Prerequisites for Right Click Tools, Insights & Patching

Last Modified on 2026-11-05

Before starting the implementation workflow, ensure that your system meets the following hardware, software, network, and certificate requirements for Recast Management Server, Right Click Tools, RCT Patching, and RCT Insights.

Hardware Requirements

> The Recast Management Server hardware requirements listed in this document are meant to guide the setup of a simple Recast environment for all Recast Software products or add-ons that connect to a Recast Management Server. These guidelines assume that all default settings are used, that the server has Internet access, and that your environment includes fewer than 20K Agents.
> For larger or more complex environments, refer to the comprehensive list of RMS System Requirements.

Physical or virtual server sized as follows:

- 8-core CPU
- 28 GB RAM
- 2 GB of Disk Space on the C: drive

NOTE: Additional disk space required for the Recast Management Server database or for Application Manager does not need to be located on the C: drive.

Software Requirements

Recast Management Server	Supported version of Microsoft Windows Server (Windows Server 2025 recommended) Microsoft .NET 10 Supported version of Microsoft SQL Server Standard (SQL Server Standard 2025 recommended)
Right Click Tools Console Extension	Supported version of Microsoft Configuration Manager Supported version of Windows 11
Right Click Tools Patching	Supported version of Microsoft Configuration Manager
Right Click Tools Insights	Supported version of SQL Server Reporting Services Power BI Report Server September 2022 version or later

Network Requirements

Inbound Network Traffic

The default network port for inbound network traffic to the Recast Management Server is TCP/444.If you change the port for the website, this firewall rule must be changed to match.

External Domains

Recast Management Server and/or Recast Proxy require outbound access to the following external domains.

Recast license activation	• https://activation.recastsoftware.com
Right Click Tools Enterprise Intune- and Entra-Specific Tools	• https://login.microsoftonline.com – for Entra ID authentication • https://graph.microsoft.com – to connect to the Microsoft Graph REST API
Right Click Tools Insights warranty information collection	Recast Management Server requires outbound access to the Warranty API at: • https://warranty.recastsoftware.com (TCP/443)
Right Click Tools Insights warranty information for devices managed in Intune and access to the Warranty Information dashboard	Recast Proxy requires outbound access to: • https://login.microsoftonline.com (TCP/443) – for Entra ID authentication • https://graph.microsoft.com (TCP/443) – to connect to the Microsoft Graph REST API
Right Click Tools Patching Enterprise	Recast Management Server and Recast Proxy require outbound access to: • https://amprod02.recastsoftware.com (TCP/443) – to access the application catalog • https://amprodpub02.recastsoftware.com (TCP/443) – to download application media and icons
RCT Patching Standard	Recast Management Server and Recast Proxy require outbound access to: • https://amprod01.recastsoftware.com (TCP/443) – to access the application catalog • https://amprodpub01.recastsoftware.com (TCP/443) – to download application media and icons
RCT Patching Intune integrations only	Recast Proxy requires outbound access to: • https://login.microsoftonline.com (TCP/443) – for Entra ID authentication • https://graph.microsoft.com (TCP/443) – to connect to the Microsoft Graph REST API

WebSockets

Your Recast Management Server and Recast Agents communicate with one another using WebSockets. To ensure successful communication, you may need to enable WebSocket communications.

Certificate Requirements

Recast Software strongly recommends using public certificates or Active Directory certificates (AD CS).

The certificate's subject name (or a subject alternative name) should match the server name in the URL to which Right Click Tools and/or Recast Proxies are pointed.

Proxy Permissions for Right Click Tools, Insights & Patching

Right Click Tools

Recast

Access web dashboards and trends Schedule Builder actions Schedule kiosk profile application	• Local admin access on the server where the proxy is being installed • Read permissions in Active Directory • **db_datareader** in the Configuration Manager SQL server database • Read-only access to the Configuration Manager console (**Read-only Analyst** security role in ConfigMgr)
Run actions as a service account	• Local admin access on any device that actions will be run against • Read/Write permissions in Active Directory (Write only required to delete devices from AD) • Appropriate ConfigMgr Security Role for intended actions in the Configuration Manager console (Full Administrator for all actions) • Permission to MBAM, if applicable
Elevate permissions	• Local admin access on all devices managed by Right Click Tools
Add or remove from collections	• Permission to modify a collection in Configuration Manager configmgr collection > modify permission
Run actions over Fast Channel	• Permission to run scripts in Configuration Manager • If using **Read-only Analyst** in ConfigMgr as your base security role, also grant the following privileges: Collection > Run Script = Yes SMS Scripts > Read = True
Run Intune- and Entra-Focused Tools	• Add permissions specified for each action to Graph API permissions Access to the necessary external domains: • https://login.microsoftonline.com – for Entra ID authentication • https://graph.microsoft.com – to connect to the Microsoft Graph REST API

Right Click Tools Insights

To collect warranty information	• Local admin access on the server where the proxy is being installed • Read permissions in Active Directory • **db_datareader** in the Configuration Manager SQL server database • Read-only access to the Configuration Manager console (**Read-only Analyst** security role in ConfigMgr) **NOTE**: These permissions match those required to access web dashboards and trends in Right Click Tools • Internet access for the proxy account in order for the Recast Management Server to reach our API at **https://warranty.recastsoftware.com** over TCP 443
To collect warranty information if RMS is installed on a server other than your ConfigMgr SQL database	• Add proxy account to the **SMS_SiteSystemToSiteServerConnection_MP_<YourSiteCode>** local group on that server, allowing it to read/write to your **inboxes\auth\ddm.box**
Collect warranty information for devices managed in Intune and view that information on the Warranty Information dashboard	• Add Application permission to Graph API permissions: **DeviceManagementManagedDevices.Read.All**

Recast

Right Click Tools Patching

Configuration Manager Integration	• Grant any of the following built-in roles/role combinations to the proxy account:
	  ◦ Full Administrator
	  ◦ Operations Administrator
	  ◦ Application Administrator **and** Compliance Settings Manager
	  ◦ Application Administrator **and** Read-only Analyst
	• Grant modify permissions to the SMB share (UNC path) that will be used to store downloaded applications
	• Access to the necessary external domains. See System Requirements.

Intune Integration	• Grant modify permissions to the SMB share (UNC path) that will be used to store downloaded applications • Access to the necessary external domains. See System Requirements.
Software Updates in ConfigMgr	• Add proxy account as a member of the WSUS Administrators on the server where WSUS connected to ConfigMgr is located • Add proxy account as a member of the local Administrators group on the WSUS server. If security policies does not allow this, you can work around the requirement by granting the proxy account full control over specific items that allow package publishing. • Install the RSAT Windows Server Update Services Tools feature on the Recast Proxy server and restart the Recast Proxy service. PowerShell command: • `Install-WindowsFeature -Name UpdateServices-RSAT -IncludeAllSubFeature`

NOTE: Group Managed Service Accounts (gMSAs) are not currently supported.

API Permissions for Right Click Tools, Insights & Patching

Specific Microsoft Graph API permissions are required for individual Entra/Intune features in Right Click Tools, as well as for access to all features in Right Click Tools Patching and Right Click Tools Privileged Access.

Right Click Tools

Add Devices to Entra Group	Application permissions • Device.Read.All • Device.ReadWrite.All • Group.Read.All • Group.ReadWrite.All
Delete Device(s) From Azure (Intune/Entra)	Application permissions • DeviceManagementManagedDevices.ReadWrite.All – for deleting devices from Intune • Device.ReadWrite.All – for deleting devices from Entra

Entra ID BitLocker Recovery Keys	Application permission • Device.Read.All • BitlockerKey.Read.All • BitlockerKey.ReadBasic.All Delegated permissions • User.Read • DeviceManagementConfiguration.Read.All • DeviceManagementManagedDevices.Read.All
Autopilot Actions Register Device(s) in Autopilot Set Autopilot Group Tag Remove Device(s) from Autopilot	Application permission • DeviceManagementServiceConfig.ReadWrite.All • DeviceManagementManagedDevices.Read.All **or** DeviceManagementManagedDevices.ReadWrite.All
Retrieve All LAPS Passwords (to retrieve passwords from Entra ID)	Application permission • DeviceLocalCredential.Read.All

Right Click Tools Insights

Collect warranty information for devices managed in Intune	Application permissions • DeviceManagementManagedDevices.Read.All

Right Click Tools Privileged Access

For all Privileged Access features	Application permissions • Device.Read.All • GroupMember.Read.All • User.Read.All

Right Click Tools Patching

For all Patching features	Application permissions • DeviceManagementApps.ReadWrite.All • GroupMember.Read.All • DeviceManagementConfiguration.Read.All – required to test an integration • Device.Read.All – required to test the Azure Active Directory (Entra ID) service connection