Recast

Implementation Workflow for Right Click Tools, Insights & Patching

Last Modified on 11.24.25

With prerequisites in place, you're ready to install and configure Right Click Tools, Recast Management Server, Insights, and Patching one after the other.

Task 1: Install Right Click Tools Console Extension

To get you up and running with Right Click Tools Enterprise as quickly as possible, you'll first install the Right Click Tools Console Extension (aka Right Click Tools in Standalone mode). The Tools will be available in ConfigMgr—for users with Local Administrator permissions on target devices—while the prerequisites and permissions for other Recast components and/or products are being put in place.

Beginning with Recast Software Version 5.9.2503, you can install Right Click Tools, add the Right Click Tools browser extension, and run actions from within the Intune Admin Center on a device where no Configuration Manager console is present.

NOTE: When you enter your ConfigMgr site details during or after Right Click Tools installation (instructions below), you'll be able to run actions that require ConfigMgr information.

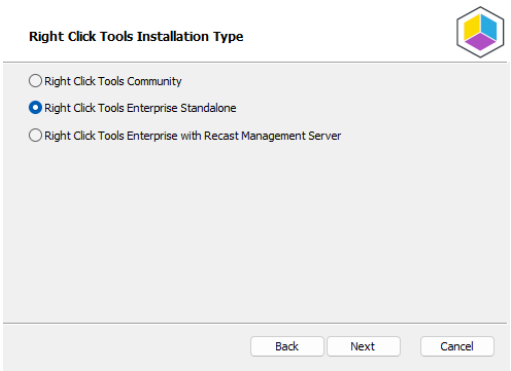
Run the Right Click Tools Installer

Make sure any Configuration Manager console installed on the device is closed before opening the installer.

To install the Right Click Tools console extension, double-click the .msi file to open the Recast Console Extension installer you downloaded from the Recast Portal.

Choose Installation Type

To choose a Right Click Tools installation type, click **Right Click Tools Enterprise Standalone**. Then click **Next**.



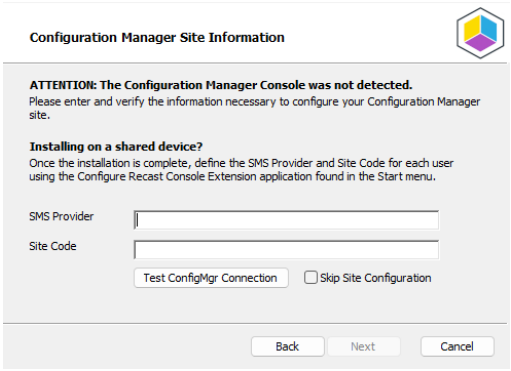
Add Configuration Manager Site Information

If you are installing Right Click Tools in order to use the browser extension on a device with no ConfigMgr console installed, you will need to add site information for the Configuration Manager console in your environment.

To add ConfigMgr site information:

1. Enter the **SMS Provider** and **Site Code**.

2. Click **Test ConfigMgr Connection**.



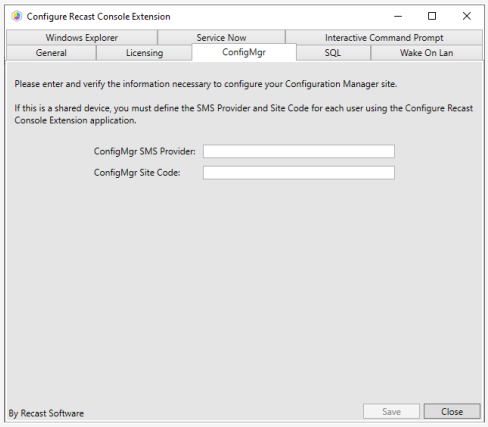
Add ConfigMgr Site Information After Installing Right Click Tools

On the **Configuration Manager Site Information** page, you can choose to **Skip Site Configuration** and add the SMS Provider and Site Code after the installation completes.

NOTE: You'll need to provide those details before you can run any Right Click Tools action that requires ConfigMgr site information.

To add ConfigMgr site information after Right Click Tools installation:

1. Open the Windows Start menu and select the **Configure Recast Console Extension** application.
2. On the ConfigMgr tab, add the **SMS Provider** and **Site Code**. If Right Click Tools is installed on a shared device, you'll need to add ConfigMgr site information for each user of the Configure Recast Console Extension application.



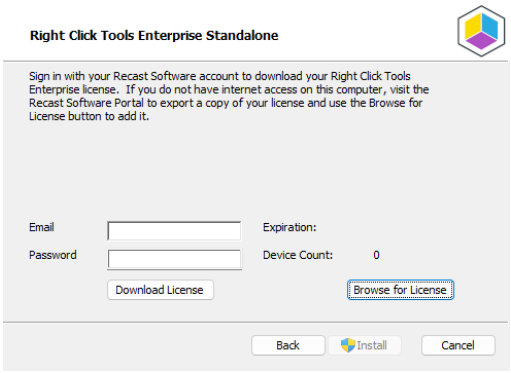
Import License

To download your Recast license:

1. Sign into your Recast Software account by entering your Recast Portal**Email** address and **Password**.

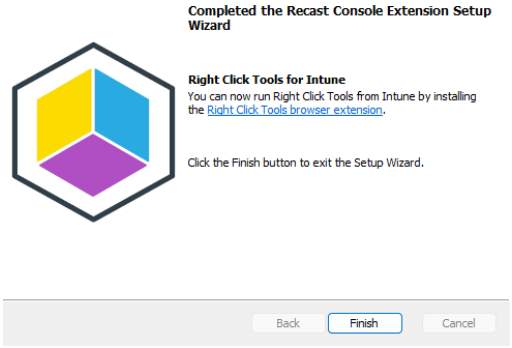
2. Click **Download License**. Your account's **Expiration** and **Device Count** details will appear in the right-hand column.

TIP: If the computer with your Configuration Manager console does not have internet access, click**Browse for License** to search the filesystem for a license file exported from the Recast Portal.



Initiate Installation

Once you have filled in the license information, click **Install**. When the installation completes, you can click the link for Right Click Tools browser extension installation instructions, or click **Finish** to close the installer.



Silent install without Recast Management Server

If you have not installed Recast Management Server, you will need to use the `LICENSEPATH=` parameter to specify the license file to use for your installation. You can download your license file from the Recast Portal or copy it from `C:\ProgramData\Recast Software\Licenses` if you already have Right Click Tools installed on a device.

The license path can be a relative or full path.

Example:

```
msiexec.exe /i "Right Click Tools.msi" /qn LICENSEPATH=".\License\my.license"
```

Task 1A (Optional): Set Up Configuration Manager for Right Click Tools

When Right Click Tools is run in Standalone mode, some actions will not work without Remote Registry or Remote WMI enabled. We recommend that you bypass the need to enable Remote Registry and Remote WMI by deploying and using Recast Agents on your devices to elevate permissions.
If, however, the installation and configuration of your Recast Management Server isn't planned for the short term and you want access to all the Right Click Tools in Standalone mode, you can start the Remote Registry service, create firewall rules for Remote Registry, Remote WMI, and ICMP Echo, and configure the Interactive Command Prompt.

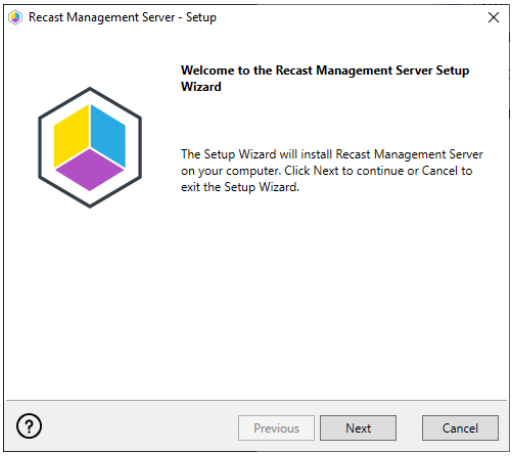
Recast

Task 2: Install RMS 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.

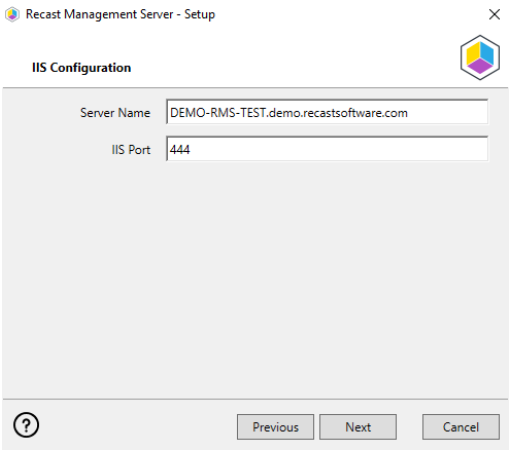


IIS

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.



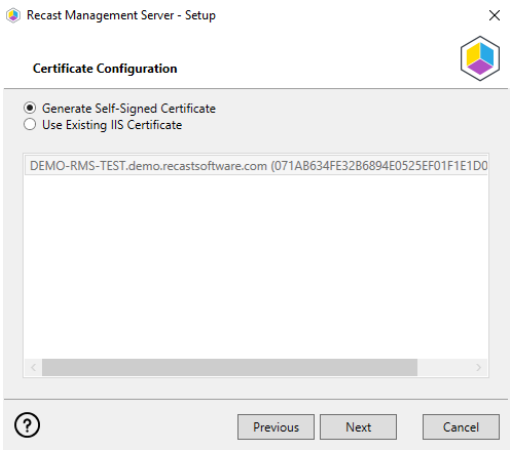
Certificates

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

Recast

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.



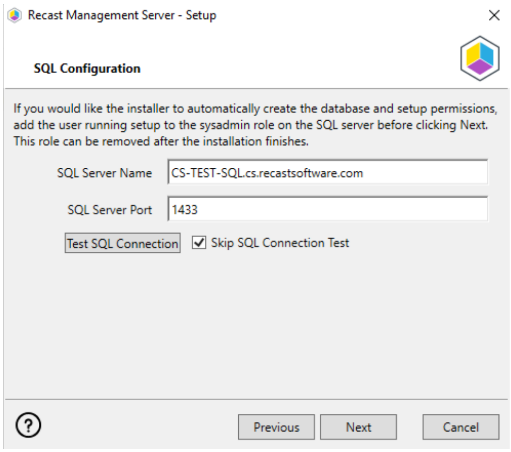
CERTIFICATE NOTES:

- 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.
- Recast strongly recommends a fully licensed version of SQL to avoid the 10GB storage limitation of SQLExpress. SQLExpress use is only supported for POC implementations of Right Click Tools.
- 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_ownerpermissions 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

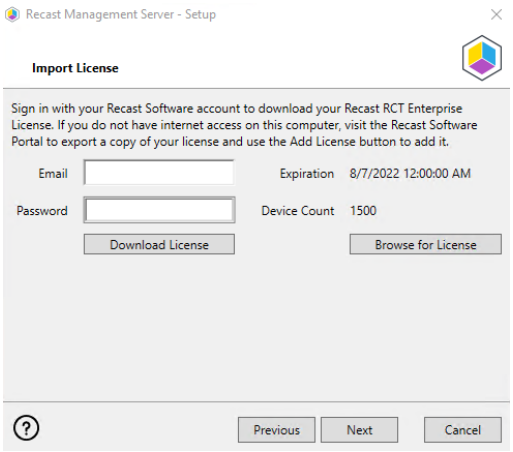
You can download and import your Recast licenses when installing Recast Management Server.

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

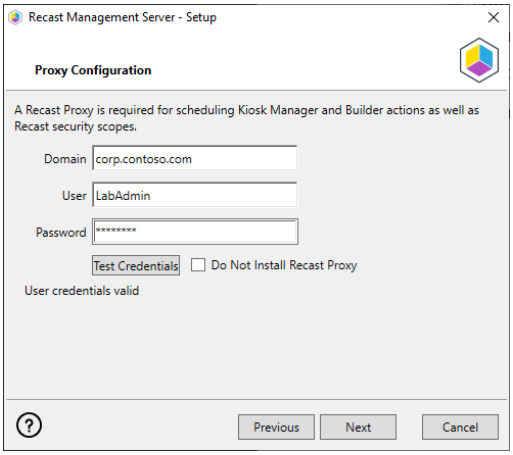
If the Recast Proxy is being installed on a server other than the Recast Management Server, install the Proxy separately after Recast Management Server installation.

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**, **Username**, 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**.

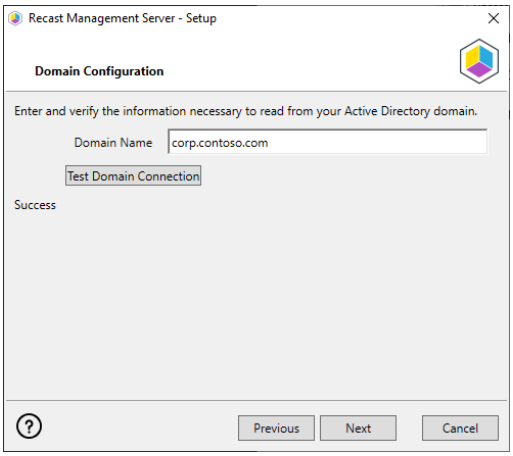


Domain

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

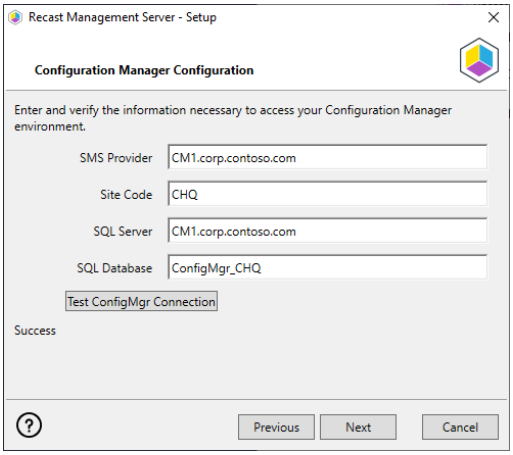
NOTE: Configuration Manager does not need to be set up for Privilege Manager.

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

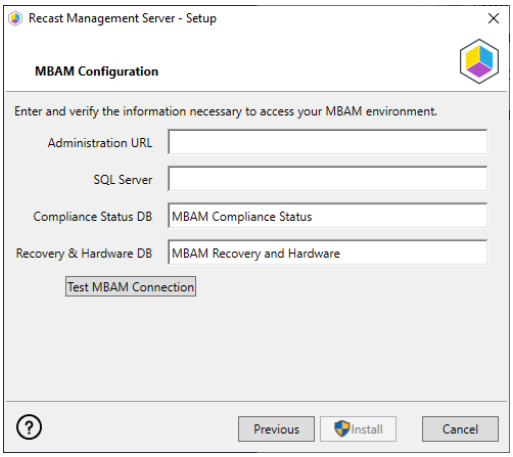
MBAM configuration is only required for a separate MBAM Server. If you are using the ConfigMgr-integrated BitLocker or AD, you can skip this section. MBAM also does not need to be configured for Privilege Manager or Application Manager.

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

Recast

Task 5b: Set Up Intune for Patching

For Right Click Tools Patching to work with Intune, you'll first need to do the following within the Microsoft Azure portal:

- Create the Entra ID App Registration to be used with Patching
- Add client secret
- Grant the application API permissions

Create the Entra ID App Registration for Right Click Tools Patching

To create the app registration:

1. Log into https://portal.azure.com using your Azure credentials with full admin rights.

2. Search for **App registrations**.

3. On the **App registrations** page, click **New registration**.

4. Give the application a meaningful display **Name**. You can change the name later.

5. As the **Supported account type**, select **Accounts in this organizational directory only (Recast Software only – Single tenant)**.

6. Click **Register**.

7. In the **Overview** pane that opens, copy the **Application (client) ID** and **Directory (tenant) ID**. You'll need to enter these later in your Recast Management Server.

Add Client Secret

1. On the **App registrations** page, under **Manage**, click **Certificates & secrets**.

2. On the **Client secrets** tab, add a **New client secret**.

3. Add a client secret **Description** (for example. Patching service), choose when the secret **Expires,** and click **Add**.

   NOTE: You must create a new client secret before the current one expires and change the client secret for your Recast Management Server service connection.

   TIP: Schedule a support ticket, task or calendar entry before the expiry time to perform these actions.

   DO NOT navigate away from the page before completing the next step!

4. Copy the client secret value to a clipboard and save it to a secure location. You will not be able to see the client secret after navigating away from the page. You will need to specify the client secret whenever you modify Entra ID details in Patching, for example, if you want to change the display name of the Entra ID tenant).

Add API Permissions for Right Click Tools Patching

To add API permissions:

1. On the **App registrations** page, under **Manage**, click **API Permissions**.

2. Select **Add a permission**.

3. On the **Microsoft APIs** tab, click **Microsoft Graph**.

4. Add the following permissions:

Application permissions	DeviceManagementApps.ReadWrite.All	Read and write Intune apps
	DeviceManagementConfiguration.Read.All	Read Intune device configuration and policies, permission only required to specify application categories in AM deployment processes
	GroupMember.Read.All	
	Device.Read.All	
Delegated permissions	User.Read	

5. Click **Grant admin consent for [Tenant Name]**.

Once the Entra ID App Registration is done and you have the **Application (client) ID**, **Directory (tenant) ID** and **Client secret** available, you can then add a service connection from your Recast Management Server to Entra ID for Patching.