Recast Management Server System Requirements

Last Modified on 12.16.24

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 be either a physical or a virtual device with 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
SQL Server	50 GB for database files, no snapshots 100 GB for database files, with snapshots

Agent Gateway Servers

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-supported version of SQL Server; 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.

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 2016 or later

Microsoft .NET Framework: Version 8

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

Inbound Network Traffic

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

External Domains

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

For Recast license activation

- https://activation.recastsoftware.com

For Endpoint Insights warranty information collection

- https://warranty.recastsoftware.com (TCP/443)

For Application Manager

MECM and Intune Integrations

Application Manager checks for new application versions over the Internet and downloads application media from Azure using the HTTPS protocol over TCP/443.

Recast Management Server and Recast Proxy require outbound access to the following external domains:

Application Manager Enterprise

- https://amprod02.recastsoftware.com - to access the application catalog
- https://amprodpub02.recastsoftware.com - to download application media and icons

Application Manager Standard

- https://amprod01.recastsoftware.com - to access the application catalog
- https://amprodpub01.recastsoftware.com - to download application media

Intune Integrations Only

For Intune integrations of Application Manager, the Recast Proxy requires outbound access to the following domains over TCP/443:

- https://login.microsoftonline.com - for Entra ID authentication
- https://graph.microsoft.com - to connect to the Microsoft Graph REST API

Certificate Requirements

The Recast Management Server requires certificates. Recast Software recommends using public certificates or Active

Directory certificates (AD CS).

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.