Link: [**https://www.thewindowsclub.com/how-to-allow-pings-icmp-echo-requests-through-windows-firewal**](https://www.thewindowsclub.com/how-to-allow-pings-icmp-echo-requests-through-windows-firewall)

**How to allow Pings (ICMP Echo requests) through Windows Firewall**

1. **Run powershell as administrator**
2. **Set-ExecutionPolicy Unrestricted**
3. **Enter to create the ICMPv4 exception: netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow**
4. **Enter to create the ICMPv6 exception: netsh advfirewall firewall add rule name="ICMP Allow incoming V6 echo request" protocol=icmpv6:8,any dir=in action=allow**
5. **To disable ping requests for the ICMPv4 exception, run the command below: netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=block**
6. **To disable ping requests for the ICMPv6 exception, run the command below: netsh advfirewall firewall add rule name="ICMP Allow incoming V6 echo request" protocol=icmpv6:8,any dir=in action=block**

By default, the [Windows Firewall with Advanced Security](https://www.thewindowsclub.com/how-to-configure-windows-7-firewall) blocks ICMP Echo Requests (Pings) from the network. In this post, we will show you how to allow **Pings (ICMP Echo requests)** through your **Windows Firewall** using *Command Promp*t or via the *Windows Firewall with Advanced Security UI*.

### **Should I enable ICMP?**

For many network administrators, they consider the Internet Control Message Protocol (ICMP) a security risk, and therefore as a security measure, should have ICMP always be blocked at the firewall. In as much as ICMP is widely known to have some security issues associated with it, and for just that reason, ICMP should be blocked; it’s still no reason to block all ICMP traffic!

### **What ICMP types should I allow?**

Apart from Type 3 and Type 4 – the only essential ICMP traffic you need to allow in and out of your firewall on your Windows 10/11 PC, everything else is either optional or should be blocked. Bear in mind that to send ping requests, you need to allow type 8 OUT and type 0 IN.

## **Allow Pings (ICMP Echo requests) through Windows Firewall**

Generally, the way the [ping command works](https://www.thewindowsclub.com/ping-and-traceroute-network-tools) amongst other network tools, is simply by sending special packets known as Internet Control Message Protocol (ICMP) Echo Requests to a target device, and then wait for that receiving device to respond and send back an ICMP Echo Reply packet. This action of pinging, apart from testing whether a network-connected device is active, it also measures the response time and outputs the result for you to review.

We can allow Pings (ICMP Echo requests) through your Firewall on Windows 10 or Windows 11 PC in either of two ways. We’ll explore this topic under the methods outlined below as follows.

**Note**: If you have a third-party security software with its own firewall installed on your system or just another type of dedicated third-party firewall program installed, you’ll need to [open ports in that firewall](https://www.thewindowsclub.com/block-open-port-windows-8-firewall) instead of the in-built Windows Firewall.

#### **1] Allow Pings (ICMP Echo requests) through Firewall on Windows PC via Windows Firewall with Advanced Security UI**

#### 

#### **To allow Pings (ICMP Echo requests) through Firewall on Windows PC via Windows Firewall with Advanced Security user interface, do the following:**

#### 

* Click Start or press the Windows key on the keyboard.
* Type *windows firewall*, and then select **Windows Defender Firewall** from the top of the search result.
* Click the **Advanced settings** link on the left side of the Control Panel window that opens.
* In the left pane, right-click *Inbound Rules* and choose **New Rule**.
* In the *New Inbound Rule* window, select **Custom**.
* Click **Next**.
* On the *Does this rule apply to all programs or specific programs?* page, make sure the radio button is selected for **All programs**.
* Click **Next**.
* On the *To which ports and protocol does this rule apply?* page, click the **Protocol type** drop-down, and select *ICMPv4*.
* Click the **Customize** button.
* In the *Customize ICMP Settings* window, select the **Specific ICMP types** option.
* In the list of ICMP types, enable **Echo Request**.
* Click **OK**.
* Back on the T*o which ports and protocol does this rule apply?* page, click **Next**.
* On the page that appears, select the radio button for **Any IP address** option for under the *Which local IP addresses does this rule apply to?* and *Which remote IP addresses does this rule apply to?* sections.

If you want, you can configure specific IP addresses to which your PC will respond to a ping request. Other ping requests are ignored.

* On the *What action should be taken when a connection matches the specified conditions?* page, make sure the radio button is selected for **Allow the connection** option.
* Click **Next**.
* On the *When does this rule apply* page, check/uncheck the available options per your requirement.
* Click **Next**.
* At the final screen, you need to give your new rule a name, and optionally provide a description. It’s recommended to add **ICMPv4** to the rule name to differentiate from the **ICMPv6** rule that you will create also.
* Click the **Finish** button.

Now, you can go ahead and create the ICMPv6 rule by repeating the steps above, but this time at the *To which ports and protocol does this rule apply?* page, click the **Protocol type** drop-down, and select *ICMPv6* instead*.*

* Exit Windows Defender Firewall when done.

If at anytime you want to disable the rule, open Windows Firewall with Advanced Security Control Panel, select **Inbound Rules** on the left, and locate the rules you created in the middle pane, right-click the rule and choose **Disable**. These rules can also be deleted – but it’s best just disabling the rules instead, so you can easily and quickly re-enable them without recreating them.

#### **2] Allow Pings (ICMP Echo requests) through Firewall on Windows PC using Command Prompt**

This is the fastest way to create an exception for ping requests on Windows 11/10.

To allow Pings (ICMP Echo requests) through Firewall on Windows PC using Command Propt, do the following:

* Press **Windows key + R** to invoke the Run dialog.
* In the Run dialog box, type *cmd* and then press **CTRL + SHIFT + ENTER** to [open Command Prompt in admin/elevated mode](https://www.thewindowsclub.com/how-to-run-command-prompt-as-an-administrator).
* In the command prompt window, type or copy and paste the command below and hit Enter to **create the ICMPv4 exception**.

netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow

* To **create the ICMPv6 exception**, run the command below:

netsh advfirewall firewall add rule name="ICMP Allow incoming V6 echo request" protocol=icmpv6:8,any dir=in action=allow

Changes takes effect immediately without system reboot.

* To **disable ping requests for the ICMPv4 exception**, run the command below:

netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=block

* To **disable ping requests for the ICMPv6 exception**, run the command below:

netsh advfirewall firewall add rule name="ICMP Allow incoming V6 echo request" protocol=icmpv6:8,any dir=in action=block

If at anytime you want to disable a rule but have forgotten the name of the rule, you can run the command below to see a list of all rules:

netsh advfirewall firewall show rule name=all

That’s it on how to allow Pings (ICMP Echo requests) through Windows Firewall!

### **What is ICMP attack?**

An ICMP attack (also referred to as a Ping flood attack), is a common [Denial-of-Service (DoS) attack](https://www.thewindowsclub.com/dos-denial-of-service-attack) in which a threat actor maliciously attempts to overwhelm a targeted device with ICMP echo-requests (pings).