

## Installation & Upgrades

Last Modified on 12.18.25

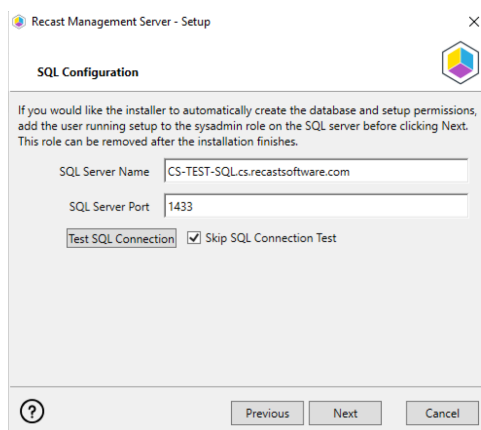
### SQL Server Permissions

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.

**NOTE:** Before removing SysAdmin permissions on the newly created database, check that **db\_owner** permissions are granted on the database for the **computer account** running the Recast Management Server app pool. Add **db\_owner** permissions, if missing. This additional step may only be required for a remote SQL server.

- The computer account of the Recast Management Server can be granted **db\_creator** permissions. In this case, check the **Skip SQL Connection Test** box on the installer's **SQL Configuration** page.



### Pre-create the RecastManagementServer Database

If the account running the Recast Management Server installer does not have permission to create a SQL database, the database administrator can pre-create a database named **RecastManagementServer** and assign permissions manually.

**Remote SQL Server:** Where the database is remote from the Recast Management Server, assign **db\_owner** permissions on the database to the **computer account** of the Recast Management Server.

**Local SQL Server:** Where the database is local to the Recast Management Server, assign **db\_owner** permissions on the database to the **IIS AppPool\Recast Management Server** account.

**NOTE:** The IIS AppPool\Recast Management Server account will not exist until after the installation is finished, so **db\_owner** permissions will need to be assigned after installation.

### Add the Computer Account via SSMS

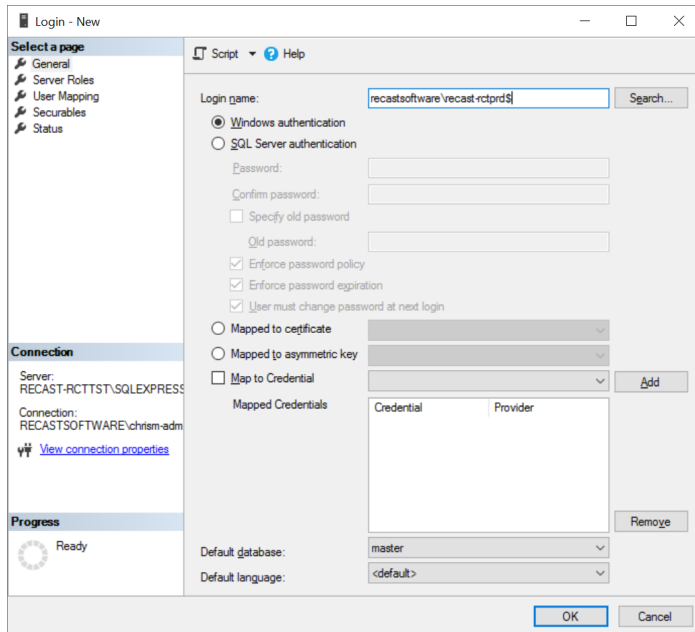
If the computer account for the Recast Management Server computer does not exist in SQL, users will need to add the computer account manually, as a Login Account in SQL Server Management Studio (SSMS).

#### Add the Computer Account as a Login Account

To create the computer account as a login account:

# Recast

1. Open SSMS and expand the folder of the server instance in which you want to create the new login.
2. Right-click on the Security folder, point to New and select Login.
3. In the **Login – New** window, on the **General** page, enter the Login name of the account in the following format: **<domain name>\<computer name>\$**. Including the dollar sign (\$) treats the login name as a computer account rather than a user account.



4. On the **User Mapping** page, in the **Users mapped to this login** section, select **RecastManagementServer**.
5. In the **Database role membership** section, select **db\_owner**.

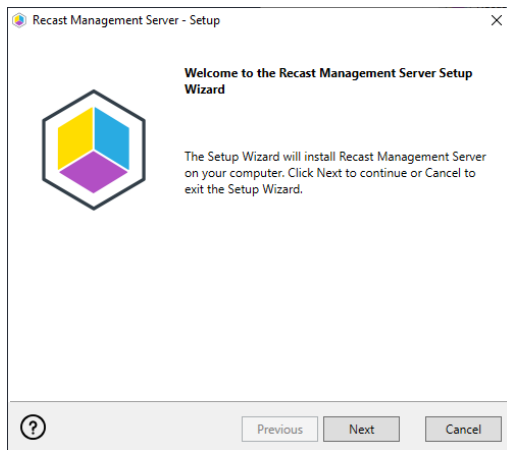
## Install RMS With Proxy

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.

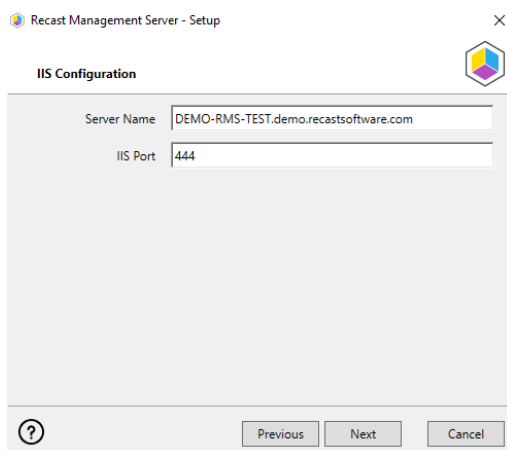
# Recast



## 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.



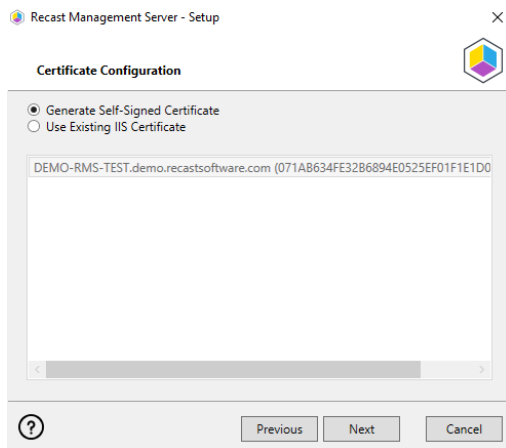
## Certificates

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.

# Recast



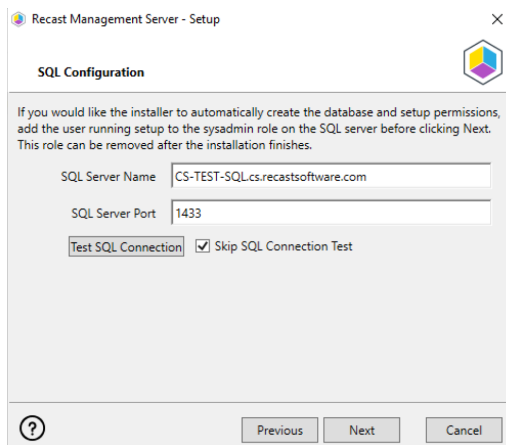
## CERTIFICATE NOTES:

- 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\_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

# Recast

AppPool\Recast Management Server account will not exist until after the installation completes, so the permissions will need to be given after installation.

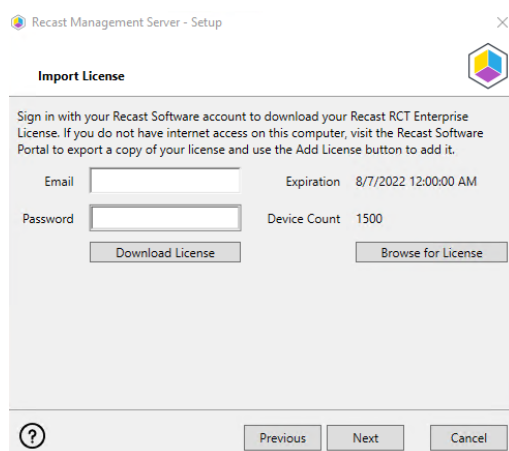
## Import License

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](#).



The image shows a screenshot of the 'Recast Management Server - Setup' window. The title bar includes the Recast logo and a close button. The window has a standard Windows-style title bar with 'Recast Management Server - Setup' and a close button. The main content area is titled 'Import License' and contains the following text: 'Sign in with your Recast Software account to download your Recast RCT Enterprise License. If you do not have internet access on this computer, visit the Recast Software Portal to export a copy of your license and use the Add License button to add it.' Below this text are two input fields: 'Email' and 'Password'. To the right of the 'Email' field is the 'Expiration' date, which is '8/7/2022 12:00:00 AM'. Below the 'Password' field is the 'Device Count', which is '1500'. At the bottom of the input fields are two buttons: 'Download License' and 'Browse for License'. At the very bottom of the window are three buttons: a help button (question mark icon), 'Previous', 'Next', and 'Cancel'.

## 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.

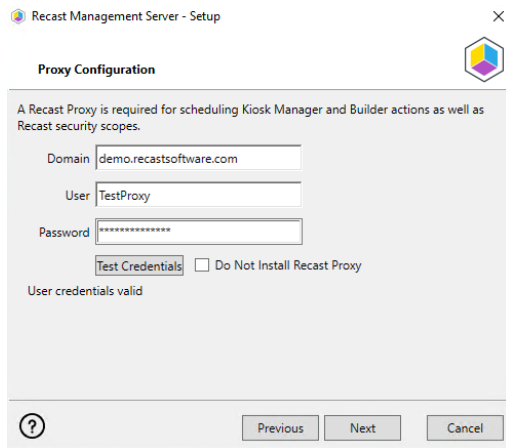
**NOTE:** Proxy configuration is optional for Privileged Access where Active Directory or Entra ID objects are not used to target rules.

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**.

# Recast



Recast Management Server - Setup

**Proxy Configuration**

A Recast Proxy is required for scheduling Kiosk Manager and Builder actions as well as Recast security scopes.

Domain: demo.recastsoftware.com

User: TestProxy

Password: \*\*\*\*\*

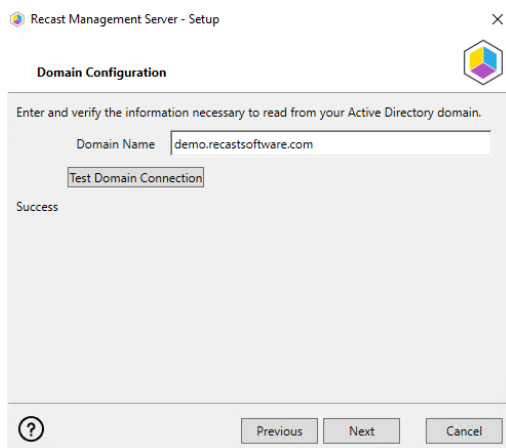
☐ Do Not Install Recast Proxy

User credentials valid

## 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. The test should show **Success**.



Recast Management Server - Setup

**Domain Configuration**

Enter and verify the information necessary to read from your Active Directory domain.

Domain Name: demo.recastsoftware.com

Success

## Configuration Manager

**NOTE:** Configuration Manager does not need to be set up for Privileged Access.

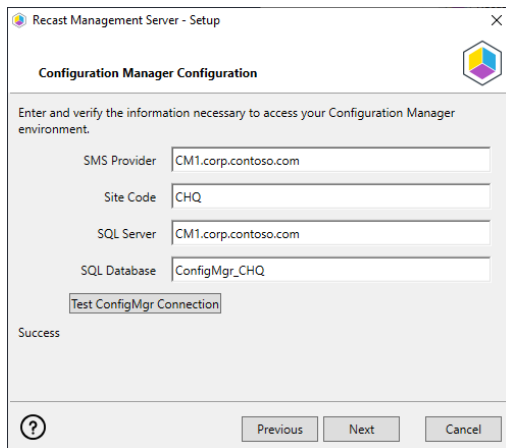
To set up your Configuration Manager for the proxy:

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.

# Recast



Recast Management Server - Setup

**Configuration Manager Configuration**

Enter and verify the information necessary to access your Configuration Manager environment.

SMS Provider: CM1.corp.contoso.com

Site Code: CHQ

SQL Server: CM1.corp.contoso.com

SQL Database: ConfigMgr\_CHQ

[Test ConfigMgr Connection](#)

Success

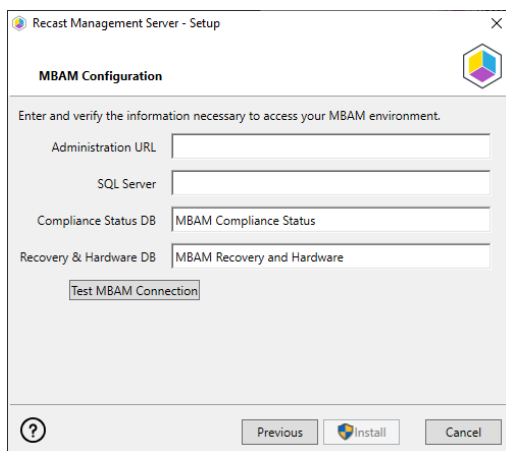
Previous Next Cancel

## 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 Privileged Access or Patching.

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.



Recast Management Server - Setup

**MBAM Configuration**

Enter and verify the information necessary to access your MBAM environment.

Administration URL:

SQL Server:

Compliance Status DB: MBAM Compliance Status

Recovery & Hardware DB: MBAM Recovery and Hardware

[Test MBAM Connection](#)

Previous [Install](#) Cancel

## 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://<Server FQDN>:<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`

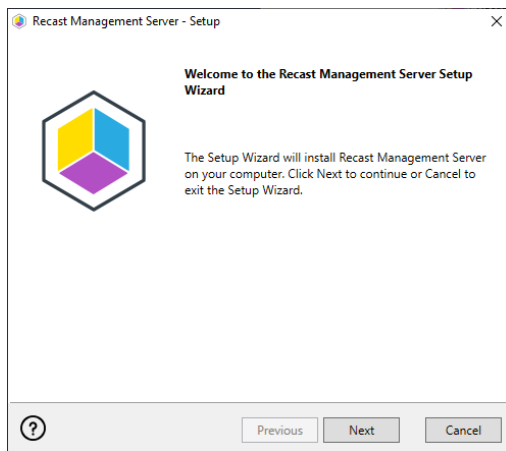
## Install RMS Without Proxy

Before installing Recast Management Server, ensure that your system meets the application's [hardware and software requirements](#).

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

## Run the Recast Management Server Installer

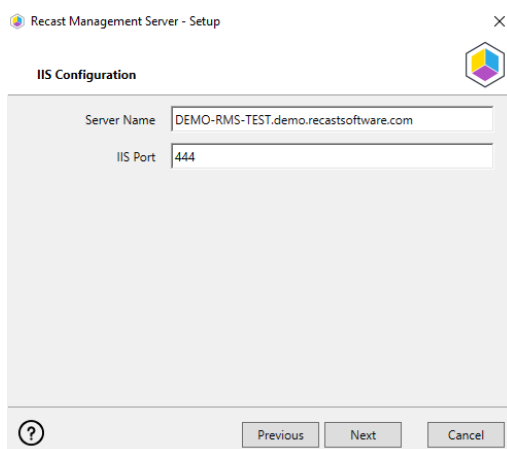
After downloading Recast Management Server from the [Recast Portal](#), run the installer and follow its prompts.



## 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

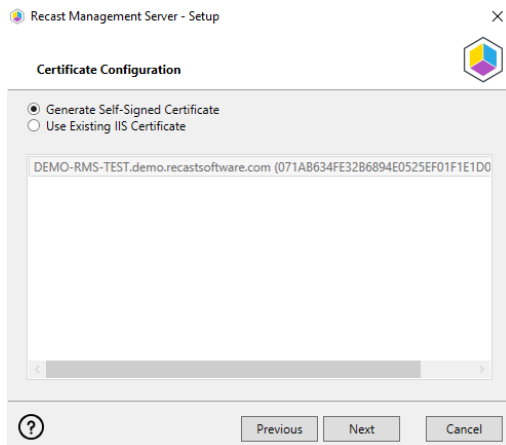


# Recast

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.



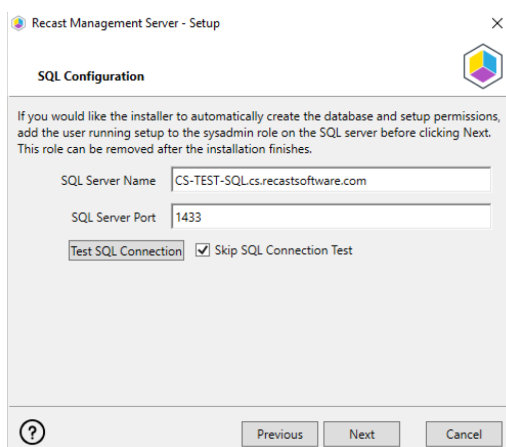
## CERTIFICATE NOTES:

- 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.
- Recast strongly recommends a fully licensed version of SQL to avoid the 10GB storage limitation of SQLExpress.

# Recast

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\_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.

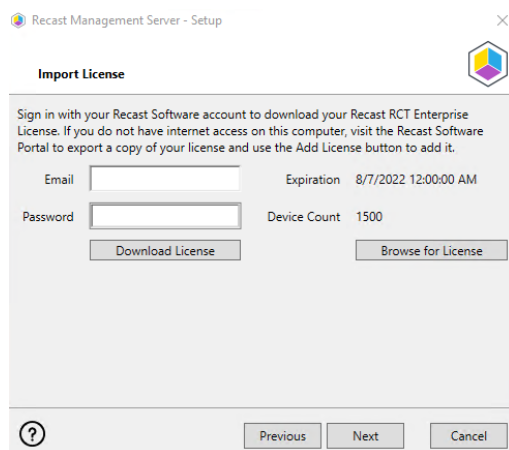
## Import License

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](#).



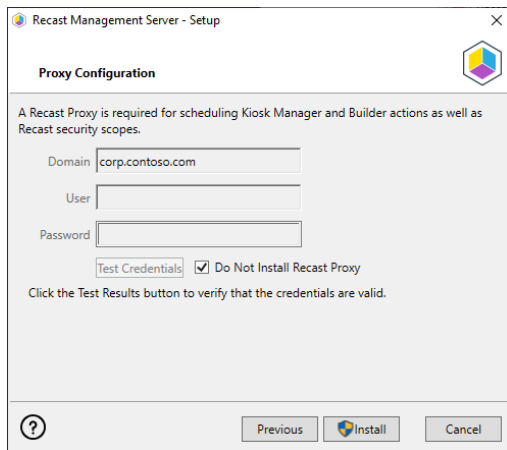
The screenshot shows the 'Recast Management Server - Setup' window with the 'Import License' tab selected. The window title bar includes a close button (X) and a Recast logo. The 'Import License' section contains the following text: 'Sign in with your Recast Software account to download your Recast RCT Enterprise License. If you do not have internet access on this computer, visit the Recast Software Portal to export a copy of your license and use the Add License button to add it.' Below this text are two input fields: 'Email' and 'Password'. To the right of the 'Email' field, the 'Expiration' date is displayed as '8/7/2022 12:00:00 AM'. To the right of the 'Password' field, the 'Device Count' is displayed as '1500'. At the bottom of the input section are two buttons: 'Download License' and 'Browse for License'. At the very bottom of the window are three buttons: a help button (question mark icon), 'Previous', 'Next', and 'Cancel'.

## Configure Without Recast Proxy

A Recast Proxy allows you to schedule Kiosk Manager and Builder actions as well as Recast security scopes. For instructions on installing Recast Proxy, see [Installing Recast Management Server with Recast Proxy](#)

If you do not wish to install a Recast Proxy during Recast Management Server installation, enable **Do Not Install Recast Proxy** and click **Install**.

# Recast



When the installation completes, click **Finish** to exit the setup wizard.

## Verify Recast Management Server Installation

To confirm that you can open the Recast Management Server, navigate to `https://<Server FQDN>:<Port>` in a web browser. Chrome, Edge, or Firefox are recommended. On the Recast Management Server login page, enter the username and password for the account that you were using to install the Recast Management Server.

## Install Recast Proxy

You can install a Recast Proxy separately if it was not installed during the Recast Management Server installation, or if it needs to be installed on a server other than the Recast Management Server. After installing a Recast Proxy separately, you'll need to [approve it manually](#) and [add service connections](#).

For an overview of proxy types, uses, permissions, installation and configuration, see [Recast Proxy](#).

The Recast Proxy SQLite file is located at `C:\Users\<Proxy Username>\AppData\Roaming\Recast Software\Recast Proxy`

### Prerequisites

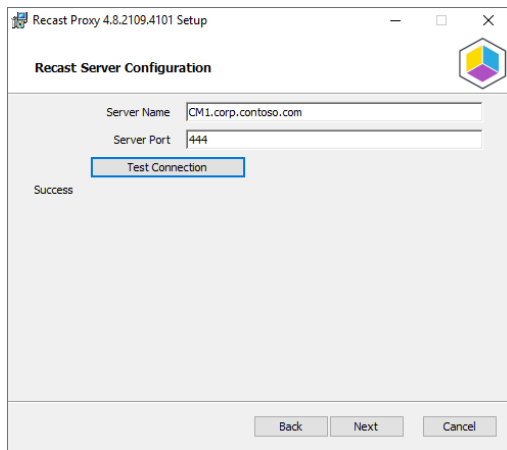
- [Recast Management Server installed](#)

### Run the Proxy Installer

To install Recast Proxy:

1. Download the Recast Proxy installer from the [Recast Portal](#) and run it.
2. On the **Recast Server Configuration** page, enter the Recast Management **Server Name** and **Server Port** number.
3. Click **Test Connection** to make sure that the proxy can connect to the Recast Management Server.

# Recast

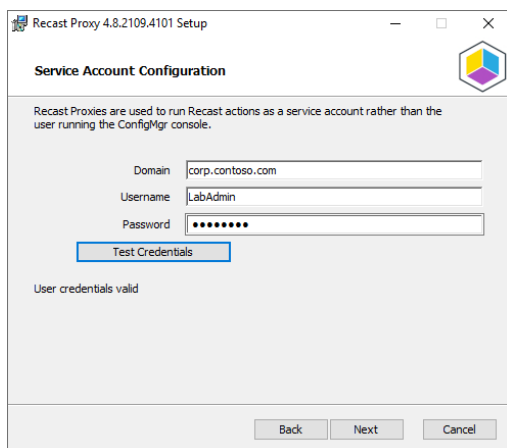


The screenshot shows the 'Recast Server Configuration' window of the Recast Proxy 4.8.2109.4101 Setup. It features a title bar with standard Windows window controls and a Recast logo. The main area contains two text input fields: 'Server Name' with the value 'CM1.corp.contoso.com' and 'Server Port' with the value '444'. Below these fields is a 'Test Connection' button. A 'Success' message is displayed in the lower-left area. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.



If the installer does not connect to the Recast Management Server, the proxy will not install successfully. Troubleshoot any error messages that appear in the installer before continuing with the install.

4. On the **Service Account Configuration** page, enter the **Domain**, **Username** and **Password** that you would like to use for your proxy and click **Test Credentials** to verify service account details.



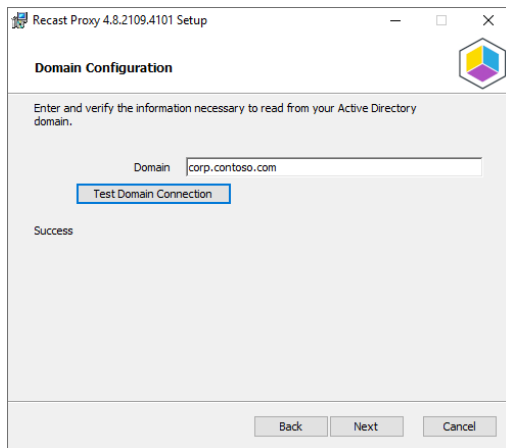
The screenshot shows the 'Service Account Configuration' window of the Recast Proxy 4.8.2109.4101 Setup. It features a title bar with standard Windows window controls and a Recast logo. Below the title bar is a note: 'Recast Proxies are used to run Recast actions as a service account rather than the user running the ConfigMgr console.' The main area contains three text input fields: 'Domain' with the value 'corp.contoso.com', 'Username' with the value 'LabAdmin', and 'Password' with masked characters '\*\*\*\*\*'. Below these fields is a 'Test Credentials' button. A 'User credentials valid' message is displayed in the lower-left area. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.



If the User Account Credentials that you enter on the Service Account Proxy Screen do not validate correctly, the Service Account Proxy will not work correctly. Troubleshoot any login errors before continuing to the next step.

5. On the **Domain Configuration** page enter your primary **Domain** and click **Test Domain Connection** to check that the service account can read from the domain.

# Recast



Recast Proxy 4.8.2109.4101 Setup

### Domain Configuration

Enter and verify the information necessary to read from your Active Directory domain.

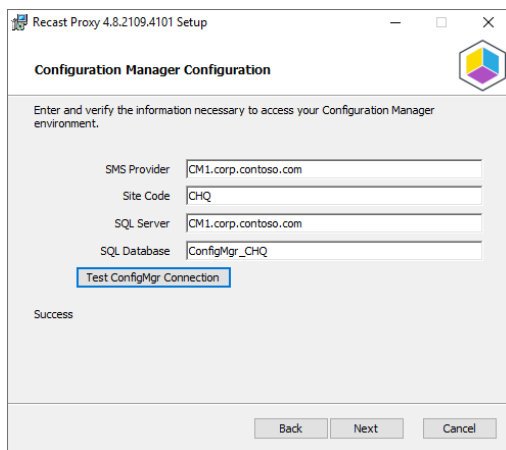
Domain: corp.contoso.com

Test Domain Connection

Success

Back Next Cancel

6. On the **Configuration Manager Configuration** page, enter your **SMS Provider**, **Site Code**, **SQL Server**, and **SQL Database** information and click **Test ConfigMgr Connection** to check that your service account has permission to access your Configuration Manager environment.



Recast Proxy 4.8.2109.4101 Setup

### Configuration Manager Configuration

Enter and verify the information necessary to access your Configuration Manager environment.

SMS Provider: CM1.corp.contoso.com

Site Code: CHQ

SQL Server: CM1.corp.contoso.com

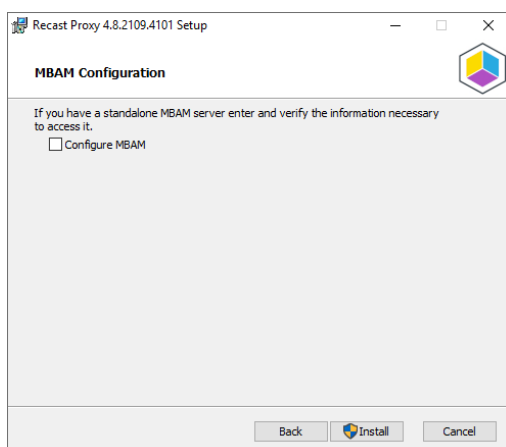
SQL Database: ConfigMgr\_CHQ

Test ConfigMgr Connection

Success

Back Next Cancel

7. If you have a standalone MBAM server (and are not managing BitLocker in ConfigMgr), enable **Configure MBAM** and enter the information for your MBAM environment. If you are not using an MBAM Server, leave the checkbox blank and click **Install**.



Recast Proxy 4.8.2109.4101 Setup

### MBAM Configuration

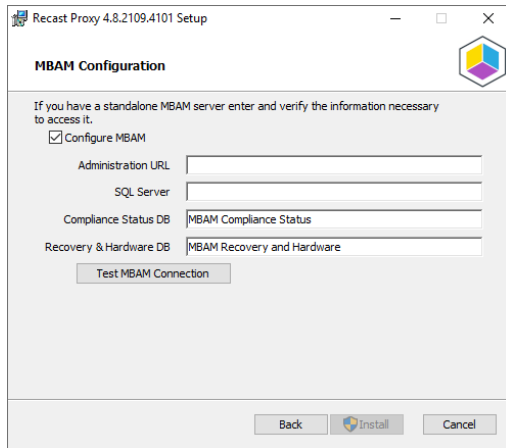
If you have a standalone MBAM server enter and verify the information necessary to access it.

☐ Configure MBAM

Back Install Cancel

8. If you have a standalone MBAM environment, enter its details and click **Test MBAM Connection** to ensure that the service account you selected has permission to use MBAM.

# Recast



9. Click **Install**.

10. After the installation completes, click **Finish** to close the installer.

## Silent Install for Standalone Recast Proxy

Add the parameter `RCTENTERPRISESERVER=https://<FQDN>:<Port>` to your install string so your standalone Recast Proxy can connect to your Recast Management Server. Substitute the FQDN for your RMS server followed by the port number.

Example:

```
msiexec /i "Recast Proxy.msi" /! *v %temp%\RecastProxy.log PROXYLOGONUSER="<Domain>\<Username>" RCTENTERPRISESERVER="https://<FQDN>:<Port>" SERVICEACCOUNTPASSWORD="<Password>" SERVICEACCOUNTDOMAIN="<Domain>" SERVICEACCOUNTUSERNAME="<Username>" /qn
```

## RMS with Web Proxy

The Recast Management Server requires [access to specific external domains](#) depending on which Recast Software products are in use. If you are using a web proxy on the Recast Management Server, or on the server running Recast Proxy, you will need to direct network traffic to those external domains through the web proxy, as the web proxy will not automatically detect settings on the server where the RMS or Recast Proxy is installed.

You can direct network traffic through the web proxy by changing the environment variables in your Recast Management Server `web.config` file.

To change environment variables for a web proxy:

1. Open the `web.config` file located at `C:\Program Files (x86)\Recast Software\Recast Management Server\web.config`.

**TIP:** We recommend making a copy of the existing `web.config` file before editing.

2. In the `aspNetCore` module, edit the **Environment Variables** information and add opening and closing tags.

```
<environmentVariables>
  <environmentVariable name="all_proxy" value="http://proxyserver:port" />
  <environmentVariable name="no_proxy" value="RmsServer.example.com,SccmServer.example.com" />
</environmentVariables>
```

For details about the environment variables used for default proxy initialization, see [HttpClient.DefaultProxy Property](#).

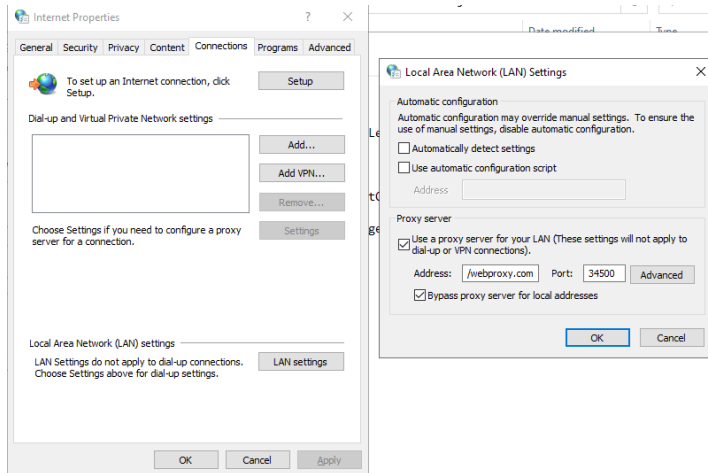
# Recast

3. Recycle the Recast Management Server application pool and restart the site in IIS.

After editing the environment variables in the web.config file, follow these steps to verify the web proxy settings are correct for the account running the Recast Proxy service.

4. Log into the server as the Recast Proxy service account, open **Internet Options** and verify the proxy information is correct there.

5. If you are defining the web proxy manually, navigate to **Internet Properties > Connections > LAN settings** and check that **Automatically detect settings** and **Use automatic configuration script** are deselected. If both those options and **Use a proxy server for your LAN** are configured, they will conflict.



**NOTE:** If the RCT Patching catalog fails to load and returns an error: 'The proxy tunnel request failed with status code 407', add a rule to allow NoAuth access from the Recast Management Server to the [external domains required for RCT Patching](#).

## Deploy Agents

## Proof Of Concept

## Set Database Recovery Model

By default, the RecastManagementServer database is set to full recovery. We recommend switching your SQL Server recovery model from full recovery to simple recovery to prevent the database from running out of disk space due to an overload of transaction logging.

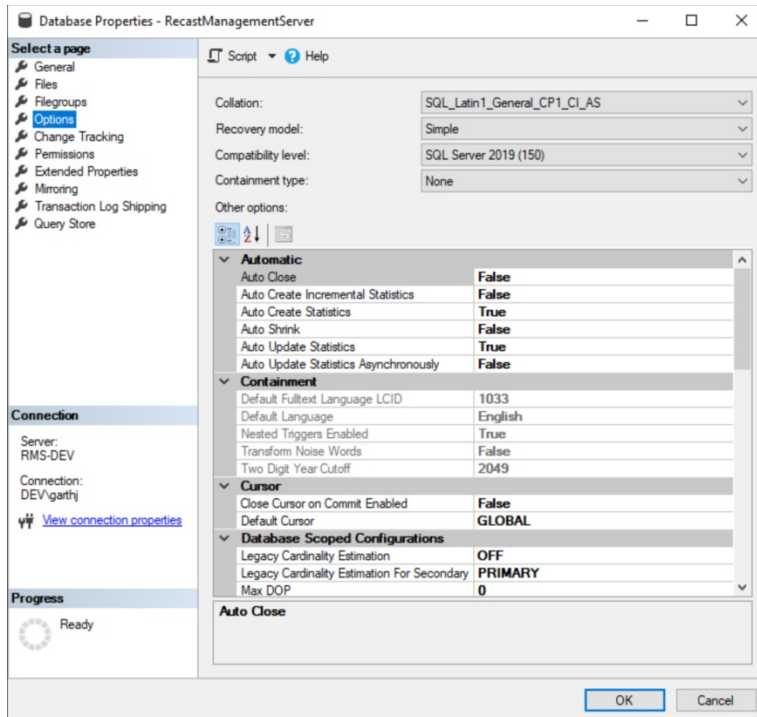
To learn more about the difference between simple, full, and bulk-logged recovery, see [Recovery Models \(SQL Server\) | Microsoft Learn](#).

To switch the SQL Server recovery model to simple recovery:

1. Open SQL Server Management Studio (SSMS).
2. Expand the **Databases** folder.

# Recast

3. Right-click on the RecastManagementServer database and select **Properties** from the drop-down menu.
4. In Database Properties, click the **Options** page.
5. Change the **Recovery model** to **Simple** and click OK to save your changes.



## Server Migration

Instructions for migrating your Recast Management Server database to a new server.

To migrate the RecastManagementServer database:

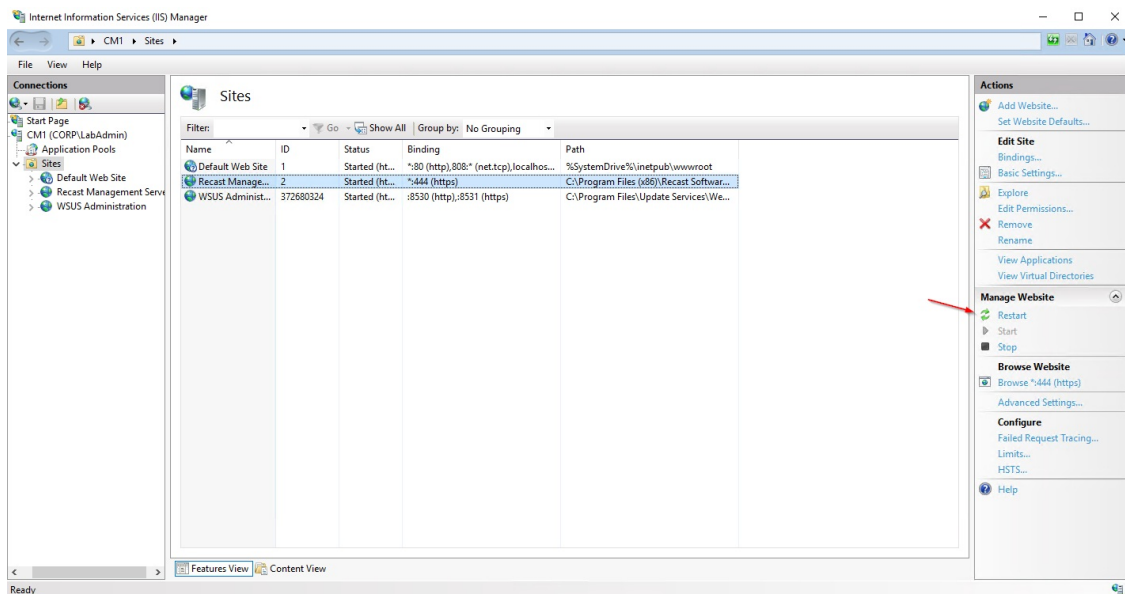
1. Back up your RecastManagementServer database.
2. Copy the database over to the new location.
3. Navigate to `C:\Program Files (x86)\Recast Software\Recast Management Server` on your management server and open the `appsettings.Production.json` file.
4. Update your server information in the .json file to specify the new server name.

```
{
  "ConnectionStrings": {
    "DefaultConnection": "Server=localhost;Database=RecastManagementServer;Trusted_Connection=True;MultipleActiveResultSets=true"
  }
}
```

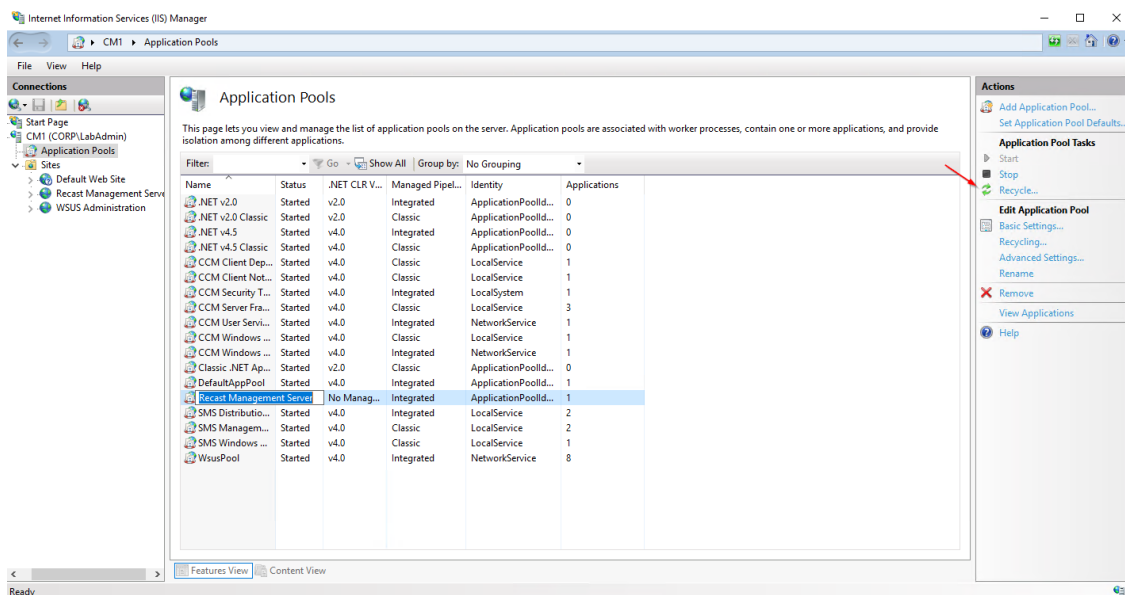
5. Open IIS Manager, under **Manage Website**, click to **Restart** your Recast Management Server website.



# Recast

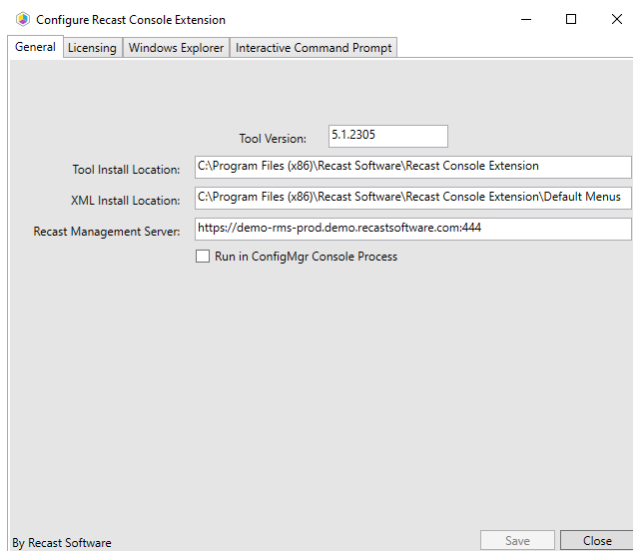


6. Under **Application Pool Tasks**, click **Recycle**.



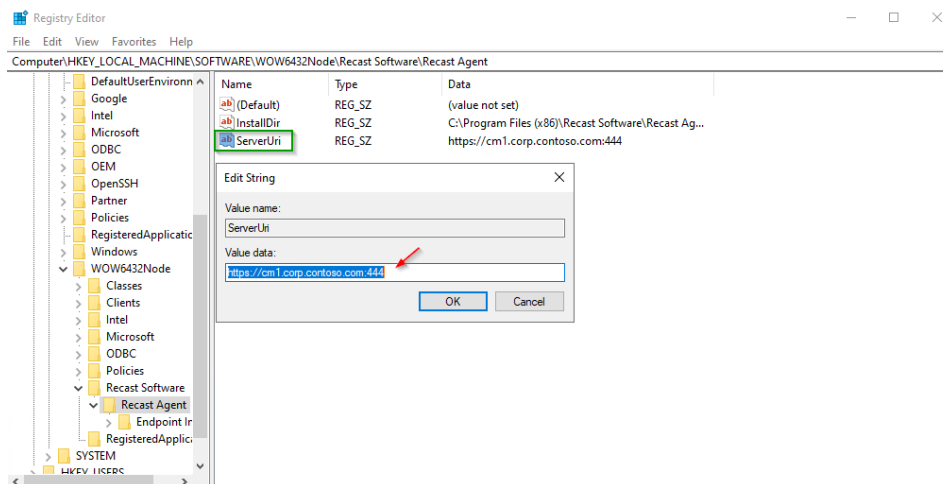
7. If the name changes for the server, update any Right Click Tools installations to point to the new server by adding the **Recast Management Server** URL on the **General** tab in the Configure Recast Console Extension application.

# Recast



8. If you have agents in your environment, update the **ServerUri** registry keys to point to the new server's name.

## Agent Server Uri Registry Entry:

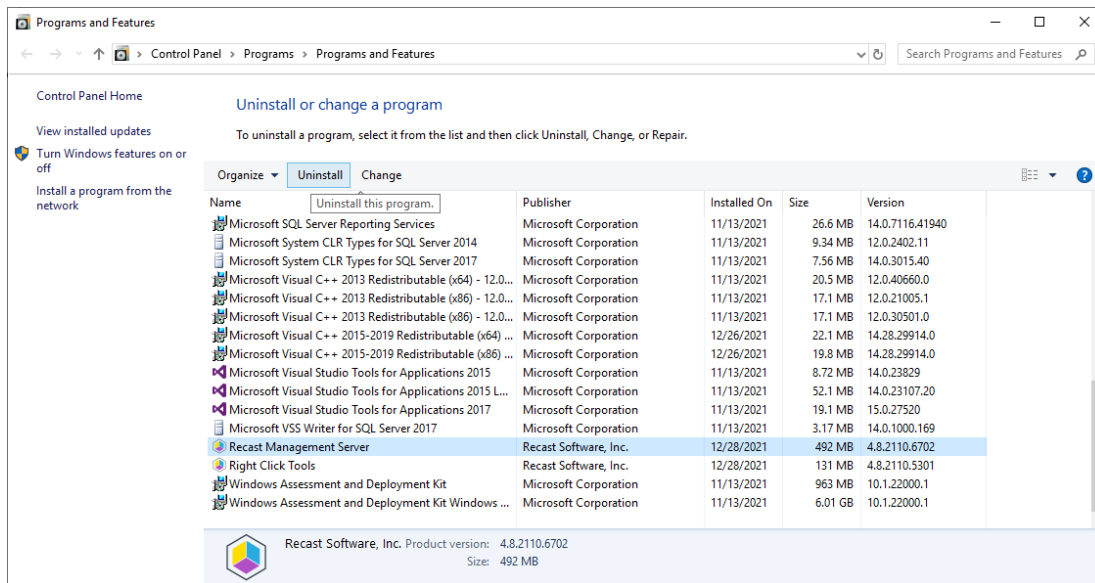


## Uninstall RMS

To uninstall Recast Management Server:

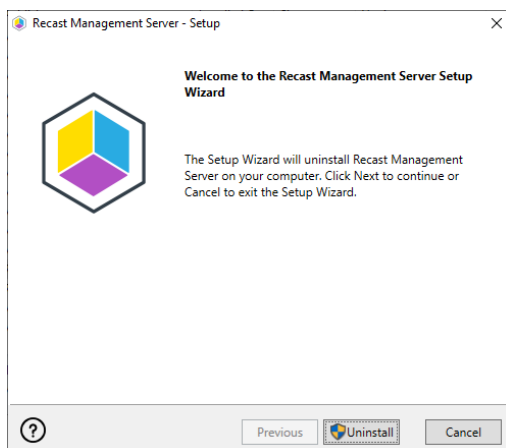
1. Under **Programs and Features**, click to highlight **Recast Management Server** in the program list.
2. Click **Uninstall**.

# Recast



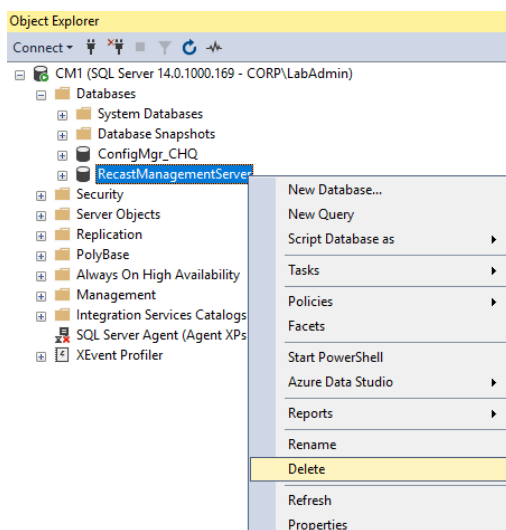
3. Click **Yes** to allow the app to make changes to your device.

4. In the Recast Management Server Setup Wizard click **Uninstall**.



5. Once the uninstall process is complete, click **Finish** to exit the Setup Wizard.

6. Remove all Recast Management Server components from your environment by deleting your SQL RecastManagementServer database.



If you experience issues uninstalling Recast Management Server, you can use Microsoft's uninstaller tool to fully uninstall any lingering files. To download the tool, see [Fix problems that block programs from being installed or removed](#).

## Antivirus Exclusions

Real-time antivirus protection can cause issues on Configuration Manager site servers, site systems, and clients.

The recommendations in this article are meant to help you diagnose causes of potential instability on a device when running antivirus software alongside a supported version of Recast Management Server (RMS), Recast Agent Gateway, Recast Proxy, and/or Recast Agent.

We suggest temporarily applying these exclusions to evaluate a system. If system performance or stability improves as a result, contact your vendor for instructions or an updated antivirus software version.

### Folder Exclusions for RMS and Agent Gateway

%SystemRoot%\IIS Temporary Compressed Files

%SystemRoot%\inetpub\temp\IIS Temporary Compressed Files

### File Exclusions for RMS and Agent Gateway

%windir%\System32\inetsrv\w3wp.exe (x86 systems)

%windir%\SysWOW64\inetsrv\w3wp.exe (x64 systems)

## Process Exclusions

Process exclusions are only needed when aggressive antivirus programs consider Recast executables (.exe) to be high-risk processes.

### Process Exclusions for RMS and Agent Gateway

C:\Program Files (x86)\Recast Software\Recast Agent Gateway\Recast.AgentGateway.exe

%windir%\System32\inetsrv\w3wp.exe (x86 systems)

%windir%\SysWOW64\inetsrv\w3wp.exe (x64 systems)

### Process Exclusions for Agent Gateway (Kestrel)

C:\Program Files (x86)\Recast Software\Recast Agent Gateway\Recast.AgentGateway.exe

## SQL Exclusions

On your SQL server, we recommend following Microsoft's guidance: [Configure antivirus software to work with SQL Server – SQL Server | Microsoft Learn](#)

## Intrusion Detection and AV Software with Insights

Intrusion detection and AV software, such as CrowdStrike and Carbon Black, will sometimes prevent Insights from

# Recast

completing its setup. This is due to the EI setup uploading 250+ reports to your Configuration Manager Reporting Point within a short period. To work around the issue, exclude the EI setup or temporarily exclude EI setup during any installation, on both the ConfigMgr site server where the setup is run and on the SQL Server Reporting Service (SSRS) server.

---