Endpoint Insights with RMS

Last Modified on 04.01.25

Implementation Workflow for Endpoint Insights with RMS

If you plan to collect warranty information, you'll need to install Endpoint Insights with Recast Management Server and Recast Proxy. To install Endpoint Insights on its own, see Install Endpoint Insights Standalone.

To install Endpoint Insights along with Right Click Tools and Application Manager, see our Multi-Product Implementation Guide.

Before beginning installation steps, make sure that Endpoint Insights system requirements are in place.

Recommended workflow for Endpoint Insights with device warranty reports

1. Download the following Recast application and components from the Recast Portal:

   - Endpoint Insights
   - Recast Management Server
   - Recast Proxy

2. Install Recast Management Server with Recast Proxy on the primary Configuration Manager server or on its own server.

> If you've already installed Recast Management Server with a Recast Proxy for another Recast product, there's no need to reinstall RMS and Proxy to add Endpoint Insights.

3. Install Endpoint Insights with Recast Management Server on your Configuration Manager server.

4. Install the Recast Agent application.

Once you've completed these tasks, you're ready to configure Recast Management Server for warranty information collection.

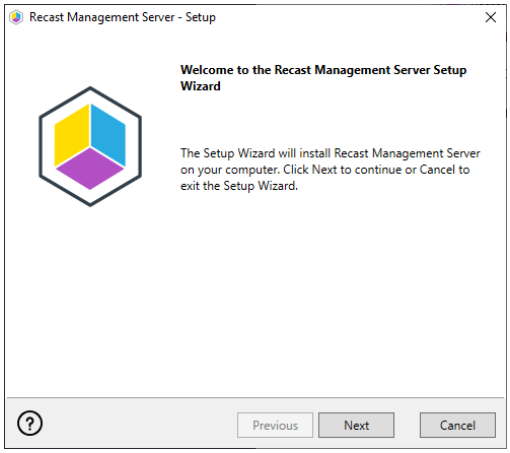
Install Recast Management Server with Recast

Proxy

Recast Management Server software can be installed on its own server or on the primary Configuration Manager server.

Run the Recast Management Server Installer

After downloading Recast Management Server from the Recast Portal, run the installer and follow its prompts.

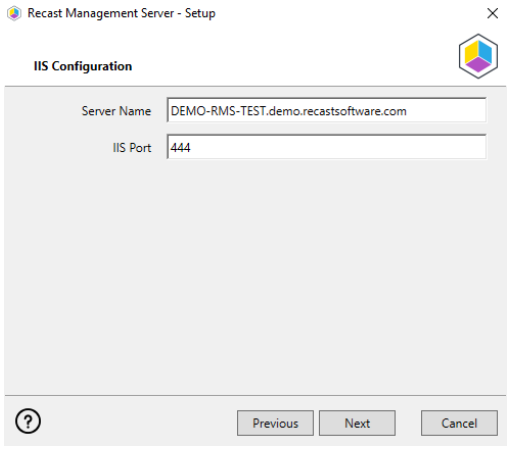


IIS

To configure IIS:

1. On the **IIS Configuration** page, change the **Server Name** only if the client is going to use a DNS alias.

2. Set the **IIS Port**. The default IIS Port is **TCP 444**, to prevent conflicts when Recast Management Server is installed on Configuration Manager servers. The IIS Port can be changed to 443, or any open TCP port, to suit your environment.



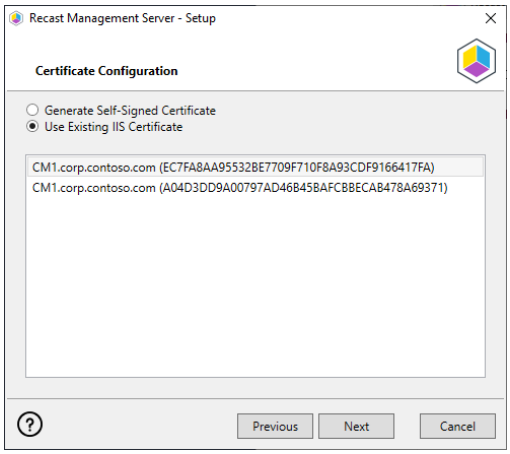
Certificates

Recast Management Server requires a certificate for secure communication with Right Click Tools and any Recast Proxies.

To configure a certificate:

On the **Certificate Configuration** page, we recommend that you **Use an Existing IIS Certificate** issued by a trusted

Certificate Authority (CA). If you choose to **Generate a Self-Signed Certificate**, you must import the Recast Management Server self-signed certificate to the Trusted Root Certificate Authorities store on devices running Right Click Tools, Recast Agent, or Recast Proxy.



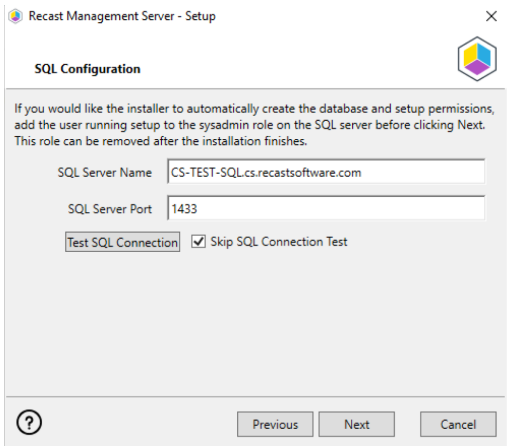
CERTIFICATE NOTES:

- The certificate subject name (or a subject alternative name) should match the server name in the URL that Right Click Tools and Recast Proxies are pointed toward.
- Right Click Tools will prompt for any untrusted certificates and add them to an allowed list.
- The certificate can be changed later by editing the Binding in IIS Manager.

SQL Server

There are two types of permissions that will allow the Recast Management Server installer to automatically create the SQL database with all the necessary permissions:

- The user account running the installation can be assigned a SysAdmin role in the SQL instance. If the user account has permission to connect remotely, use the **Test SQL Connection** button to check connectivity to the SQL Server during the install. After the RMS installer creates the database, the SysAdmin permission can be removed.
- The computer account of the Recast Management Server can be granted **db_creator** permissions. In this case, check the **Skip SQL Connection Test** box.



SQL SERVER NOTES:

- The default SQL Server Port Number is 1433.

- A fully licensed version of SQL is strongly recommended to avoid the 10GB storage limitation of SQLExpress.
- After the SQL database is created, set the database recovery model to simple to prevent storage issues.
- **Remote SQL Server**: The computer account of Recast Management Server will need db_owner permissions to create the database on the remote device. If the account running the Recast Management Server installer does not have permission to create a SQL database, the database administrator can pre-create the RecastManagementServer database and manually give the computer account db_owner permissions.
- **Local SQL Server**: The IIS AppPool\Recast Management Server account will need db_owner permissions to create the database on the local device. Alternatively, the database administrator can pre-create the database and give the IIS AppPool\Recast Management Server account db_owner permissions to the database. The IIS AppPool\Recast Management Server account will not exist until after the installation completes, so the permissions will need to be given after installation.

Import License

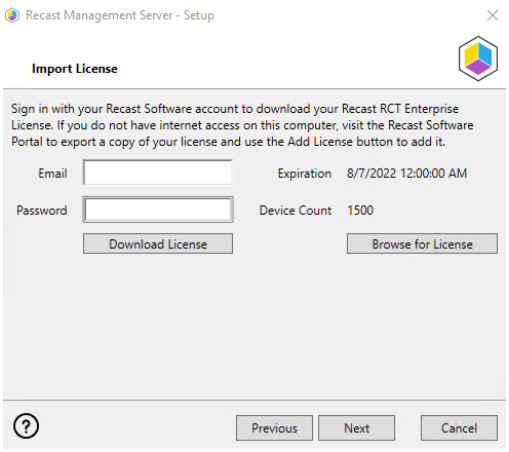
You can download and import your Recast licenses when installing Recast Management Server.

To download your Enterprise license:

1. On the **Import License** page, enter your Recast Portal email address and password.

2. Click **Download License**. The license information will appear in the right-hand column.

NOTE: If your server does not have internet access, click **Browse for License** to browse the filesystem for a license file that has been exported from the Recast Portal.



Proxy

If the Recast Proxy is being installed on a server other than the Recast Management Server, install the Proxy separately after Recast Management Server installation.

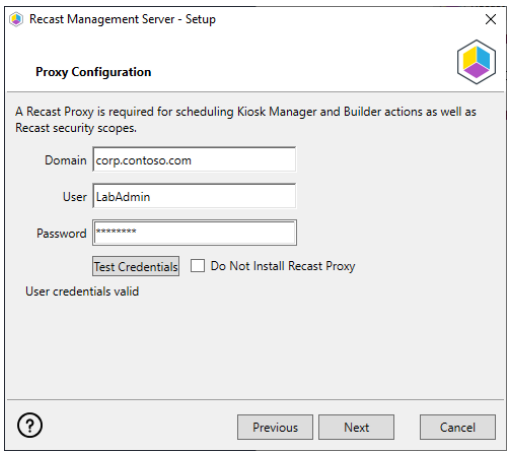
NOTE: Proxy configuration is optional for Privilege Manager where Active Directory or Microsoft Entra ID objects are not used to target rules.

To configure the proxy during RMS installation:

On the installer's **Proxy Configuration** page, enter the service account **Domain**, **User**name, and **Password** and click

Test Credentials to verify service account details.

TIP: If you haven't already set up the required proxy permissions, remove any information from the text fields, select **Test ConfigMgr Connection** and the **Skip ConfigMgr Verification** checkbox, and click **Next.**

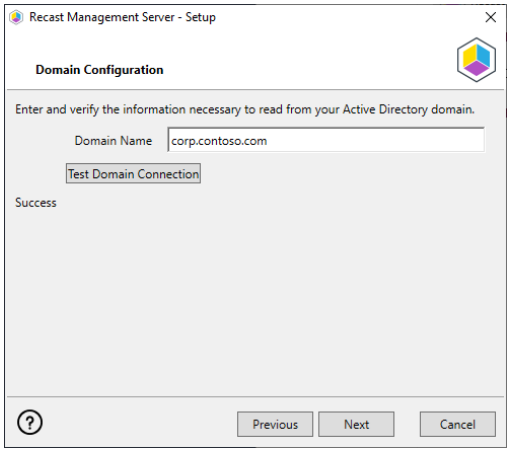


Domain

To configure your domain:

1. On the **Domain Configuration** page, enter the **Domain Name**.

2. Click **Test Domain Connection** to verify that the service account has access to read from your domain.



Configuration Manager

NOTE: Configuration Manager does not need to be set up for Privilege Manager.

To set up your Configuration Manager for the proxy:

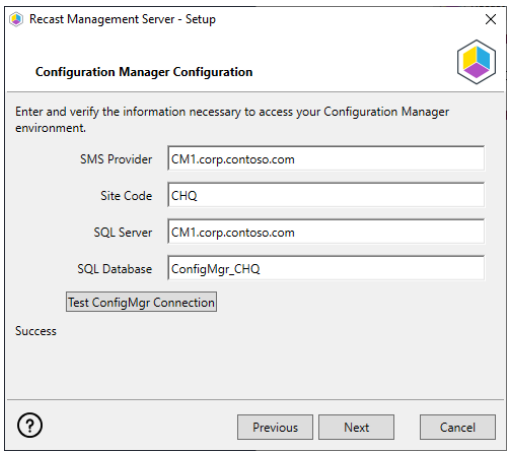
1. On the **Configuration Manager Configuration** page, enter the following information:

- Name of the site server that has your **SMS Provider** role
- **Site Code**
- Name of the **SQL Server** where your Configuration Manager SQL database is located
- **SQL Database** name

  NOTE: You can skip the **Configuration Manager Configuration** page during Recast Management Server or Recast

Proxy installation by removing any information from the text fields, selecting **Test ConfigMgr Connection** and the **Skip ConfigMgr Verification** checkbox, and clicking **Next.**

2. Click **Test ConfigMgr Connection** to check that the service account has access.



MBAM

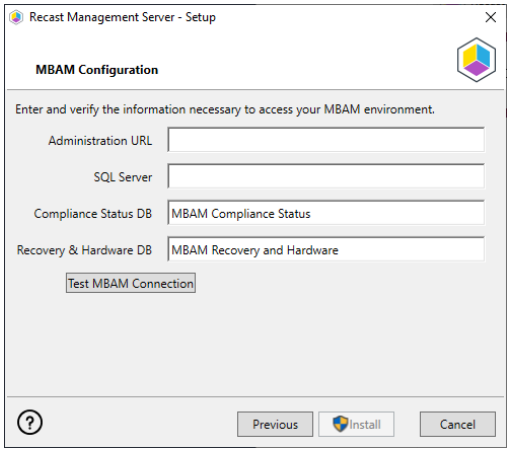
MBAM configuration is only required for a separate MBAM Server. If you are using the ConfigMgr-integrated BitLocker or AD, you can skip this section. MBAM also does not need to be configured for Privilege Manager or Application Manager.

To configure MBAM:

1. Tap **Click Here to Configure MBAM.**

2. Add your **Administration URL** and **SQL Server** information.

3. Click **Test MBAM Connection** to verify that the service account has access to MBAM.



Initiate RMS Installation

Once you have filled in all the necessary information, click **Install** at the bottom of the **MBAM Configuration** page.

When the installation is complete, open the Recast Management Server by navigating to `https://ServerFQDN:Port` in a web browser (Chrome, Edge, or Firefox are recommended).

When asked to sign in, enter the username and password for the account used to install the Recast Management Server.

Installation Log Location

To check the installation logs for Recast Management Server and Recast Proxy (when installed together), navigate to `C:\Users\user account running the install\AppData\Local\Temp`

NOTE: The log is named something like Recast_Management_Server_2022*****.log

---

Install Endpoint Insights with Recast Management Server

Installing Endpoint Insights with Recast Management Server and Recast Proxy allows you to collect the warranty data that populates EI's device warranty reports.

Endpoint Insights must be installed on your Configuration Manager server after you've installed Recast Management Server with Recast Proxy. See the Endpoint Insights Implementation Workflow for an overview of deployment and configuration steps.

During installation, Endpoint Insights completes the following tasks:

- Imports SQL Server Reporting Services (SSRS) reports, Power BI Report Server (PBRS) report sets, and Power BI desktop report sets
- Imports client settings to extend the hardware inventory
- Creates a Configuration Manager application for Recast Agent
- Via Configuration Manager methods (API), creates warranty details to allow the warranty date to be stored in the ConfigMgr database

Prerequisites

- For a remote SSRS/PBRS reporting point, the Configuration Manager Primary Site Server's computer account requires SysAdmin permissions on each remote database during the installation. These permissions can be removed after Endpoint Insights is installed.
- We recommend setting a static port on the remote SSRS/PBRS servers. If there are multiple reporting points, configure them all to use the same port, as only a single port can be defined during installation.

Run the Endpoint Insights Installer

To install Endpoint Insights:

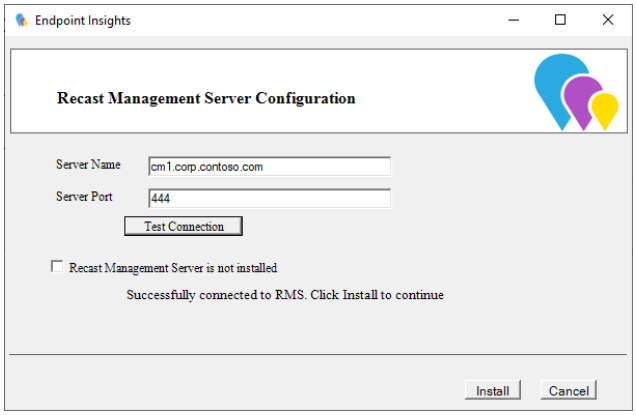
1. Download and run the Endpoint Insights installer.

2. Under **Recast Management Server Configuration**, enter the **Server Name** and **Server Port**.

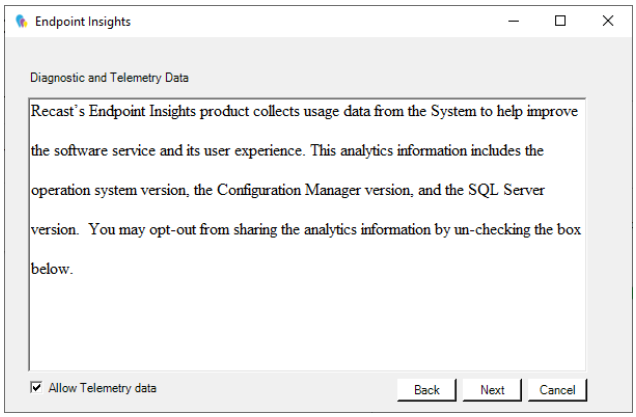
3. Click **Test Connection.** When connected, click **Next**.

4. Make sure **Recast Management Server is not installed** remains unchecked.

5. Click **Install**.



6. Enable **Allow Telemetry data** to allow the collection of the operating system version, the ConfigMgr version, and the SQL Server version during Endpoint Insights Setup (optional). Click **Next**.

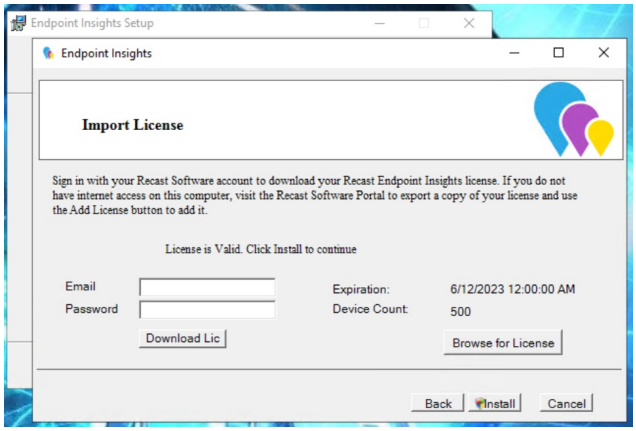


NOTE: Once Endpoint Insights Setup is complete, EI does not continue to collect usage data.

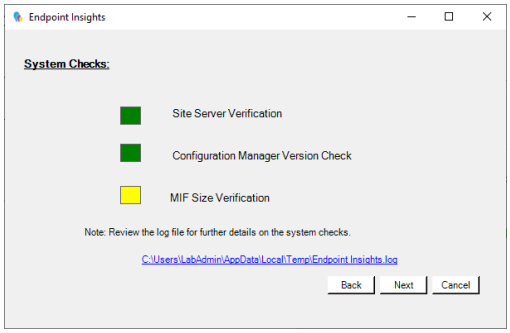
7. On the **Import License** page, enter your Recast Portal credentials, or browse to a previously downloaded license file.

> **NOTE**: The **Import License** page will not appear if licensing was configured during Recast Management Server installation.

8. Click **Install**.



The Endpoint Insights System Checks will run and report any issues with installing Endpoint Insights in your environment.

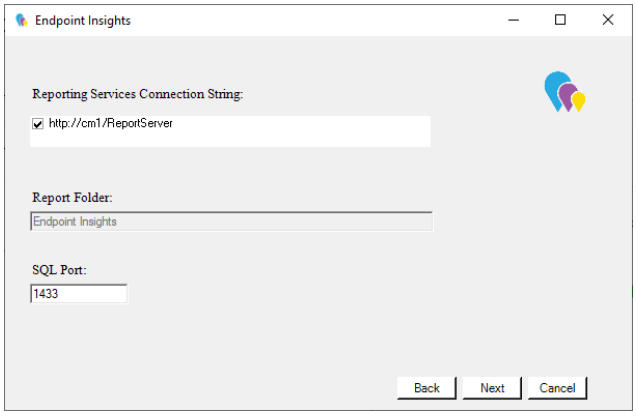


If MIF Size displays as an issue, you can increase the MIF size. To learn more, see Change the Maximum File Size of a MIF .

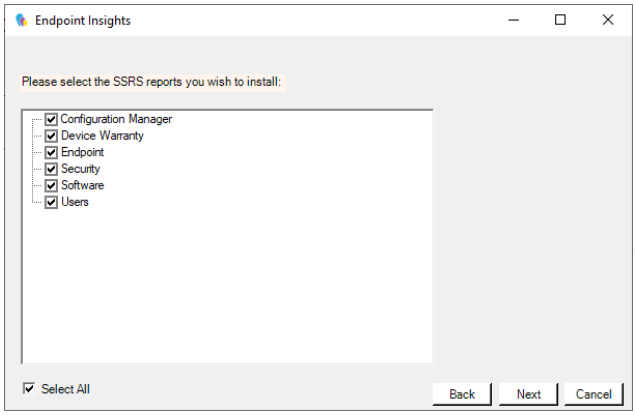
9. On the options page, you can set the following Endpoint Insight options.

- Select **Configure hardware inventory to import ER settings** to upgrade from Enhansoft Reporting to Recast Endpoint Insights.
- Select **Create Application** to automatically create the Recast Agent application in Configuration Manager.
- Select **Create Reports** to create the reports that display data collected by Endpoint Insights.
- De-select **Do not create RBA reports** only if your organization does not require role-based access on the Endpoint Insights reports.
- Enter a **SSRS Reader Group** to give an Active Directory group access to read SSRS reports.
    - To leave the SSRS Reader Group field blank, click **No** when prompted.
    - You can add the SSRS Reader Group later by re-running the EI setup.

10. Verify that the **Reporting Services Connection String**, **Report Folder** and **SQL Port** are correct for your environment. Click **Next**.



11. De-select any report categories to exclude from this installation. Click **Next**.



When setup completes, configure Asset Intelligence in your Configuration Manager to ensure that all data is returned to Endpoint Insights.

> **NOTE**: Once Recast Management Server and Endpoint Insights are installed, you may be tempted to kick off an Endpoint Insights warranty scan on the RMS **Warranty** page. Because Endpoint Insights relies on Recast Agent and Configuration Manager hardware inventory, you'll need to wait for Recast Agent software to be deployed to your end clients and for the next hardware inventory cycle to return inventory. The default hardware inventory setting within Configuration Manager is 7 days. It's recommended to reduce that to daily. For additional information, see ConfigMgr Inventory Cycle Recommendations.

Install Recast Agent for Endpoint Insights

Installing Endpoint Insights creates a Configuration Manager application for Recast Agent. Using a Recast Agent with Endpoint Insights creates additional hardware inventory classes on each machine. The extra classes populate related Endpoint Insights reports.

That same Recast Agent can be used with other Recast Software applications, such as Right Click Tools and Privilege Manager. To learn more, see the Recast Agent Overview.

NOTES:

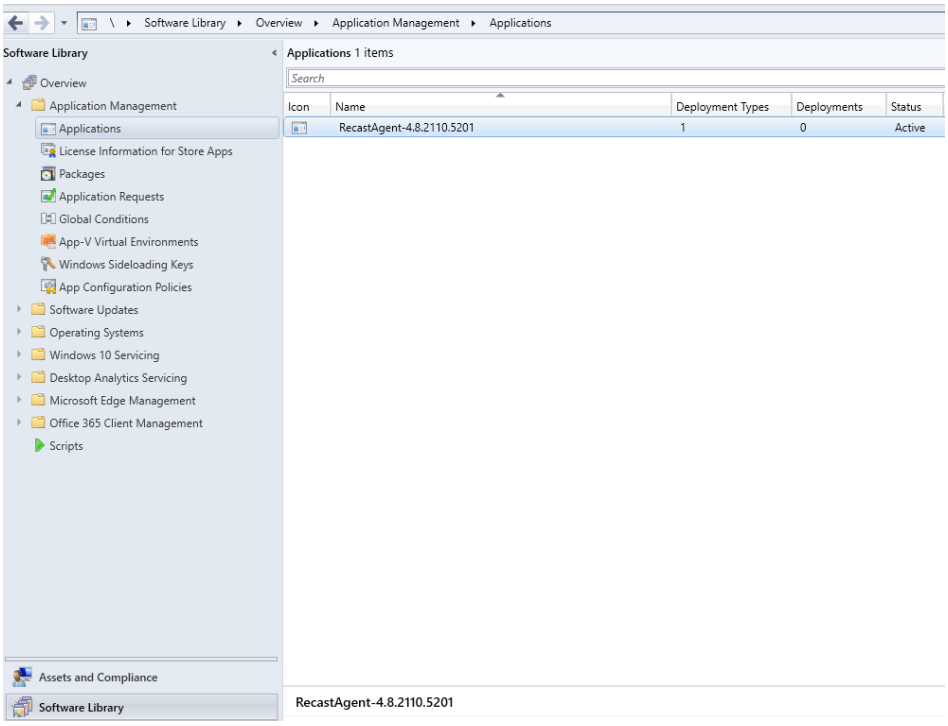
- If deploying 5000+ Recast Agents, follow the 503.2 IIS Error instructions before proceeding.
- If your Recast Management Server is using a self-signed certificate, you must first import the certificate into the Trusted Root Certificate Authorities Store on all devices that will have Agents.

To install the Recast Agent application for Endpoint Insights:

1. Open the Configuration Manager console.

2. Navigate to **Software Library** > **Application Management** > **Applications**. A **RecastAgent** application will be created.

3. Deploy the Agent as you would any other application.



NOTE: Recast Agents will take time to deploy and report their data back to the ConfigMgr database. By default, the hardware inventory cycle can take **up to 7 days**. Shortening the time to install and increasing the frequency of reporting back to ConfigMgr can shorten this time significantly.

Silent Install for Agent without Recast Management Server

If you are not connecting Recast Agents to Recast Management Server, use the **LICENSEPATH=** parameter to specify the license file to use for your Agent installation. This option will install the Full Agent on a device.

Example:

```
msiexec.exe /i "Recast Agent.msi" /qn LICENSEPATH=".\License\<their.license>"
```

NOTE: The license path can be a relative or full path.