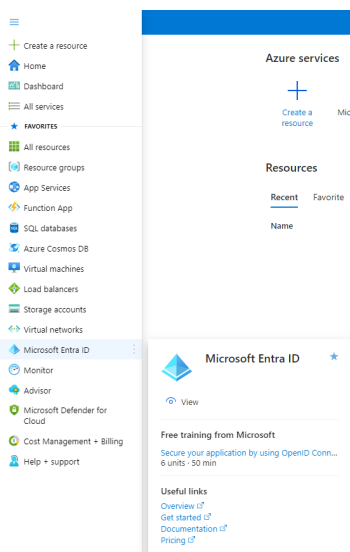


Configure Single Sign-On with Microsoft Entra ID

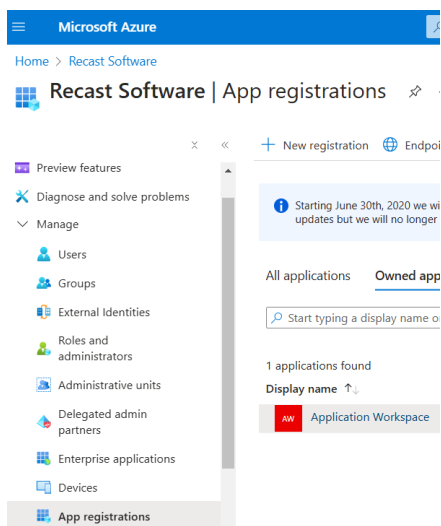
Last Modified on 2026-05-29

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

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 about the supported account types, see [Microsoft documentation](#).

Recast

- 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.

Example:

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

Home > Recast Software | App registrations >

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

6. Click on **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, in the left pane, navigate to **Manage > Certificates & secrets**. On the **Client secrets** tab, add a **New client secret**.

Search (Ctrl+/) << Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

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.

9. You need to add permissions to your app registration. In the left pane, navigate to **Manage > API permissions** and add the following permissions:

Recast

- *Directory.Read.All* – Allows Application Workspace to read data in your organization's directory, such as users, groups and apps. This is an Application type permission so it requires Admin Consent.
- *User.Read* – Allows users to sign in to Application Workspace. This is a Delegated type permission.
- (Optional) *User.Read.All* – Allows Application Workspace to read the user data and retrieve photos from Microsoft Entra ID (Azure AD). This is an Application type permission so it requires Admin Consent.
- (Optional) *GroupMember.ReadWrite.All* – Allows Application Workspace to modify group memberships. This is an Application type permission so it requires Admin Consent.

API / Permissions name	Type	Description	Admin Consent Requir...
▼ Microsoft Graph (3)			
Directory.Read.All	Application	Read directory data	Yes
User.Read	Delegated	Sign in and read user profile	-
User.Read.All	Application	Read all users' full profiles	Yes

For more information about permissions, see [Microsoft documentation](#).

10. Click on the **Grant admin consent for {your tenant}**. 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

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](#).

Messages:

- ⚠ 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](#)
- ℹ 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](#)

Creating the identity source in Application Workspace

1. Navigate to **Manage > Authentication > Identity Sources**
2. Click **+ Create** in the table toolbar. The **Create identity source** dialog box opens.
3. In the **Type** screen, select *Microsoft Entra ID (Azure AD)*. Click **Next**.
4. In the **Overview** screen:
 - For the **Name** field, we recommend you use only letters without spaces. If you plan to use Kerberos/NTLM, use the NETBIOS name.

Recast

- If the **Hidden** checkbox is selected, this identity source will not be shown as an option on the login page. Even hidden, you can configure it in the Agent file or using URL parameters as described in [URL Parameters](#).
5. After you finish inserting all necessary information, click **Next**.
 6. For an overview of the Microsoft Entra ID (Azure AD) identity source settings, see [Microsoft Entra ID \(Azure AD\)](#).
-