

Console Configuration for Right Click Tools

Last Modified on 03.19.25

Enable Remote Registry

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 🗸
	S <u>e</u> lect Cancel

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

-	RemoteRegistry Properties
General Recovery	Common
Startup:	Automatic V
Service <u>n</u> ame:	RemoteRegistry
Service action:	Start service V
Wait timeout if serv	ice is locked: 30 🗢 seconds
O <u>T</u> his account:	
Password:	
Confirm passw	ord:
0	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.

a	New Inbound	I Rule Wizard
Protocol and Ports		
Specify the protocols and ports to	which this rule applies.	
Steps:		
Rule Type	Does this rule apply to TCP or U	DP?
Protocol and Ports	TCP	
Action	○ UDP	
Profile		
Name	Does this rule apply to all local p	orts or specific local ports?
	All local ports	
	Specific local ports:	445
		Example: 80, 443, 5000-5010
		< Back Next > Cancel
		Town Control
1		

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.

Enable Remote WMI

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 o	create.
Steps: Predefined Rules Action	What type of rule would you like to create? Pogram Rule that controls connections for a program. Pol Rule that controls connections for a TCP or UDP pot. Prodefined: Windows Management Instrumentation (WMI) Rule that controls connections for a Windows experience. O pation 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.

Enable ICMP Echo (Ping)

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: Pule Type Program	To which ports and pr	otocols does this rule apply?
 Protocol and Ports Scope Action 	Protocol type: Protocol number:	ICMPv4 v
ProfileName	Local port:	All Ports
	Remote port:	All Ports v Example: 80, 443, 5000-5010
	Internet Control Mess (ICMP) settings:	age Protocol Qustomize
		< Back Next > 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	
Specific ICMP types	
Packet Too Big Destination Unreachable Source Quench Redirect	
Cho Request Router Advertisement Router Solicitation Time Exceeded Parameter Problem Timestamp Request Address Mask Request	
This ICMP type: Type: 0 V Code: Any V Add	
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**.



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

Configure SQL

Configuring your Recast tools to query the ConfigMgr SQL database directly for some actions can speed up actions and help with WMI quota violations. Configuring your tools to access your MBAM Recovery and Hardware database to query RecoveryKey IDs will help with the MBAM Dashboards and with the Security Tools management of BitLocker keys. These SQL options offer enhanced performance for larger environments and large datasets.

The method you'll follow for SQL configuration depends on whether you're using Right Click Tools Enterprise with Recast Management Server or in Standalone mode.

Right Click Tools with Recast Management Server

ConfigMgr and MBAM databases are automatically detected during Recast Management Server installation. You can also add or edit database details on the **Service Connections** page in your Recast Management Server. See Service Connections.

Right Click Tools Standalone

If you are running Right Click Tools in Standalone mode, you'll need to enter SQL and MBAM database information in the Configure Recast Console Extension application.

To open the Configure Recast Console Extension application, open the Windows Start menu and select **Configure Recast Console Extension**.

TIP: You can also access the Configure Recast Console Extension application from your Configuration Manager console by navigating to **Assets and Compliance** > **Recast Software** and clicking **Configure Recast** in the 'How Can We Help?' section.



To enter SQL and MBAM database information for Right Click Tools Standalone:

1. Open the SQL tab.				
Configure Recast Console Extension General Licencing SOL Wake On Lan Windows Evolution	Service Now Interactive	- Command P		×
Configure your Reset tools to optionally query the ConfigMe help with some WMI quota violation issues and may speed up SQL Server: SQL Database:	r SQL database directly for some of the actions.	r some action	s. This sl	hould
Configure your Recast tools to access to your MBAM Recover linked to a device for use in requesting recovery keys from the	y and Hardware database e MBAM Administration V	to query Reco Veb Service.	veryKey	IDs
MBAM Administration URI:				
SQL Server:				
MBAM Recovery and Hardware DB:				
MBAM Compliance Status DB:				
		Caus	C	
By Recast Software		JodVe	U	use

2. Enter the following details:

- SQL Server: FQDN of the Server that hosts the SQL database for ConfigMgr
- SQL Database: Name of the database hosted on the above server (usually CM_Three letter site code)

3. If you have MBAM in your environment, enter:

- **MBAM Administration URI**: Administration URI for your MBAM server, the address is usually correct after the FQDN is entered unless it was changed at the time of installation
- SQL Server: FQDN of the server that hosts the SQL Database for MBAM
- MBAM Recovery and Hardware Database name (default name is entered)
- MBAM Compliance Status Database name (default name is entered)

4. Click Save.

Configure Wake on LAN (WOL)

Wake on LAN settings impact all WOL packets sent by Recast.

Right Click Tools with Recast Management Server

If you are using Right Click Tools Enterprise with Recast Management Server, Wake on LAN settings can be configured in the Settings section of the Recast Management Server interface.

To configure Wake on LAN options in RMS:

1. In your Recast Management Server, navigate to **Administration** > **Settings**.

2. Under **ConfigMgrServer** options, configure the following settings:

- WakeOnLanPort: Sets the UDP port from which WoL packets will be sent.
- Unicast: Determines if WoL packets are sent with unicast or subnet directed broadcasts.
- NumberOfPackets: Sets the number of WoL packets to send when trying to wake up devices.

Right Click Tools Standalone

If you are running Right Click Tools Enterprise in Standalone mode, you can set Wake on LAN options in the Configure Recast Console Extension application.

To open the Configure Recast Console Extension application, open the Windows Start menu and select **Configure Recast Console Extension**.

TIP: You can also access the Configure Recast Console Extension application from your Configuration Manager console by navigating to **Assets and Compliance** > **Recast Software** and clicking **Configure Recast** in the 'How Can We Help?' section.

← → - 🔍 \ → Assets and Compliance →	Overview + Recast Software +				
Assets and Compliance					
Subst	Welcome to Right Click To You currently have access to our ent We're here to help you get the most contact our Customer Success Team Contact Support	Hols re feature set of 80+ tools included in i out of our tools. If you have questions	the Right Click Tools Enterprise Edition. or feedback at any time, please	Installation Informati Desktop Installed Version: Server Installed Version: Enterprise License: License Expiration Date: Remote Server Status: License Org:	01 5.2.207.703 5.2.207.703 6.2 6 6 10/7/2023 Connected Preset Software
Endpoint Protection All Corporate-owned Devices Recast Software	Getting Started Check out some of our most used to productivity, and automate complex	ols and dashboards created to surface workflows.	more actionable insights, improve	How Can We Help?	
Stand and Company	Software Update Deployment Status (SUDS) Run a highly-targeted scan of software update deployment compliance, returning results in	LAPS Dashboard Surfaces compliance data about the Microsoft LAPS tool. The scan can be directed at a specific Domain, OU, and/or Collection.	Active Directory Cleanup Dashboard Scans Configuration Manager and Active Directory for devices. showing results about where	Configure Recast	Contact Support
Software Library	two categories: compliance by device and non-compliant devices by update category.	Results are returned in a simple LAPS Present/Not Present chart Expand this node to view the	those devices are: in just ConfigMgr, just AD, or (properly) in both.		
Administration	Expand this node to view the dashboard Enterprise Tool	dashboard Enterprise Tool	Expand this node to view the dashboard Emergine Tool	Documentation	Enterprise Portal
20 Community				0	Contraction of the local division of the loc

To configure Wake on LAN options in Configure Recast Console Extension:

1. Open the **Wake On Lan** tab.

Configure	e Recast C	onsi	ole Extension					×
General Lice	ensing S	QL	Wake On Lan	Windows Explorer	Service Now	Interactive Command P	rompt	
These setting	These settings will affect all WOL packets sent by Recast. They will have no effect on the settings in the console.						s	
				Unicast	Mode			
				Port to use:)			
			Number of	Packets to send:				
By Recast Soft	ware					Save	Clo	se

2. Enable Unicast Mode to send Wake on LAN packets with unicast or subnet directed broadcasts.

3. Set the Port to use and the Number of Packets to send when trying to wake up devices.

4. Click Save.

Configure 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. Open the Configure Recast Console Extension application by clicking the Windows Start menu and selecting **Configure Recast Console Extension**.

TIP: You can also access the Configure Recast Console Extension application from your Configuration Manager console by navigating to **Assets and Compliance** > **Recast Software** and clicking **Configure Recast** in the 'How Can We Help?' section.

🗲 🌛 🔹 🏨 🛝 + Assets and Compliance					
Assets and Compliance					
© Collini	Welcome to Right Click To You carrently have access to our ent We're have to hely you get the most contact our Customer Success Team Contact Support	bols re feature set of 80+ tools included in out of our tools. If you have questions	the Right Click Tools Enterprise Edition, or feedback at any time, please	Installation Informati Desktop Installed Version: Serve Installed Version: Enterprise License License Expiration Date: Romote Server Status: License Org:	ON 52207703 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 52207700 SC 5200 SC 5200 SC 5200 SC 5200 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC 5070 SC SC 5070 SC SC SC SC SC SC SC SC SC SC
All Corporate-owned Devices All Recent Software	Getting Started Check out some of our most used to productivity, and automate complex	ols and clashboards created to surface workflows.	more actionable insights, improve	How Can We Help?	
Assets and Compliance	Software Update Deployment Status (SUDS) Run a highly-targeted scan of software update deployment compliance, returning results in two categories compliance by	LAPS Dashboard Surfaces compliance data about the Microsoft LAPS tool. The scan can be directed at a specific Dominn, OLJ, and/or Collection. Pareith sea returned in a simple	Active Directory Cleanup Dashboard Scans Configuration Manager and Active Directory for devices, showing results about where those devices are in a set	Configure Recast	Contact Support
Software Library	device and non-compliant devices by update category. Expand this node to view the dashbaari	LAPS Present/Not Present chart Expand this node to view the dashboard	ConfigMgr, just AD, or (properly) in both. Expand this node to view the dashboard	Documentation	Enterprise Portal
S Community	Secreption Tool		Enterprice Tool	-	

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.

Configure Recast	Cons	ole Extension				-		×
General Licensing	SQL	Wake On Lan	Windows Explorer	Service Now	Interactive	Command P	rompt	
Interactive Commar If you already have	id Pro it dow	mpt relies on Ps mloaded, you ca	Exec to run. Please o an just browse for it.	download it an	d find the fil	e with the br	owse bi	utton.
			Downloa	d				
Local Path:							Bro	wse
By Recart Software						Save	0	lose

4. Save your changes.

Copyright © 2025 Recast Software Inc. All rights reserved.