

Agent Gateway

Last Modified on 05.30.24

A Recast Agent Gateway is an on-premises component that connects your Recast Management Server to your Recast Agents. An Agent Gateway lets you to manage your endpoints at scale by providing a secure communications path for:

- Agent authentication and authorization
- Agent licensing
- Directing Recast actions to Agents
- Extending Agent connectivity to the Internet
- Connecting Agents with other Recast components

Multiple Agent Gateways can be added, meaning that there's no limit to the number of Agents that can connect to your Recast Management Server. Internet-connected devices that are not on your local network can connect to the Agent Gateway, allowing you to run Recast actions against them, without the need for a Cloud Management Gateway (CMG).



View Agent Gateways

You can view and edit Agent Gateways in the Recast Management Server interface by navigating to **Administration > Agent Gateways**.

By default, the one Agent Gateway added automatically during Recast Management Server installation will appear on the **Agent Gateways** page.

Details shown include the **Computer Name**, whether an Agent Gateway is **Connected** or **Authorized**, and the Agent Gateway software **Version**.

Recast Agent Gateways

Computer Name	Connected	Version	Authorized	Actions
CM1	✓	5.0.2302.1703	✓	 

1 - 1 of 1 items

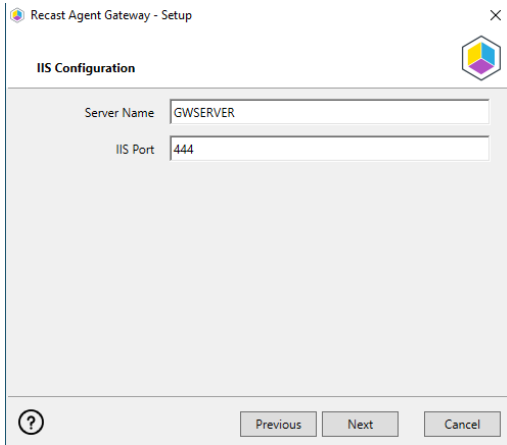
Install an Agent Gateway

A single Agent Gateway is automatically deployed and authorized when you install Recast Management Server. You can

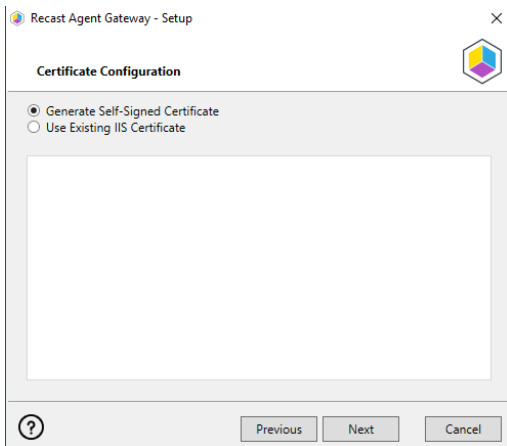
also install additional Agent Gateways, to accommodate all of your Recast Agents. Each Agent Gateway must be installed on a different server. Agent Gateway software is available from the [Recast Portal](#).

To configure an Agent Gateway:

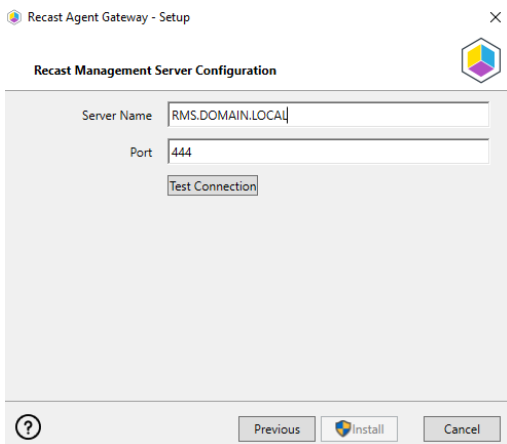
1. On the Agent Gateway installer's IIS Configuration page, specify the **Server Name** in FQDN format (server.domain.local) and **IIS Port** for the Agent Gateway.



2. On the Certificate Configuration page, select an existing certificate, or generate a self-signed certificate.



3. Click **Test Connection** to check that the Agent Gateway can connect to your Recast Management Server.



4. With a successful connection test, click **Install**.

5. When the installation completes, click **Finish** to close the installer.

Verify Agent Gateway Installation

In the Recast Management Server interface, navigate to **Administration > Agent Gateways** and check that the new Agent Gateway is connected and authorized. If you've installed an Agent Gateway on a separate server, you may need to [manually authorize it in RMS](#).

For information on the hardware needed for Agent Gateway servers, see [Recast Management Server System Requirements](#).

To learn more about installing your Recast Management Server with an additional Gateway, see [Network Architecture: RMS with Standalone Agent Gateway](#).

The Agent Gateway SQLite file is located at `C:\Users\Recast Agent Gateway\AppData\Roaming\Recast Software\Recast Agent Gateway`

Connect an Agent Gateway to the Internet

You can extend Recast Agent connectivity to devices that are not on your local network by publishing Recast Agent Gateway to the Internet. One method of publishing Agent Gateway to the Internet is to use the Microsoft Entra Application Proxy service. You can find App Proxy requirements and more information in this [Microsoft Entra ID Tutorial](#).

For more detail about this configuration of Recast Software components, see [Network Architecture: RMS with Standalone Agent Gateway](#).

Prerequisites

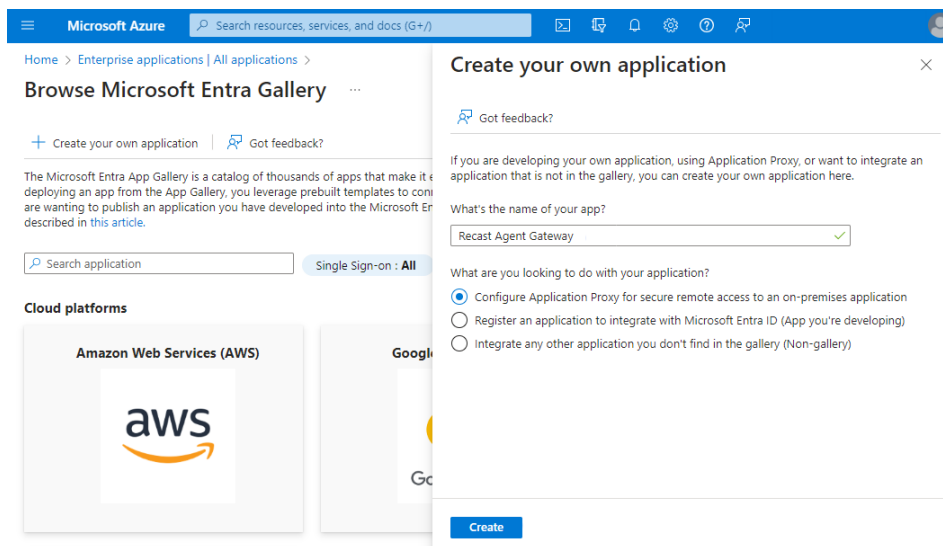
You must have an additional Agent Gateway installed on a separate server.

- This server must be Internet-connected and able to communicate with your Recast Management Server.
- If you're having issues with a self-signed certificate, you can use an http connection by adding an http connection type under **Internet Information Services (IIS) Manager > Sites > Bindings**. For details, see [How to add binding information to a site](#).

Connect the Agent Gateway to the Internet

To connect an Agent Gateway to the Internet using the Azure App Proxy service:

1. In the Microsoft Azure portal, under [Enterprise Applications](#), click **New application**.
2. Click **Create your own application**.
3. In the **Create your own application** panel, enter **Recast Agent Gateway** as the name of the application.
4. Select **Configure Application Proxy for secure remote access to an on-premises application**.
5. Click **Create**.



5. Click **Download Application Proxy Connector** then click **Accept terms & Download**.
6. After installing the Application Proxy Connector on your Agent Gateway server, click **I've finished the installation**.
7. Configure Application Proxy settings on the Basic tab:

- **Name:** Recast Agent Gateway
- **Internal Url:**
 - Your Agent Gateway server address and port
 - If you're having issues with a self-signed certificate, use http
- **External Url:** Address to set as the Gateway address when deploying Recast Agents
- **Pre Authentication:** Select **Passthrough**

Deploy Recast Agent to the Agent Gateway

You can now deploy the Recast Agent application and connect it to the Internet-connected Agent Gateway. The App Proxy Agent Gateway port is always 443.

Example:

```
msiexec.exe /i "Recast Agent.msi" /qn /norestart RCTENTERPRISESERVER="https://RMS.RecastDomain.com:444"  
AGENTGATEWAY="https://recastgw-tenant.msapproxy.net:443"
```

NOTE: Installing Recast Agent for the first time requires a Recast Management Server connection.

Authorize an Agent Gateway

When you install an Agent Gateway on a separate server, you'll need to manually authorize it in the Recast Management Server interface.

To manually authorize an Agent Gateway:

1. On the **Recast Agent Gateway** page, click the Edit icon to the right of the agent you want to authorize.
 2. In the **Edit Recast Agent** window, enable the **Authorized** checkbox and click **Save**.
-

Delete an Agent Gateway

To delete an Agent Gateway:

1. In the Recast Management Server interface, navigate to **Administration > Agent Gateways**.
 2. Click the Delete icon to the right of the Agent Gateway to remove and confirm the deletion.
-