Recast

Recast Management Server System Requirements

Last Modified on 2026-11-05

Before installing Recast Management Server, ensure that your system meets the following hardware, software, network, and certificate requirements.

Hardware Requirements

The Recast Management Server can run on a physical server or a virtual server in an on-premises or cloud-hosted environment (Azure/AWS/GCP/etc.). The server requires local network access. Internet is not a mandatory; however, some features, such as warranty information collection, require internet access.

CPU

Agents Deployed	CPU
< 10K	4-core minimum, 8-core preferred
10K – 20K	8-core minimum, 12-core preferred
> 20K	8-core minimum, 12-core preferred, with an additional Agent Gateway required on a different server. CPU requirements for each additional Agent Gateway server will depend on the number of Agents connected.

RAM

System Component	Recommended Minimum
Operating System	4 GB
RMS (core features)	4 GB
Recast Proxy	256 MB
Agent Gateway	12 GB
SQL Server	8 GB

Examples

For a system with RMS, Proxy and Gateway located on the same server:
4 GB for the OS + 16 GB for RMS/Proxy/Gateway = 20 GB Total

For a system with SQL Server, RMS, Proxy and Gateway located on the same server:
4 GB for the OS + 8 GB for SQL + 16 GB for RMS/Proxy/Gateway = 28 GB Total

Disk Space

NOTE: All Recast products currently install on the C:drive.

System Component	Recommended Minimum
RMS (core)	1GB
Recast Proxy	512 MB
Agent Gateway	512 MB

Recast

System Component	Recommended Minimum
SQL Server	50 GB for database files, no snapshots, no limiting rules (formerly known as scopes) 100 GB for database files, with snapshots and/or limiting rules Plus 1MB of storage per device

Agent Gateway Servers

The Recast Agent Gateway can run on a physical server or a virtual server in an on-premises or cloud-hosted environment (Azure/AWS/GCP/etc.). One Agent Gateway is required for every 20K Recast Agents deployed. One Agent Gateway is automatically deployed during Recast Management Server installation. Each additional Agent Gateway must be installed on a different server. The Agent Gateway server can be shared with a Recast Proxy. The Agent Gateway may be load balanced to allow for a single URI for both on-premises and cloud devices.

Hardware and Network Requirements for Additional Agent Gateway Servers

- 4-core minimum with 16 GB of RAM (4 GB for the OS + 12 GB for the Agent Gateway)
- No SQL server required
- Firewall Rules:
  - Inbound – Required, default is TCP/444
  - Outbound – The Agent Gateway server requires access to Recast Management Server on RMS' default port (TCP/444)

SQL Server

For new implementations, we recommend installing the latest version of SQL Server (SQL Standard or Enterprise). The Recast Management Server can use any Microsoft SQL Server version covered by Mainstream or Extended support; however, SQL Express can only be used at the Proof of Concept stage. We advise against hosting SQL Express and any other SQL Server edition on the same server.

The Recast Management Server supports SQL Always On (SQL OA). Additional configuration may be required.

NOTE: For the **RecastManagementServer** database only, the SQL **Compatibility level** must be set to at least 'SQL Server 2017'. For instructions to view or edit the SQL compatibility level, see RMS Database Migrations Not Applied.

For more information, see Manually Configure SQL Server Permissions and Install Recast Management Server with Azure SQL Managed Instance.

Software Requirements

Operating System: Microsoft Windows Server versions covered by Mainstream or Extended support

Microsoft .NET: Version 10

IIS: Should install automatically during Recast Management Server installation, if it is not present. Otherwise, you can enable IIS manually in Server Manager.

ASP.NET Hosting Bundle: Should install automatically during Recast Management Server installation, if not already present. You can also install the Hosting Bundle manually in Server Manager. If manually installed, the Hosting Bundle should be enabled after IIS.

Network Requirements

Recast

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

The Recast Management Server requires certificates. Recast Software strongly recommends using public certificates or Active Directory certificates (AD CS).

Recast

If no certificate is specified during Recast Management Server installation, a self-signed certificate is created and used. Self-signed certificates must be added separately to the Trusted Root Certificate Authorities store on devices running Right Click Tools, Recast Agent, or Recast Proxy, as these are not deployed by RMS or Recast Agent.

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.