## Enable Remote WMI

Last Modified on 07.04.23

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.

<b>@</b>	New Inbound Rule Wizard	ĸ
Rule Type Select the type of firewall rule to create.		
Steps: Prodefined Rules Action	What type of rule would you like to create?   Pergram   Rule that controls connections for a program.   Pergl   Rule that controls connections for a TCP or UDP pot.   Orgedinical   Windows Management Instrumentation (WMI)   Rule that controls connections for a Windows experience.   Outcom   Custom 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.