

Firewall Requirements

Last Modified on 03.20.24

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.

@	New Inbound Rule Wizard	
Protocol and Ports		
Specify the protocols and ports	to which this rule applies.	
Steps:		
Rule Type	To which ports and protocols does this rule apply?	
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	
	Bemote port: All Ports V	
	Example: 80, 443, 5000-5010	
	Internet Control Message Protocol Customize	
	(icinii) decuilge.	
	< <u>B</u> ack <u>N</u> ext >	Cancel

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	x
Apply this rule to the following Internet Control Message Protocol (ICMP) connections:	
○ <u>A</u> ll ICMP types	
<u>Specific ICMP types</u>	
Packet Too Big Destination Unreachable Source Quench Redirect Fcho Request Router Advertisement Router Solicitation Time Exceeded Parameter Problem Timestamp Request Address Mask Request	
This ICMP type: Ţype: 0	
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**.

@	New Inbound Rule Wizard	x
Profile		
Specify the profiles for which this r	ule applies.	
Specify the profiles for which the r Steps: Puble Type Protocol and Ports Action Profile Name	Us apples. When does this rule apply? Demain Apples when a computer is connected to its corporate domain. Private Apples 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.	
	< Back Next > Cancel]

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

The Remote Registry service is used by many Right Click Tools to pull information about a particular device. To enable Remote Registry, you'll need to start the service and create a new rule to allow it through the firewall.

NOTE: When configuring your clients to work with Right Click Tools Enterprise, Remote WMI must also be enabled. ICMP Echo can optionally be enabled to speed up actions for computers that are offline.

Start the Remote Registry Service

To start the service:

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

2. Edit the new Group Policy Object and go to **Computer Configuration** > **Preferences** > **Control Panel Settings** > **Services**.

3. Create a new service.

4. Change the **Startup type** to **Automatic**.

5. In the Service name field, browse to Remote Registry.

Sele	ct a Service	x
Display Name	Service Name	~
IPsec Policy Agent	PolicyAgent	
Power	Power	
Printer Extensions and Notifications	PrintNotify	
User Profile Service	ProfSvc	
Remote Access Auto Connection Man	RasAuto	
Remote Access Connection Manager	RasMan	
Routing and Remote Access	RemoteAccess	
Remote Registry	RemoteRegistry	-
RPC Endpoint Mapper	RpcEptMapper	-
Remote Procedure Call (RPC) Locator	RpcLocator	
Remote Procedure Call (RPC)	RpcSs	
Resultant Set of Policy Provider	RSoPProv	
Special Administration Console Helper	sacsvr	
Security Accounts Manager	SamSs	
Smart Card	SCardSvr	~
	<u> </u>	
	Select	Cancel
	becc	
		æ

6. Under Service action, select Start service. Click OK.

General Recovery Common Startup: Automatic V Service name: RemoteRegistry Service action: Start service V
Service name: RemoteRegistry Service action: Start service
Service name: RemoteRegistry
Service action: Start service
Log on as: No change Local System account Allow service to interact with desktop
○ <u>T</u> his account:
Password:
Confirm password:
OK Cancel Apply Help

7. Close the Group Policy Management Editor.

Create a Firewall Rule for Remote Registry

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

To create a new firewall rule:

1. Create or edit an existing 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. In the New Inbound Rule Wizard, choose **Port**.
- 5. On the Protocols and Ports page, choose **TCP** and **Specific Local Ports**. Enter **445** as the local port.

2	New Inbound F	Rule Wizard	x
Protocol and Ports			
Specify the protocols and ports to	which this rule applies.		
Steps:			
Rule Type	Does this rule apply to TCP or UDF	??	
Protocol and Ports	• TCP		
Action	O UDP		
Profile			
Name	Does this rule apply to all local port	s or specific local ports?	
	All local ports		
	 Specific local ports; 	445	
		Example: 80, 443, 5000-5010	
		< Back Next > Cancel	
		Tour > Control	_

6. On the Action page, choose **Allow the connection**.

7. On the Profile page, choose the firewall profiles to which the rule will apply. You should select at least the **Domain** level.

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

Many Right Click Tools use Remote Windows Management Instrumentation (WMI) to gather information and perform Configuration Manager client actions on devices.

NOTE: When configuring your clients to work with Right Click Tools Enterprise, Remote Registry must also be enabled. ICMP Echo can optionally be enabled to speed up actions for computers that are offline.

Create a Firewall Rule for Remote WMI

WMI is not allowed through the Windows firewall by default, but can be enabled with a Group Policy rule.

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 **Predefined** rule.

5. Select Windows Management Instrumentation (WMI) from the drop-down menu and click Next.

2	New Inbound Rule Wizard
Rule Type Select the type of firewall rule to a	create.
Steps: Pude Type Predefined Rules Action	What type of rule would you like to create? Pogram Rule that controls connections for a program. Pgd Rule that controls connections for a TCP or UDP port. Pgdefined Windows Management Instrumentation (WM) Rule that controls connections for a Windows experience. Outcom Gustem rule.

- 6. On the Predefined Rules page, click **Next**.
- 7. On the Action page, choose **Allow the connection**.
- 8. Click **Finish** to exit the New Inbound Rule Wizard.

Copyright © 2023 Recast Software, LLC. All rights reserved.