Prerequisites for Right Click Tools, Endpoint Insights & Application Manager

Last Modified on 02.10.25

Recast component, product, and proxy permission requirements for the Essentials Bundle (RCT, EI, AM).

Before starting the multi-product implementation workflow, ensure that your system meets the following hardware, software, network, and certificate requirements for Recast Management Server, Right Click Tools, Application Manager, and Endpoint 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 that connect to 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
- 512 GB of Disk Space on the C: drive

Software Requirements

Recast Management Server	Supported version of Microsoft Windows Server (Windows Server 2022 recommended) Microsoft .NET Framework Version 8 Supported version of Microsoft SQL Server Standard (SQL Server Standard 2022 recommended)
Right Click Tools Console Extension	Supported version of Microsoft Configuration Manager Supported version of Windows 10 or later
Application Manager	Supported version of Microsoft Configuration Manager

Endpoint 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.

External Domains

Recast Management Server requires outbound access to the following external domains.

Recast license activation	https://activation.recastsoftware.com
Endpoint Insights warranty information collection	One-way from RMS to the API at https://warranty.recastsoftware.com (TCP/443)
Application Manager Enterprise	https://amprod02.recastsoftware.com (TCP/443) - to access the application catalog https://amprodpub02.recastsoftware.com (TCP/443) - to download application media and icons
Application Manager Standard	https://amprod01.recastsoftware.com (TCP/443) - to access the application catalog https://amprodpub01.recastsoftware.com (TCP/443) - to download application media and icons
Application Manager for Intune	https://login.microsoftonline.com (TCP/443) - for Entra ID authentication https://graph.microsoft.com (TCP/443) - to connect to the Microsoft Graph REST API

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.

Recast Proxy Permission Requirements

Right Click Tools

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
Fast Channel support	• 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

Endpoint 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**

Application Manager

MECM 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
	• Modify permissions to the SMB share (UNC path) that will be used to store downloaded applications
	• Internet access for the proxy account used to access the application catalog, check for new application versions, and download application media and icons.