Enable Remote Registry

Last Modified on 02.01.23

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.

Select a Service			
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 C:	ancel	

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				
Wait timeout if service is locked: 30 w seconds 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.

Provide the with the						
Protocol and Ports						
Specify the protocols and ports to which this rule applies.						
Steps:						
Rule Type	Does this rule apply to TCP or UDP?					
Protocol and Ports	TCP					
Action	O UDP					
Profile						
Name	Does this rule apply to all local ports or specific local ports?					
	All local ports					
	Specific local ports:	445				
		Example: 80, 443, 5000-5010				
		< Back Next > Cancel				
			_			
F						

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.