Opening TCP Port 80 in Windows Firewall

Open Windows Firewall

Steps

The following instructions are for opening TCP Port 80 in the Window Firewall - the firewall software included with Windows. If you are using an alternate firewall, please consult their documentation.

Important: It is not adequate to open the port's inbound and outbound traffic for just the program or the service. You must create Port rules as directed below in Step 6, or it will not work.

1. Open Control Panel from the Start menu.
2. Select Windows Firewall.
Select Advanced Settings....

3. Select Advanced settings in the left column of the Windows Firewall window.

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
- Public networks  Not Connected

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: Network
Notification state: Notify me when Windows Firewall blocks a new program
Select Inbound Rules...
5. **Select New Rule** in the right column.

![Image of Windows Firewall with Advanced Security window showing Inbound Rules and New Rule option]

- Select New Rule in the right column.
Select Port in the New Inbound Rule Wizard and then click Next. Note, do not create a Program rule - you must create a Port rule.

What type of rule would you like to create?

- **Program**
  - Rule that controls connections for a program.

- **Port**
  - Rule that controls connections for a TCP or UDP port.

- **Predefined**
  - BranchCache - Content Retrieval (Uses HTTP)
  - Rule that controls connections for a Windows experience.

- **Custom**
  - Custom rule.

Learn more about rule types
Opening TCP Port 80 In Windows Firewall

Set up Protocol and Ports...

7. Select which protocol this rule will apply to TCP, select **Specific** local ports, type port number **80**, and then click **Next**.
Allow the Connection...

8. Select **Allow the connection** and then click **Next**.

![New Inbound Rule Wizard](image)

**Action**

Specify the action to be taken when a connection matches the conditions specified in the rule.

- **Allow the connection**
  - This includes connections that are protected with IPSec as well as those that are not.

- **Allow the connection if it is secure**
  - This includes only connections that have been authenticated by using IPSec. Connections will be secured using the settings in IPSec properties and rules in the Connection Security Rule node.

- **Block the connection**

*Learn more about actions*
9. Select when this rule applies (check all of them for the port to always stay open) and then click **Next**.

Profile

Specify the profiles for which this rule applies.

When does this rule apply?

- **Domain**
  - Applies when a computer is connected to its corporate domain.

- **Private**
  - Applies when a computer is connected to a private network location.

- **Public**
  - Applies when a computer is connected to a public network location.

Learn more about profiles
Name your rule and Finish...

TCP Port 80 is now open and ready to be used.