

# Task 1A: Set Up Configuration Manager for Right Click Tools

Last Modified on 08.14.24

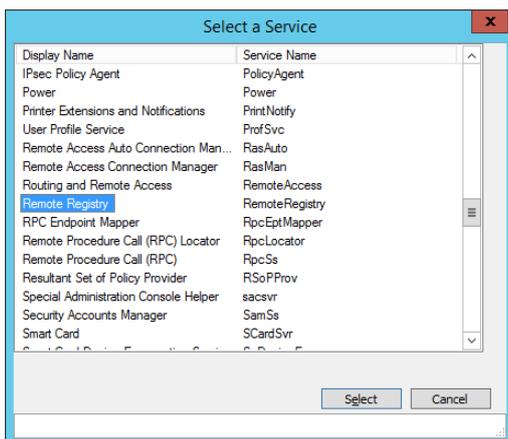
If there will be an extended period of time before you install and configure your Recast Management Server, you can use the following instructions to start the Remote Registry service, create firewall rules for Remote Registry, Remote WMI, and ICMP Echo, and configure the Interactive Command Prompt.

## Start the Remote Registry Service

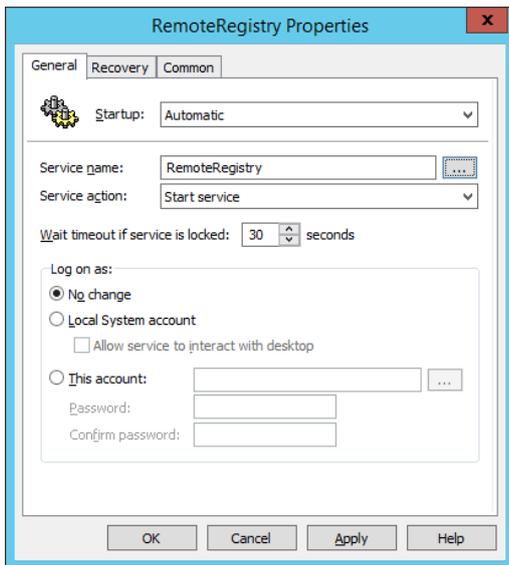
The Remote Registry service is used by many Right Click Tools to pull information about a particular device. To enable Remote Registry, you'll need to start the service and create a new rule to allow it through the firewall.

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**.



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



7. Close the Group Policy Management Editor.

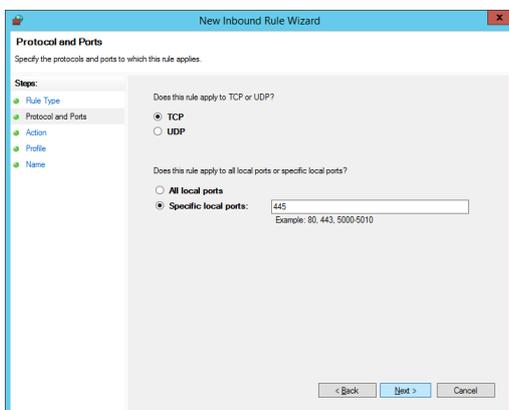
## Create Firewall Rules for Remote Registry, Remote WMI, and ICMP Echo

By default, Remote Registry, Remote WMI, and ICMP are not allowed through the Windows firewall, but you can enable them with group policy rules.

### Remote Registry

To create a firewall rule for Remote Registry:

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. 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.



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

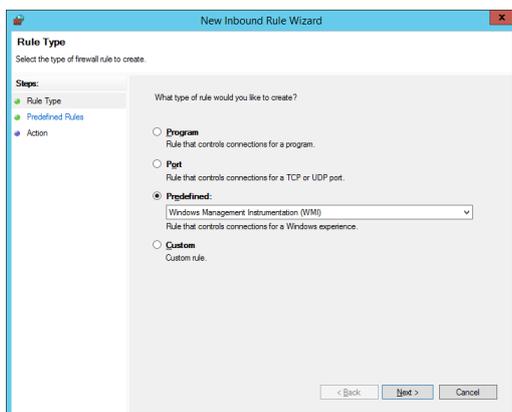
7. On the Profile page, choose the firewall profiles to which the rule will apply. You should select at least the **Domain** level.
8. Give the new firewall rule a descriptive name and click **Finish** to exit the New Inbound Rule Wizard.

## Remote WMI

Remote Windows Management Instrumentation (WMI) is used by many Right Click Tools to gather information and perform Configuration Manager client actions on devices.

To create a firewall rule for Remote WMI:

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**.



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.

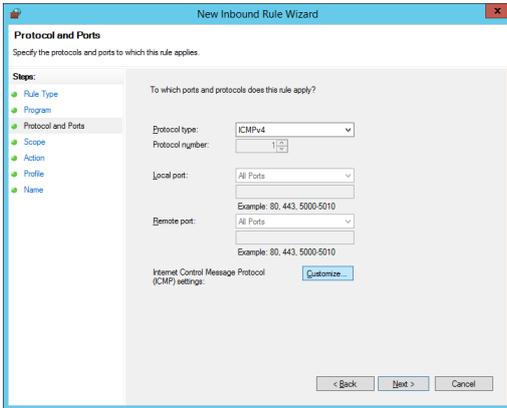
## ICMP Echo (Ping)

ICMP Echo can optionally be used to speed up actions for computers that are offline. 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.

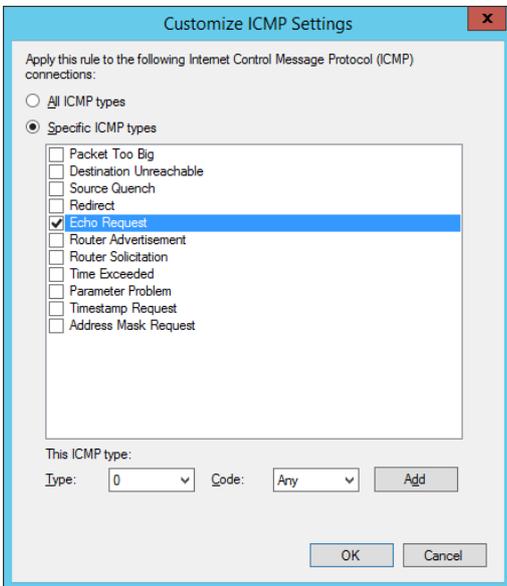
To create a firewall rule for ICMP Echo:

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**.

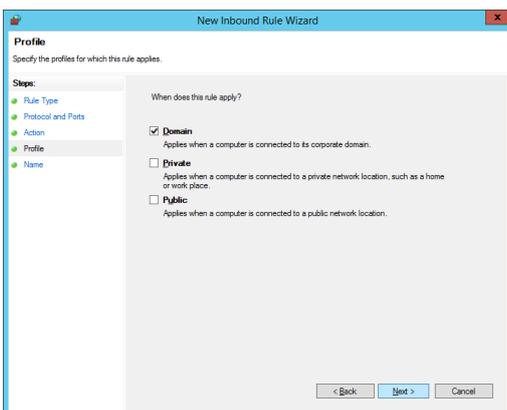
- On the **Rule Type** page, choose to create a **Custom** rule and click **Next**.
- On the **Program** page, choose **All programs** and click **Next**.
- On the **Protocols and Ports** page, choose a **Protocol type** of **ICMPv4**. Click **Customize**.



- On the **Customize ICMP Settings** page, select **Specific ICMP types** and **Echo Request**. Click **OK** and then **Next** on the **Protocols and Ports** page.



- On the **Scope** page, choose **Any IP address** for both the local and remote IP addresses. Click **Next**.
- On the **Action** page, choose **Allow the connection**. Click **Next**.
- On the **Profile** page, choose the firewall profiles to which the rule will apply. At a minimum, select the **Domain** level. Click **Next**.



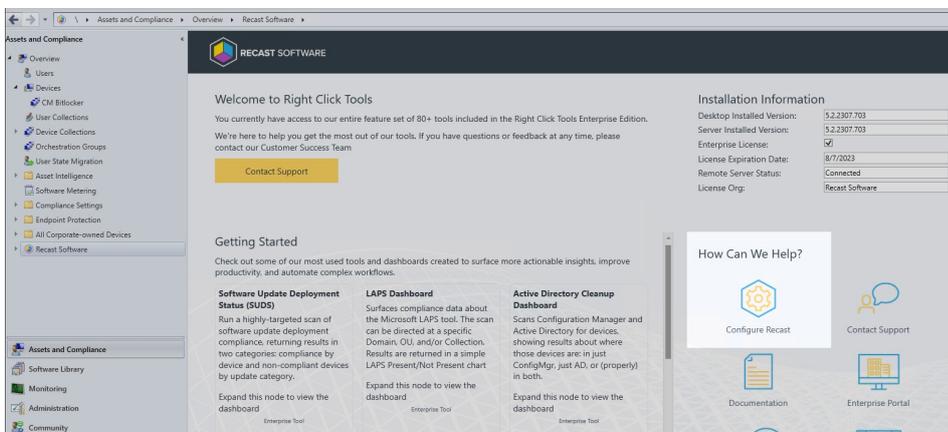
11. Give the new firewall rule a descriptive name and click **Finish** to exit the New Inbound Rule Wizard.

## Set Up Interactive Command Prompt

Interactive Command Prompt setup is done in the Configure Recast Console Extension application regardless of whether you've installed Right Click Tools with or without Recast Management Server. The Interactive Command Prompt tool requires a download of [PsExec](#) from the Microsoft website before proceeding.

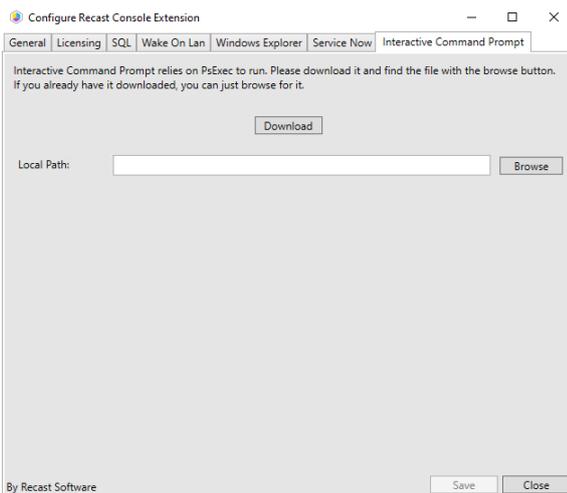
To configure the Interactive Command Prompt:

1. In your Configuration Manager console, navigate to **Assets and Compliance > Recast Software** and click **Configure Recast** in the 'How Can We Help?' section.



2. On the **Interactive Command Prompt** tab, click to **Download** the PsExec utility from Microsoft.

3. Click **Browse** and navigate to your local path or copy PsExec over manually into the **Local Path** field.



4. **Save** your changes.

Next Up — [Task 2: Install Recast Management Server with Recast Proxy](#)

Copyright © 2024 Recast Software Inc. All rights reserved.