to make sure your firewall is on, your antivirus software is up to date, and your computer is set to install updates automatically. For more information, see How does Action Center check for problems?

How does Action Center check for problems?

Action Center checks several security and maintenance-related items of your computer that help indicate your computer's overall performance.

When the status of a monitored item changes (for example, your antivirus software becomes out of date) Action Center notifies you with a message in the notification area on the taskbar, the status of the item in Action Center changes color to reflect the severity of the message, and an action is recommended.

To change which items Action Center checks:

1. Open Action Center by clicking the Start button, clicking Control Panel, and then, under System and Security, clicking Review your computer's status.
2. Click Change Action Center settings.
3. Select a check box to make Action Center check an item for changes or problems, or clear a check box to stop checking the item.
4. Click OK.

If you prefer to keep track of an item yourself (for example, you use a backup program other than the one included in Windows, or you back up your files manually), and you don't want to see notifications about its status, you can turn off notifications for the item.

When you clear the check box for an item on the Change Action Center settings page, you won’t receive any messages, and you won’t see the item's status in Action Center. We recommend checking the status of all items listed, since many can help warn you about security issues.

However, if you decide to turn off messages for an item, you can always turn messages back on. On the Change Action Center settings page, select the check box for the item and then click OK. Or, click the appropriate Turn on messages link next to the item on the main page.

Note

To change how solutions to problems appear in Action Center, click Change Action Center settings, and then click Problem reporting settings. On the Change problem reporting settings page, choose how much information is sent, and how often to check for new solutions, and then click OK.

Windows Defender

Use Windows Defender to help prevent spyware and other potentially unwanted software from being installed on your computer without your knowledge. For more information, see Using Windows Defender.

Using Windows Defender

Windows Defender is antispyware software that's included with Windows and runs automatically when it's turned on. Using antispyware software can help protect your computer against spyware and other potentially unwanted software. Spyware can be installed on your computer without your knowledge any time you connect to the Internet, and it can infect your computer when you install some programs using a CD, DVD, or other removable media. Spyware can also be programmed to run at unexpected times, not just when it's installed.

Windows Defender offers two ways to help keep spyware from infecting your computer:

- Real-time protection. Windows Defender alerts you when spyware attempts to install itself or to run on your computer. It also alerts you when programs attempt to change important Windows settings.
- Scanning options. You can use Windows Defender to scan for spyware that might be installed on your computer, to schedule scans on a regular basis, and to automatically remove anything that's detected during a scan.

When you use Windows Defender, it's important to have up-to-date definitions. Definitions are files that act like an ever-growing encyclopedia of potential software threats. Windows Defender uses definitions to alert you to potential risks if it determines that software detected is spyware or other potentially unwanted software. To help keep your definitions up to date, Windows Defender works with Windows Update to automatically install new definitions as they're released. You can also set Windows Defender to check online for updated definitions before scanning. For information about keeping your definitions up to date and how to manually download the latest definitions, see Keep Windows Defender definitions up to date.

- Open Windows Defender by clicking the Start button . In the search box, type Defender, and then, in the list of results, click Windows Defender.

User Account Control

User Account Control asks for your permission before installing software or opening certain kinds of programs that could potentially harm your computer or make it vulnerable to security threats. For more information, see What is User Account Control?

What is User Account Control?

User Account Control (UAC) is a feature in Windows that can help you stay in control of your computer by informing you when a program makes a change that requires administrator-level permission. UAC works by adjusting the permission level of your user account. If you're doing tasks that can be done as a standard user, such as reading e-mail, listening to music, or creating documents, you have the permissions of a standard user—even if you're logged on as an administrator.

When changes are going to be made to your computer that require administrator-level permission, UAC notifies you. If you are an administrator, you can click Yes to continue. If you are not an administrator, someone with an administrator account on the computer will have to enter their password for you to continue. If you give permission, you are temporarily given the rights of an administrator to complete the task and then your permissions are returned back to that of a standard user. This makes it so that even if you're using an administrator account, changes cannot be made to your computer without you knowing about it, which can help prevent malicious software (malware) and spyware from being installed on or making changes to your computer.

When your permission or password is needed to complete a task, UAC will notify you with one of four different types of dialog boxes. The table below describes the different types of dialog boxes used to notify you and guidance on how to respond to them.

Icon	Type	Description
🛡	A setting or feature that is part of Windows needs your permission to start.	This item has a valid digital signature that verifies that Microsoft is the publisher of this item. If you get this type of dialog box, it's usually safe to continue. If you are unsure, check the name of the program or function to decide if it's something you want to run.

Icon	Type	Description
?	A program that is not part of Windows needs your permission to start.	This program has a valid digital signature, which helps to ensure that the program is what it claims to be and verifies the identity of the publisher of the program. If you get this type of dialog box, make sure the program is the one that you want to run and that you trust the publisher.
!	A program with an unknown publisher needs your permission to start.	This program doesn't have a valid digital signature from its publisher. This doesn't necessarily indicate danger, as many older, legitimate programs lack signatures. However, you should use extra caution and only allow a program to run if you obtained it from a trusted source, such as the original CD or a publisher's website. If you are unsure, look up the name of the program on the Internet to determine if it is a known program or malicious software.
✖	You have been blocked by your system administrator from running this program.	This program has been blocked because it is known to be untrusted. To run this program, you need to contact your system administrator.

We recommend that you log on to your computer with a standard user account most of the time. You can browse the Internet, send e-mail, and use a word processor, all without an administrator account. When you want to perform an administrative task, such as installing a new program or changing a setting that will affect other users, you don't have to switch to an administrator account; Windows will prompt you for permission or an administrator password before performing the task. We also recommend that you create standard user accounts for all the people who use your computer.

In this version of Windows, you can adjust how often UAC notifies you when changes are made to your computer. If you want to be informed when any change is made to your computer, choose to always be notified.

Backup and Restore

It's important to back up your files and settings regularly so that if you get a virus or have any kind of hardware failure, you can recover your files. For more information about backing up your files, search for "back up" in Help and Support.

Windows Update

Set Windows Update to download and install the latest updates for your computer automatically. For more information, see Install Windows updates in Windows 7.

Install Windows updates in Windows 7

If you'd like Windows to install important updates as they become available, turn on automatic updating. Important updates provide significant benefits, such as improved security and reliability. You can also set Windows to automatically install recommended updates, which can address noncritical problems and help enhance your computing experience. Optional updates are not downloaded or installed automatically. To learn more about the types of updates that Microsoft publishes,

Windows Firewall

Windows Firewall can help prevent hackers and malicious software, such as viruses, from gaining access to your computer through the Internet. For more information, see Windows Firewall: recommended links.

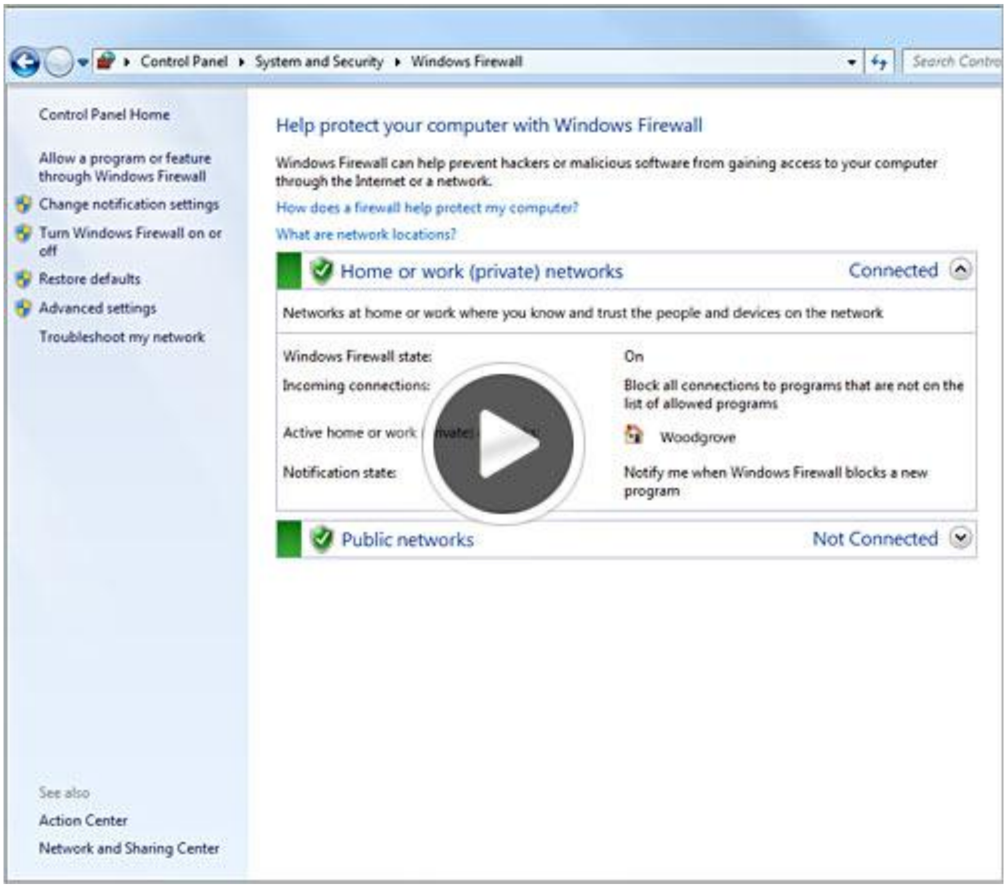
Windows Firewall: recommended links

A firewall can help prevent hackers or malicious software (such as worms) from gaining access to your computer through a network or the Internet. A firewall can also help stop your computer from sending malicious software to other computers.

Allow a program to communicate through Windows Firewall

By default, most programs are blocked by Windows Firewall to help make your computer more secure. To work properly, some programs might require you to allow them to communicate through the firewall.

Watch this video to learn how to allow a program to communicate through Windows Firewall (1:12)


Control Panel ▸ System and Security ▸ Windows Firewall
Search Contro
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks   Connected

Networks at home or work where you know and trust the people and devices on the network

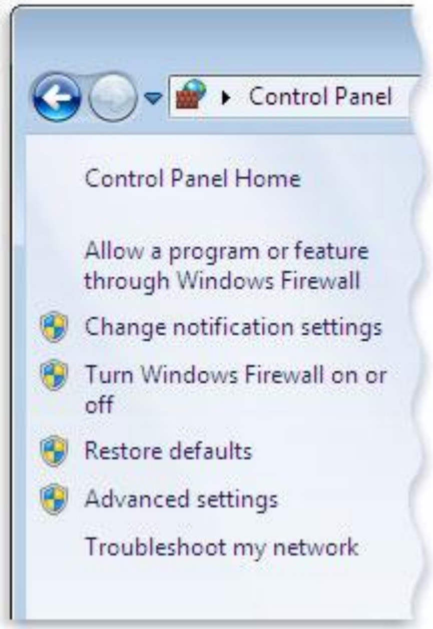
Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	Woodgrove
Notification state:	Notify me when Windows Firewall blocks a new program

Public networks   Not Connected

To allow a program to communicate through Windows Firewall

1. Open Windows Firewall by clicking the Start button, and then clicking Control Panel. In the search box, type firewall, and then click Windows Firewall.

2. In the left pane, click Allow a program or feature through Windows Firewall.


Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Left pane of Windows Firewall

3. Click Change settings. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Select the check box next to the program you want to allow, select the network locations you want to allow communication on, and then click OK.

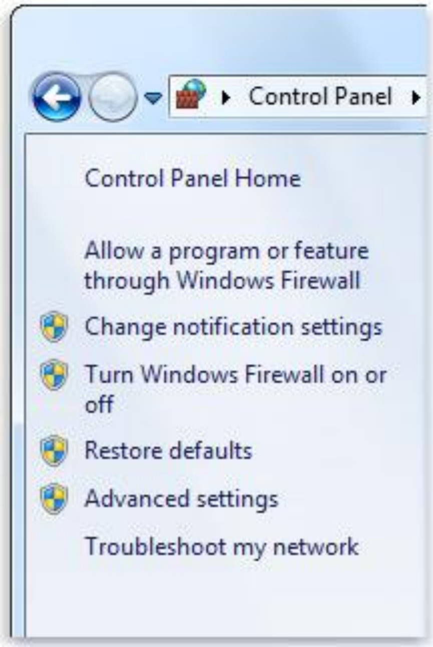
Warning

Before allowing a program through the firewall, make sure you understand the risks involved.

Turn Windows Firewall on or off

If your computer is connected to a network, network policy settings might prevent you from completing these steps.

1. Open Windows Firewall by clicking the Start button, and then clicking Control Panel. In the search box, type firewall, and then click Windows Firewall.
2. In the left pane, click Turn Windows Firewall on or off. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.

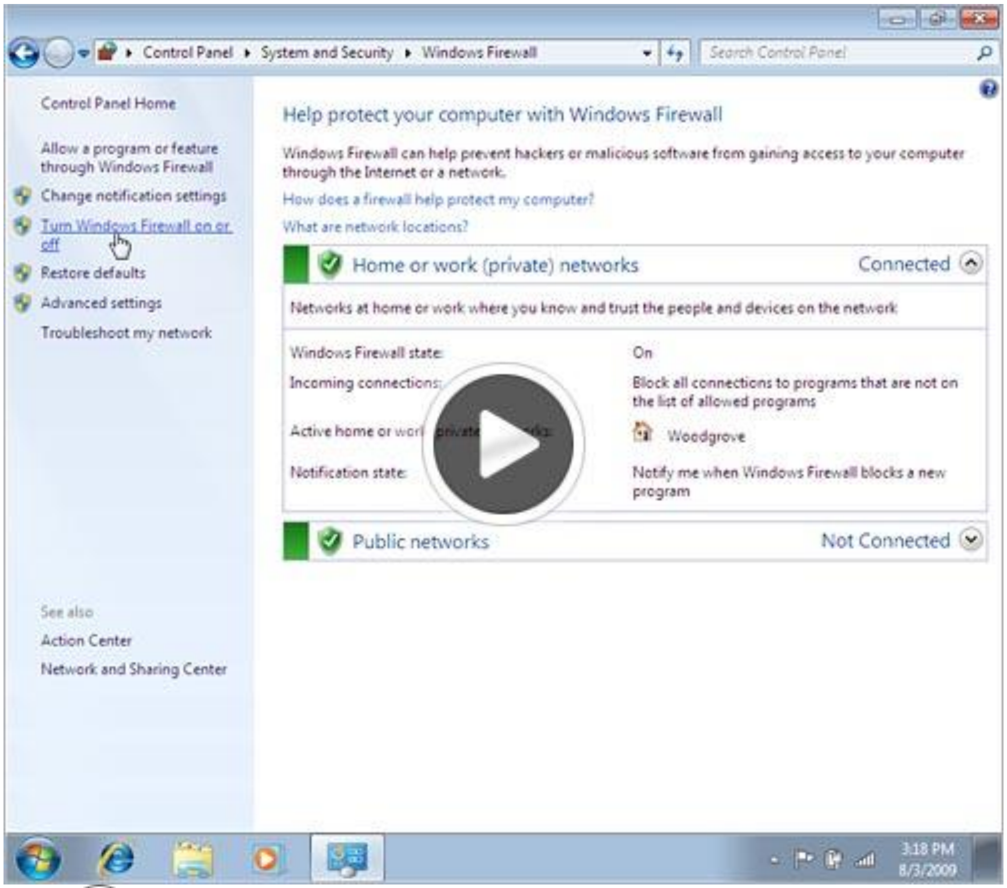

Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Turn Windows Firewall on or off link in Windows Firewall

3. Click Turn on Windows Firewall under each network location that you want to help protect, and then click OK.

   If you want the firewall to prevent all programs from communicating, including programs that you have previously allowed to communicate through the firewall, select the Block all incoming connections, including those in the list of allowed programs check box.

Watch this video to learn how to turn off Windows Firewall (1:09)


Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
3:18 PM
8/3/2009

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	Woodgrove
Notification state:	Notify me when Windows Firewall blocks a new program

Public networks — Not Connected

Warning

- You should not turn off Windows Firewall unless you have another firewall enabled. Turning off Windows Firewall might make your computer (and your network, if you have one) more vulnerable to damage from worms or hackers.
- In addition to a firewall, you also need an antivirus and anti-malware program to help protect your computer. Install Microsoft Security Essentials or another antivirus and anti-malware program, and keep it up to date. Many of these programs update automatically.

1. Open Windows Firewall by clicking the Start button, and then clicking Control Panel. In the search box, type firewall, and then click Windows Firewall.
2. Click Turn Windows Firewall on or off. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
3. Click Turn off Windows Firewall (not recommended) under each network location that you want to stop trying to protect, and then click OK.

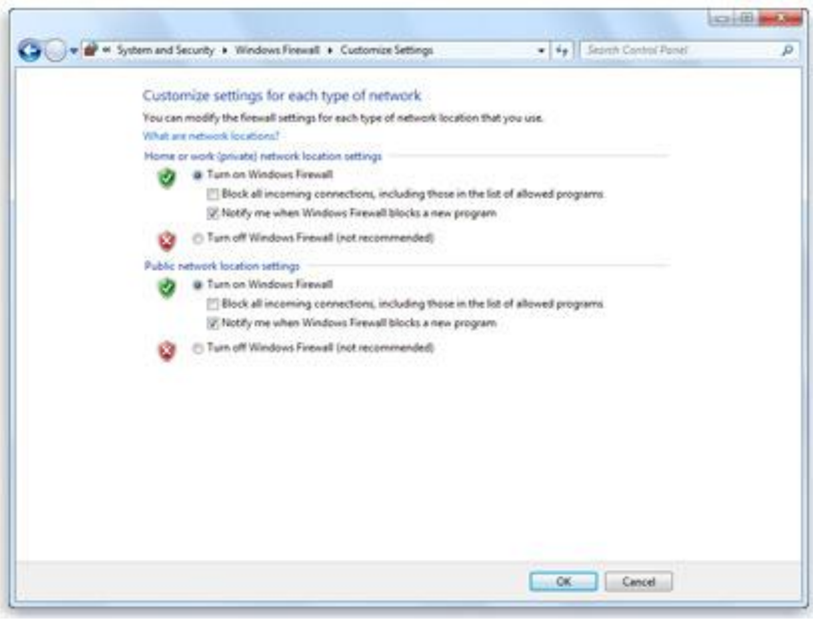
Understanding Windows Firewall settings

A firewall can help prevent hackers or malicious software (such as worms) from gaining access to your computer through a network or the Internet. A firewall can also help stop your computer from sending malicious software to other computers.

You can customize four settings for each type of network location in Windows Firewall. To find these settings, follow these steps:

1. Open Windows Firewall by clicking the Start button, and then clicking Control Panel. In the search box, type firewall, and then click Windows Firewall.
2. In the left pane, click Turn Windows Firewall on or off. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.

Here's what the settings do and when you should use them.



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Public network location settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Customize Settings dialog box

Turn on Windows Firewall

This setting is selected by default. When Windows Firewall is on, most programs are blocked from communicating through the firewall. If you want to allow a program to communicate through the firewall, you can add it to the list of allowed programs. For example, you might not be able to send photos in an instant message until you add the instant messaging program to the list of allowed programs. To add a program to the list, see Allow a program to communicate through Windows Firewall.

Block all incoming connections, including those in the list of allowed programs

This setting blocks all unsolicited attempts to connect to your computer. Use this 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 computer worm is spreading over the Internet. With this setting, you aren't notified when Windows Firewall blocks programs, and programs in the list of allowed programs are ignored.

When you block all incoming connections, you can still view most webpages, send and receive e-mail, and send and receive instant messages.

Notify me when Windows Firewall blocks a new program

If you select this check box, Windows Firewall will inform you when it blocks a new program and give you the option of unblocking that program.

Turn off Windows Firewall (not recommended)

Avoid using this setting unless you have another firewall running on your computer. Turning off Windows Firewall might make your computer (and your network, if you have one) more vulnerable to damage from hackers and malicious software.

Notes

- If some firewall settings are unavailable and your computer is connected to a domain, your system administrator might be controlling these settings through Group Policy.

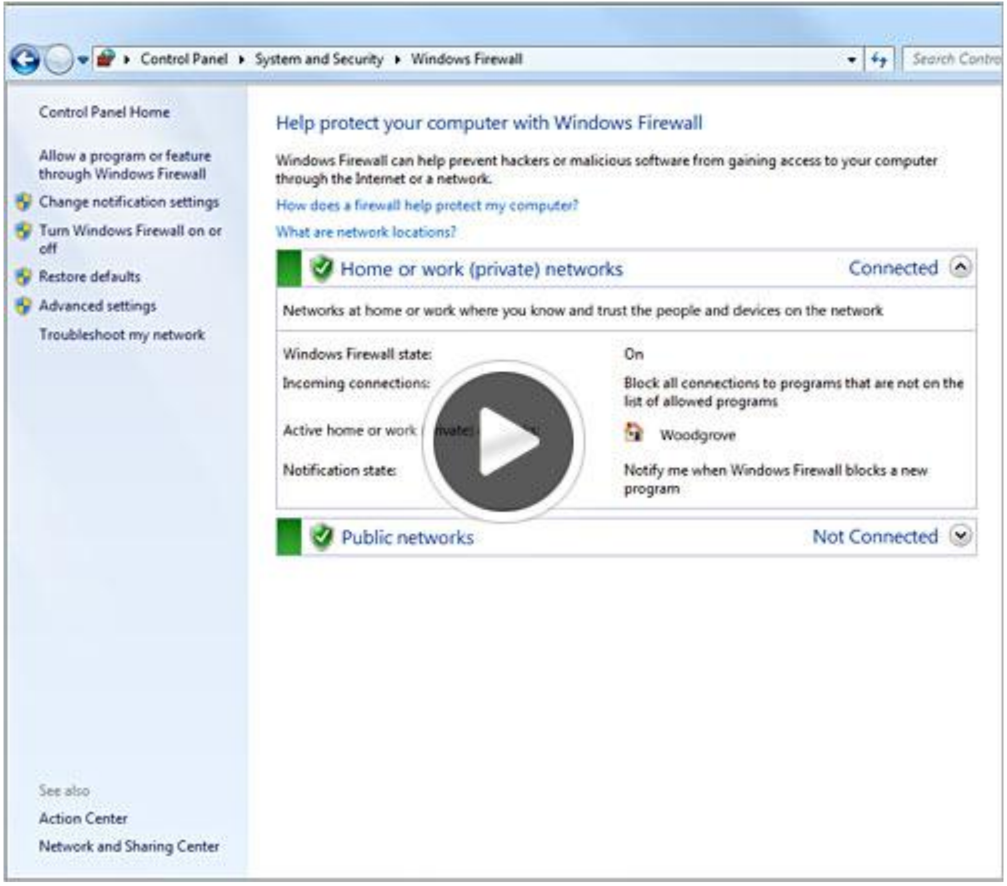
Open a port in Windows Firewall

If Windows Firewall is blocking a program and you want to allow that program to communicate through the firewall, you can usually do that by selecting the program in the list of allowed programs (also called the exceptions list) in Windows Firewall. To learn how to do this, see Allow a program to communicate through Windows Firewall.

Allow a program to communicate through Windows Firewall

By default, most programs are blocked by Windows Firewall to help make your computer more secure. To work properly, some programs might require you to allow them to communicate through the firewall.

Watch this video to learn how to allow a program to communicate through Windows Firewall (1:12)


Control Panel ▸ System and Security ▸ Windows Firewall
Search Contro
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

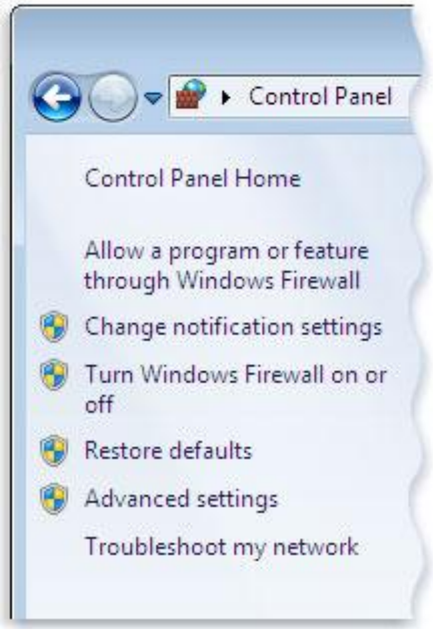
Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	Woodgrove
Notification state:	Notify me when Windows Firewall blocks a new program

Public networks — Not Connected

To allow a program to communicate through Windows Firewall

1. Open Windows Firewall by clicking the Start button, and then clicking Control Panel. In the search box, type firewall, and then click Windows Firewall.
2. In the left pane, click Allow a program or feature through Windows Firewall.



Control Panel

Control Panel Home

Allow a program or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Left pane of Windows Firewall

3. Click Change settings. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Select the check box next to the program you want to allow, select the network locations you want to allow communication on, and then click OK.

Warning

Before allowing a program through the firewall, make sure you understand the risks involved.

For information about opening ports in Windows Firewall, see Open a port in Windows Firewall.

If you’re having trouble allowing other computers to communicate with your computer through Windows Firewall, you can try using the Incoming Connections troubleshooter to automatically find and fix some common problems.

Open the Incoming Connections troubleshooter by clicking the Start button , and then clicking Control Panel. In the search box, type troubleshooter, and then click Troubleshooting. Click View all, and then click Incoming Connections.

However, if the program isn't listed, you might need to open a port. For example, to play a multiplayer game with friends online, you might need to open a port for the game so that the firewall allows the game information to reach your computer. A port stays open all the time, so be sure to close ports that you don't need open anymore.

1. Open Windows Firewall by clicking the Start button , and then clicking Control Panel. In the search box, type firewall, and then click Windows Firewall.
2. In the left pane, click Advanced settings. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
3. In the Windows Firewall with Advanced Security dialog box, in the left pane, click Inbound Rules, and then, in the right pane, click New Rule.
4. Follow the instructions in the New Inbound Rule wizard.

If you’re having trouble allowing other computers to communicate with your computer through Windows Firewall, you can try using the Incoming Connections troubleshooter to automatically find and fix some common problems.

Open the Incoming Connections troubleshooter by clicking the Start button , and then clicking Control Panel. In the search box, type troubleshooter, and then click Troubleshooting. Click View all, and then click Incoming Connections.

If you’re having trouble allowing other computers to communicate with your computer through Windows Firewall, you can try using the Incoming Connections troubleshooter to automatically find and fix some common problems.

Open the Incoming Connections troubleshooter by clicking the Start button , and then clicking Control Panel. In the search box, type troubleshooter, and then click Troubleshooting. Click View all, and then click Incoming Connections.