Enable ICMP Echo (Ping)

Last Modified on 02.01.23

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.

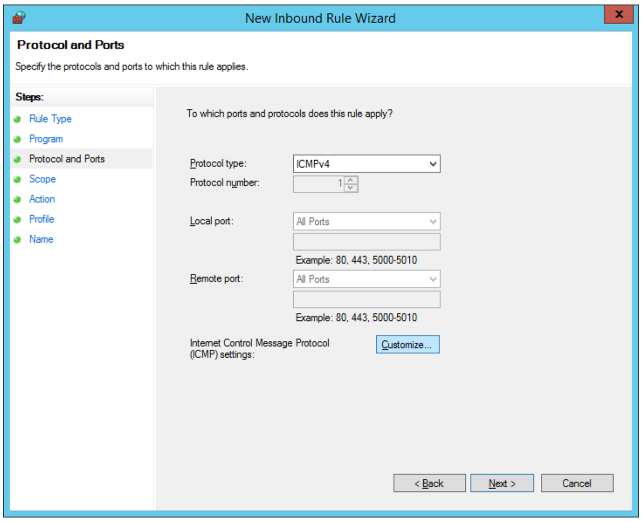
2. Navigate to **Computer Configuration** > **Policies** > **Security Settings** > **Windows Firewall with Advanced Security** > **Windows Firewall with Advanced Security**.

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**.



Protocol and Ports

Specify the protocols and ports to which this rule applies.

To which ports and protocols does this rule apply?

Protocol type: ICMPv4

Protocol number: 1

Local port: All Ports

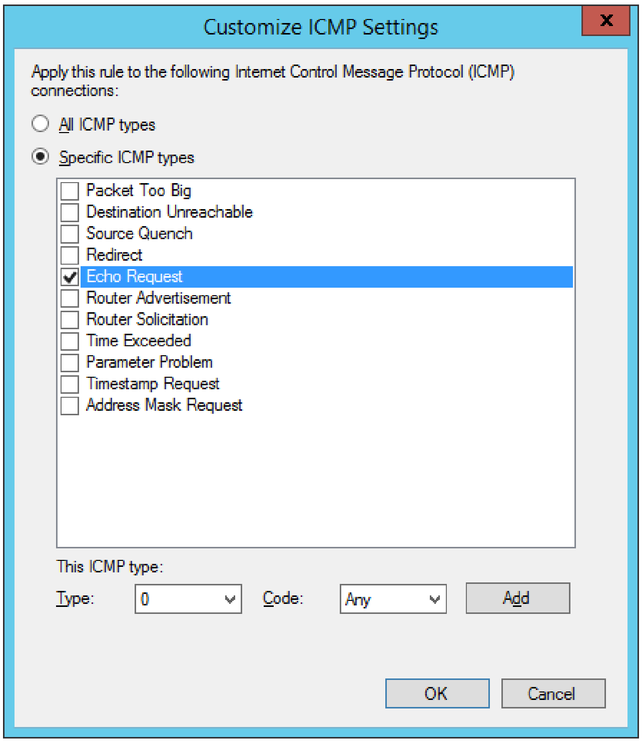
Example: 80, 443, 5000-5010

Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

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.



Apply this rule to the following Internet Control Message Protocol (ICMP) connections:

○ All ICMP types

● Specific ICMP types

- ☐ Packet Too Big
- ☐ Destination Unreachable
- ☐ Source Quench
- ☐ Redirect
- ☑ Echo Request
- ☐ Router Advertisement
- ☐ Router Solicitation
- ☐ Time Exceeded
- ☐ Parameter Problem
- ☐ Timestamp Request
- ☐ Address Mask Request

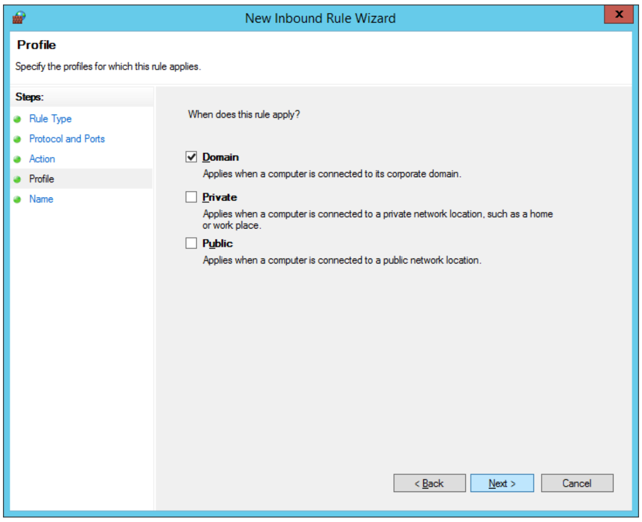
This ICMP type:

Type: 0 Code: Any

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**.



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, such as a home or work place.

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

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