

# Deploy Recast Agents for Privileged Access

Last Modified on 08.06.25

A Recast Agent is installed on a computer and runs actions on that computer as the local system account. A Recast Agent should be deployed on each device you want to run actions against. After deploying Recast Agents, you can configure them to run [Right Click Tools actions](#) or for [Fast Channel Support](#). You can also use the same Recast Agent for Endpoint Insights and Privilege Manager.

To learn more, see [Recast Agents](#) and [Recast Agent Gateways](#).

## Prerequisites for Deploying Recast Agents:

- 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.

## Deploy Agents with Application Manager

We recommend deploying Recast Agents using Application Manager. Your Right Click Tools Enterprise license alone gives you access to Application Manager to deploy Recast Agents. In the absence of Application Manager licensing, only the Recast Agent and Right Click Tools applications will be available in the AM software catalog.

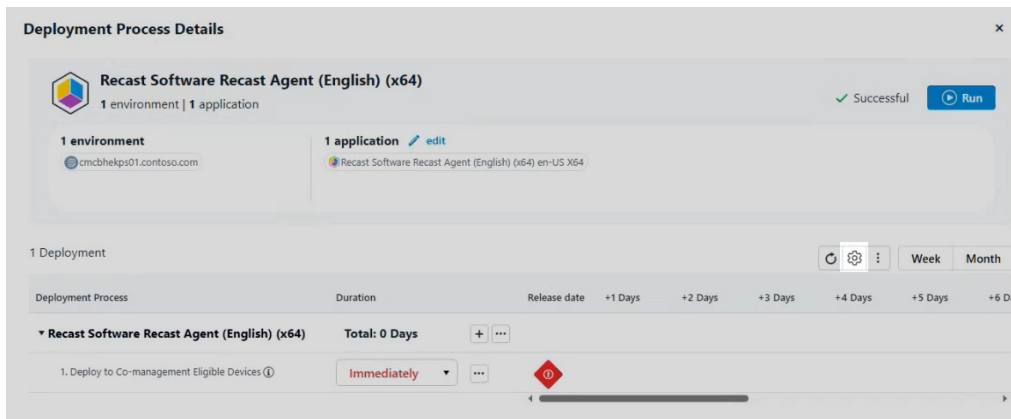
**TIP:** Alternatively, you can choose to deploy Recast Agents by downloading and running the Agent installer.

### Prerequisites for Deploying Agents using Application Manager:

- Recast Management Server is running Recast Software version 5.4 or later, as that version introduces Application Manager in RMS.
- Required [proxy permissions](#) for Application Manager are in place

To deploy the Recast Agent application with Application Manager:

1. If you haven't already done so, [complete your initial AM setup](#), skipping the Setup Wizard's Define Deployment Processes step.
2. [Add a deployment process](#) for the 'Recast Agent' application.
3. On the **Deployment Process Details** page, click the Settings cog to open your Global Deployment Process settings.



4. On the **Advanced** tab, set [Additional Installation Parameters](#):

- **Silent Agent Install:** Add the **RCTENTERPRISESERVER=https://<RMS URL>:<Port>** parameter to your install string, substituting the URL and port number for your Recast Management Server.
- **Connect Recast Agents to a specific Agent Gateway:** Add the **AGENTGATEWAY=https://<AG URL>:<Port>** parameter to your install string, substituting the URL and port number for your Agent Gateway

**NOTE:** Adding these parameters in Application Manager's deployment settings enables deployed Recast Agents to connect to your Recast Management Server, verify that [the certificate used by the RMS](#) is trusted, and successfully enroll with the RMS. Recast Agents are required to enroll with the RMS before they can communicate with a Recast Agent Gateway and be used to run actions.

## Agent Deployment Video Walkthrough

See [Recast Application Deployment with Application Manager](#) on our YouTube channel.

## Deploy Agents with Configuration Manager

### Option 1: Create an Application Manager deployment process but deploy Agents with ConfigMgr

By creating an Application Manager deployment process for the Recast Agent application without any deployment steps, you can automatically access new Recast Agent versions, with the correct install commands, and then use the Recast Agent application in a task sequence and/or to create deployments manually in Configuration Manager.

To create a deployment process without deployment steps:

1. When creating the deployment process, choose a collection.
2. Remove the deployment step.
3. Save the deployment process.

### Option 2: Use ConfigMgr to manually package and deploy Agents

#### Silent Agent Install

Add the **RCTENTERPRISESERVER=https://<FQDN>:<Port>** parameter to your install string, substituting the FQDN and port number for your Recast Management Server.

Example:

```
msiexec.exe /qn /i "Recast Agent.msi" RCTENTERPRISESERVER="https://<RMS URL>:<Port>" /L*V "%temp%\RecastAgentMSI.log"
```

**NOTE:** The default Recast Management Server port is 444. Inbound and outbound traffic over port 444 (or an alternative port you specify) must be enabled between the Recast Management Server and any device that has a Recast Agent in order for the Agent to be able to communicate with the server.

You can connect your Recast Agents to a specific Agent Gateway by adding the **AGENTGATEWAY** parameter to your install string.

Example:

```
msiexec.exe /qn /i "Recast Agent.msi" RCTENTERPRISESERVER="https://<RMS URL>:<Port>"  
AGENTGATEWAY="https://<Agent Gateway URL>:<Port>" /L*V "%temp%\RecastAgentMSI.log"
```