

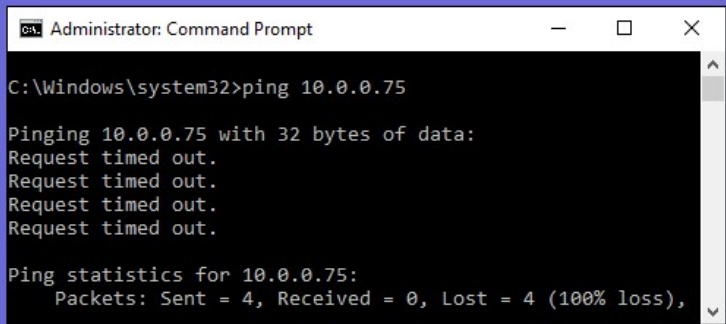
How-To Geek

How to Allow Pings (ICMP Echo Requests) Through Your Windows Firewall



WALTER GLENN [@wjglenn](#)

UPDATED MARCH 28, 2019, 7:20PM EDT



```
Administrator: Command Prompt

C:\Windows\system32>ping 10.0.0.75

Pinging 10.0.0.75 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.75:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

When Windows Firewall is enabled with default settings, you can't use the ping command from another device to see if your PC is alive. Here's how to change that.

The ping command works by sending special packets known as Internet Control Message Protocol (ICMP) Echo Requests to a target device, and then waiting for that device to send back an ICMP Echo Reply packet. This not only lets you test whether a network-connected device is active, but it also measures the response time and displays that for you, as well. By default, [Windows Firewall with Advanced Security](#) blocks ICMP Echo Requests from the network. Sure, you could take the drastic step of [disabling the firewall for testing purposes](#), but a simpler solution is just to create an exception that allows ICMP requests through the firewall. We're going to show you how to do that both from the Command Prompt and the Windows Firewall with Advanced

Security interface. (Note that, if you have an antivirus with a firewall or another type of third-party firewall program installed, you'll need to open ports in that firewall instead of the built-in Windows Firewall.)

The instructions in this article should work for Windows 7, 8, and 10. We'll point out where there are any major differences.

Warning: Creating exceptions and opening ports through your firewall does open up security risks. Allowing ping requests isn't too big a deal, but it's usually best to block anything you don't need.

Allow Ping Requests by Using the Command Prompt

The fastest way to create an exception for ping requests is with the Command Prompt. You'll need to open it with admin privileges. To do so in Windows 8 and 10, press Windows+X and then select "Command Prompt (Admin)." In Windows 7, hit Start and type "command prompt." Right-click the resulting entry and choose "Run as Administrator."

To enable ping requests, you're going to create two exceptions to allow traffic through the firewall—one for ICMPv4 requests and one for ICMPv6 requests. To create the ICMPv4 exception, type (or copy and paste) the following command at the prompt and then hit Enter:

```
netsh advfirewall firewall add rule name="ICMP Allow in
```

And to create the ICMPv6 exception, use this command:

```
netsh advfirewall firewall add rule name="ICMP Allow in
```

The changes will take place immediately—no need to restart your PC or anything. Now, if you ping your PC from a remote device, you should get an actual result.

To disable ping requests again, you'll need to disable both exceptions you created. For the ICMPv4 exception, type (or copy and paste) this command at the prompt and hit Enter:

```
netsh advfirewall firewall add rule name="ICMP Allow in
```

And to disable ICMPv6 requests, use this command:

```
netsh advfirewall firewall add rule name="ICMP Allow in
```

When requests are blocked, ping requests to your PC will be met with a “Request timed out” error.

Note that when using the commands we just covered, you can use any name for the rule you want. However, when you go to disable a rule, you'll want to use the same rule name as when you created it. If you forget the name of the rule, you can use the Command Prompt to see a list of all rules. Just type the following command and hit Enter:

```
netsh advfirewall firewall show rule name=all
```

You'll see lots of rules listed, but scroll back up to the top of the list and you should see any rules you've created right at the top.

Allow Ping Requests by Using Windows Firewall With Advanced Security

While the Command Prompt is the quickest way to add an exception to your firewall for ping requests, you can also do this in the graphic interface using the "Windows Firewall with Advanced Security" app. Hit Start, type "windows firewall with," and then launch "Windows Firewall with Advanced Security."

You're going to create two new rules—one for allowing ICMPv4 requests and one for allowing ICMPv6 requests. In the left pane, right-click "Inbound Rules" and choose "New Rule."

In the "New Inbound Rule Wizard" window, select "Custom" and then click "Next."

On the next page, make sure “All programs” is selected and then click “Next.”

On the next page, choose “ICMPv4” from the “Protocol type” dropdown and then 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” and then click “OK.”

Back in the “New Inbound Rule Wizard” window, you’re ready to click “Next.”

On the next page, it's easiest to just make sure that the "Any IP address" options are selected for both local and remote IP addresses. If you want, you can configure specific IP addresses to which your PC will respond to a ping request. Other ping requests are ignored. This lets you narrow things down a bit so that only certain devices will be able to ping your PC. You can also configure separate lists of approved IP addresses for your local and remote (Internet) networks. However you set it up, click "Next" when you're done.

On the next page, make sure that the “Allow the connection” option is enabled and then click “Next.”

The next page allows you some control over when the rule is active. If you want the rule to apply no matter what type of network it's connected to, leave the options at their default and just click "Next." However, if your PC is not part of a business (and doesn't connect to a domain), or if you prefer it not respond to ping requests when it's connected to a public network, feel free to disable those options.

Finally, you need to give your new rule a name, and optionally a description. However, we do recommend that you at least get the text “ICMPv4” in there because you’ll also be creating a second rule for allowing ICMPv6 requests. Choose whatever makes sense to you and then click “Finish.”

Unfortunately, you're not quite done yet. It's a good idea to go ahead and create a second rule that allows incoming ICMPv6 requests. Mostly, it's a good just-in-case measure. People tend to use IPv4 addresses when issuing ping commands, but some networking apps use IPv6. Might as well have your bases covered.

Follow the same steps we just went over and set all the options exactly the same as we did for the ICMPv4 rule. However, when you get to the ports and protocols page, select "ICMPv6" from the dropdown instead of "ICMPv4." That—and creating a different name for the rule—are the only two things that change.

When you have the two new rules in place, you can close the “Windows Firewall with Advanced Security” app. No need to restart your PC or anything. Your PC should immediately begin responding to pings.

If you ever want to disable all this, you could go back and delete those two rules. However, you might be better off just disabling the rules instead. That way, you can re-enable them without recreating them. In the “Windows Firewall with Advanced Security” app, select “Inbound Rules” on the left, and locate the rules you made in the middle pane. Right-click a rule and choose “Disable” to prevent ping requests from passing through the firewall.

Allowing ping requests to reach your PC is not something everyone will need to do. But, if you're doing any kind of network troubleshooting, ping can be a valuable tool. It's also pretty easy to turn on and off once you have things set up.

READ NEXT

- › [Samsung Galaxy S20: How to Edit and Disable Edge Panels](#)
- › [What Is Discord, and Is It Only for Gamers?](#)
- › [TN vs. IPS vs. VA: What's the Best Display Panel Technology?](#)
- › [What Is Microsoft Teams, and Is It Right for My Business?](#)
- › [Samsung Galaxy S20: How to Completely Disable Bixby](#)

WALTER GLENN

Walter Glenn is the Editorial Director for How-To Geek and its sister sites. He has more than 30

years of experience in the computer industry and over 20 years as a technical writer and editor. He's written hundreds of articles for How-To Geek and edited thousands. He's authored or co-authored [over 30 computer-related books](#) in more than a dozen languages for publishers like Microsoft Press, O'Reilly, and Osborne/McGraw-Hill. He's also written hundreds of white papers, articles, user manuals, and courseware over the years. [READ FULL BIO »](#)

How-To Geek is where you turn when you want experts to explain technology. Since we launched in 2006, our articles have been read more than 1 billion times. [Want to know more?](#)