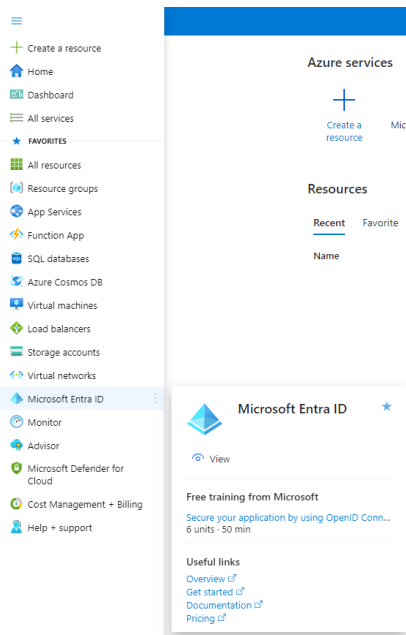


Configure the Microsoft Graph mail server

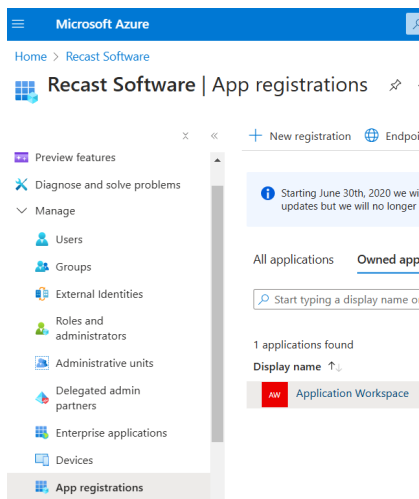
Last Modified on 04.21.26

Register an application in Azure Portal

1. Log into the [Azure Portal](#).
2. In the Azure Portal menu, navigate to **Microsoft Entra ID**.



3. In the left pane, navigate to **Manage > App registrations**.



4. Click **+ New registration** on the top toolbar.

Register an application

Application Workspace ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Recast Software only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

5. In the **Register an application** window that opens, configure the following:
 - In the **Supported account types** section select *Accounts in this organizational directory only (tenant only – Single tenant)*. For more information, see [Microsoft documentation](#).
 - In the **Redirect URI (optional)** section select *Web* and in the value field insert the FQDN of the Application Workspace Zone you want to add, with the `/api/auth/token/end` suffix.
6. Click **Register** on the bottom left, to complete the initial app registration.
7. You need to generate a client secret that facilitates communication between Application Workspace and Microsoft Entra ID (Azure AD). In the newly created app registration, navigate to **Manage > Certificates & secrets > Client secrets > New client secret**.

Application Workspace | API permissions

Search Refresh Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions**
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Recast Software

API / Permissions name	Type	Description	Admin consent requ...	Status
No permissions added				

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

8. Add a description and an expiration date for your client secret and then click **Add**. Note down your client secret after you create it because there is no way of retrieving the value after you leave this screen.

- You need to add permission to your app registration. With the new app open, navigate to **Manage > API permissions** and add the *Mail.Send* permission.
- After you add the permission, click **Grant admin consent for {your tenant}** above the permission list. It can take up to an hour before these settings take effect in Microsoft Entra ID (Azure AD).

Home > Application Workspace

Application Workspace | API permissions

Search Refresh Got feedback?

Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for Recast Software

API / Permissions name	Type	Description	Admin consent requ...	Status
No permissions added				

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Example:

```
https://<Virtual Host>/api/auth/token/end
```

Application Workspace configuration

- In Application Workspace, navigate to **Manage > System > Mail Settings**.
- Click **+ Create**. The **Create mail server** dialog box opens.
- On the **Type** screen, select *Microsoft Graph*.
- On the **Overview** screen enter the desired name, description and priority. After you finish inserting all necessary information, click **Next**.
- On the **Settings** screen, configure the following:
 - Enter the client ID and tenant ID of the application you previously registered in [Register an application in Azure Portal](#) . You can find them in the Overview screen within Microsoft Entra ID (Azure AD).
 - The client secret you generated earlier in [Register an application in Azure Portal](#) at step 7.
 - In the **From** field insert the mail address used to send the emails.
- On the **Summary** screen, click **Finish**.