

## Enable ICMP Echo (Ping)

Last Modified on 09.02.25

ICMP Echo is required by many Right Click Tools to detect if a computer is turned on. Since many of the tools use methods that are slow to timeout when a computer is turned off, Right Click Tools sends a ping packet to the computer and skips the device if no reply is received. With Right Click Tools Enterprise, there is an option to disable this feature in the server's Global Settings.

**NOTE**: ICMP Echo is an optional component for Right Click Tools Enterprise, whereas Remote Registry and Remote WMI are required for many of the tools to work.

## Create a Firewall Rule for ICMP Echo

By default, ICMP Echo is not allowed through the Windows firewall. This can easily be enabled with Group Policy.

To create a new firewall rule:

1. Open the Group Policy Management Console and create a new Group Policy Object.

2. Navigate to Computer Configuration > Policies > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security.

3. Right-click on Inbound Rules and choose New Rule.

4. On the **Rule Type** page, choose to create a **Custom** rule and click **Next**.

5. On the **Program** page, choose **All programs** and click **Next**.

6. On the **Protocols and Ports** page, choose a **Protocol type** of **ICMPv4.** Click **Customize**.

2	New Inb	bound Rule Wizard			
Protocol and Ports					
Specify the protocols and ports to	which this rule applies.				
Steps:	To which ports and protocols does this rule apply?				
Rule Type					
Program					
Protocol and Ports	Protocol type:	ICMPv4 v			
Scope	Protocol number:	1			
Action					
Profile	Local port:	All Ports V			
Name					
		Example: 80, 443, 5000-5010			
	Remote port:	Al Ports V			
		5 1 20 442 5222 5242			
		Example: 80, 443, 5000-5010			
	Internet Control Message (ICMP) settings:	e Protocol Qustomize			
	(in ) courses				
		(Barly Next) Court			
		< Back Next > Cancel			
l					

7. On the Customize ICMP Settings page, select Specific ICMP types and Echo Request. Click OK and then Next on the

## Protocols and Ports page.

Customize ICMP Settings				
Apply this rule to the following Internet Control Message Protocol (ICMP) connections:				
O <u>A</u> ll ICMP types				
Specific ICMP types				
Packet Too Big Destination Unreachable Source Quench Redirect Cho Request Router Advertisement Router Solicitation Time Exceeded Parameter Problem Timestamp Request Address Mask Request				
This ICMP type:				
_jype: 0 ✓ ⊈ode: Any ✓ Add				
OK Cancel				

8. On the **Scope** page, choose **Any IP address** for both the local and remote IP addresses. Click **Next**.

9. On the **Action** page, choose **Allow the connection**. Click **Next**.

10. On the **Profile** page, choose the firewall profiles to which the rule will apply. At a minimum, select the **Domain** level. Click **Next**.

<b>@</b>	New Inbound Rule Wizard		
Profile			
Specify the profiles for which this	rule applies.		
Specify the profiles for which this Steps: Pice Type Protocol and Pots Action Profile Name	When does this rule apply?     Image: Demain Apples when a computer is connected to its coporate domain.     Private Apples when a computer is connected to a private network location, such as a home or work place.     Public Apples when a computer is connected to a public network location.		
	< Back Next > Cancel		

11. Give the new firewall rule a descriptive name and click **Finish** to exit the New Inbound Rule Wizard.

Copyright © 2025 Recast Software Inc. All rights reserved.