

WORKING WITH WINDOWS FIREWALL IN WINDOWS 7

Firewall in Windows 7

Windows 7 comes with two firewalls that work together. One is the **Windows Firewall**, and the other is **Windows Firewall with Advanced Security (WFAS)**.

The main difference between them is the complexity of the rules configuration.

Windows Firewall uses simple rules that directly relate to a program or a service.

The rules in WFAS can be configured based on protocols, ports, addresses and authentication. By default, both firewalls come with predefined set of rules that allow us to utilize network resources. This includes things like browsing the web, receiving e-mails, etc. Other standard firewall exceptions are File and Printer

Sharing, Network Discovery, Performance Logs and Alerts, Remote Administration, Windows Remote Management, Remote Assistance, Remote Desktop, Windows Media Player, Windows Media Player Network Sharing

Service.

With firewall in Windows 7 we can configure inbound and outbound rules. By default, all outbound traffic is allowed, and inbound responses to that traffic are also allowed. Inbound traffic initiated from external sources is automatically

blocked.

Sometimes we will see a notification about a blocked program which is trying to access network resources. In that case we will be able to add an exception to our firewall in order to allow traffic from the program in the future.

Windows 7 comes with some new features when it comes to firewall. For example, "full-stealth" feature blocks other computers from performing operating system fingerprinting. OS fingerprinting is a malicious technique used to determine the operating system running on the host machine. Another feature is "boot-time filtering". This feature ensures that the firewall is working at the same time when the network interface becomes active, which was not the case in previous versions of Windows.

When we first connect to some network, we are prompted to select a network location. This feature is known as Network Location Awareness (NLA). This feature enables us to assign a network profile to the connection based on the location. Different network profiles contain different collections of firewall rules. In Windows 7, different network profiles can be configured on different interfaces. For example, our wired interface can have a different profile than our wireless interface. There are three different network profiles available:

- Public
- Home/Work - private network

- Domain - used within a domain

We choose those locations when we connect to a network. We can always change the location in the Network and Sharing Center, in Control Panel. The Domain profile can be automatically assigned by the NLA service when we log on to an Active Directory domain. Note that we must have administrative rights in order to configure firewall in Windows 7.

Configuring Windows Firewall

To open Windows Firewall we can go to **Start > Control Panel > Windows Firewall**.

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

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from accessing 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

Networks at home or work where you know and trust the people you connect to.

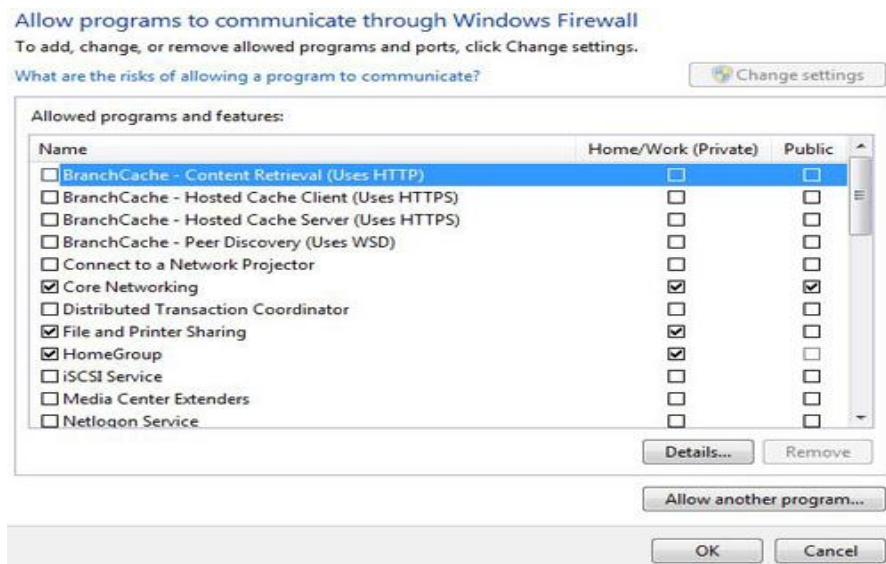
| | |
|---|--|
| Windows Firewall state: | On |
| Incoming connections: | Block all incoming connections on the Internet |
| Active home or work (private) networks: | None |
| Notification state: | Notify me when a program is blocked |

Public networks

Networks in public places such as airports or coffee shops.

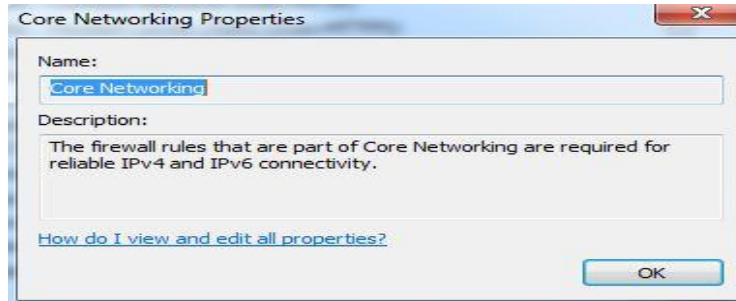
Windows Firewall

By default, Windows Firewall is enabled for both private (home or work) and public networks. It is also configured to block all connections to programs that are not on the list of allowed programs. To configure exceptions we can go to the menu on the left and select "Allow a program or feature through Windows Firewall" option.



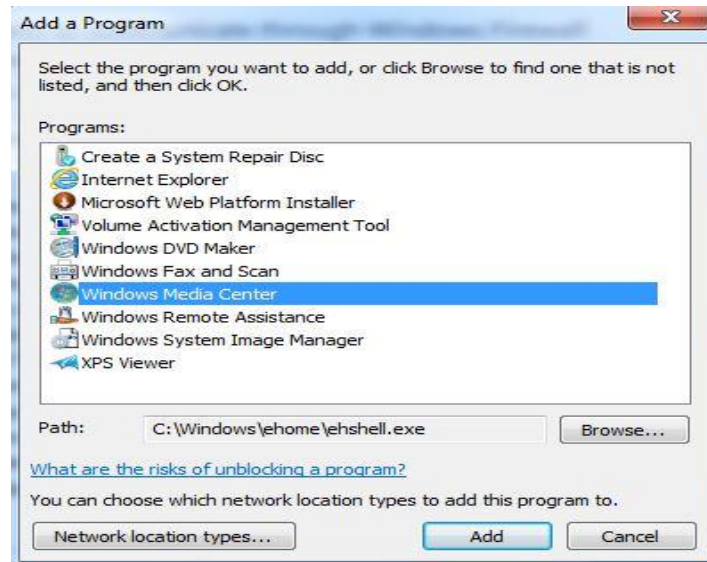
Exceptions

To change settings in this window we have to click the "Change settings" button. As you can see, here we have a list of predefined programs and features that can be allowed to communicate on private or public networks. For example, notice that the Core Networking feature is allowed on both private and public networks, while the File and Printer Sharing is only allowed on private networks. We can also see the details of the items in the list by selecting it and then clicking the Details button.



Details

If we have a program on our computer that is not in this list, we can manually add it by clicking on the "Allow another program" button.



Add a Program

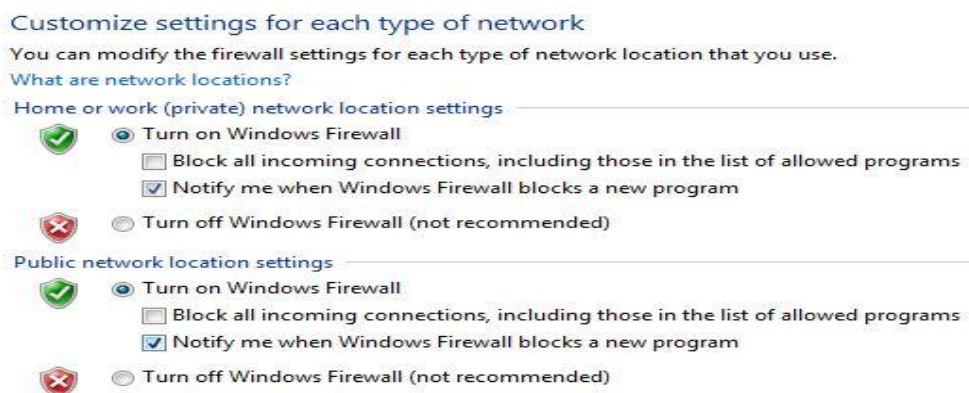
Here we have to browse to the executable of our program and then click the Add button. Notice that we can also choose location types on which this program will be allowed to communicate by clicking on the "Network location types" button.



Network Locations

Many applications will automatically configure proper exceptions in Windows Firewall when we run them. For example, if we enable streaming from Media Player, it will automatically configure firewall settings to allow streaming. The same thing is if we enable Remote Desktop feature from the system properties window. By enabling Remote Desktop feature we actually create an exception in Windows Firewall.

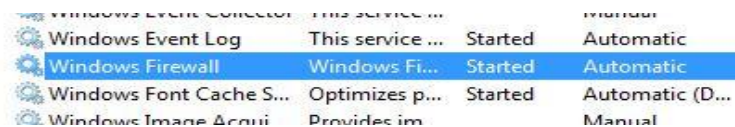
Windows Firewall can be turned off completely. To do that we can select the "Turn Windows Firewall on or off" option from the menu on the left.



Firewall Customization

Note that we can modify settings for each type of network location (private or public). Interesting thing here is that we can block all incoming connections, including those in the list of allowed programs.

Windows Firewall is actually a Windows service. As you know, services can be stopped and started. If the Windows Firewall service is stopped, the Windows Firewall will not work.



Firewall Service

In our case the service is running. If we stop it, we will get a warning that we should turn on our Windows Firewall.



Warning

Remember that with Windows Firewall we can only configure basic firewall settings, and this is enough for most day-to-day users. However, we can't configure exceptions based on ports in Windows Firewall any more.

Source: <http://www.utilizewindows.com/7/networking/452-working-with-windows-firewall-in-windows-7>