Recast

Configure Single Sign-On with Microsoft Entra ID

Last Modified on 2026-08-06

In order for Application Workspace to function with Intune, you'll first need to configure the following within the Microsoft Azure portal:

- Create the Entra ID App Registration to be used with Application Workspace
- Add client secret
- Grant the application API permissions

Create the Entra ID App Registration for Application Workspace

To create the app registration:

1. Log into https://portal.azure.com using your Azure credentials with full admin rights.

2. Search for **App registrations**.

3. On the **App registrations** page, click **New registration**.

4. Give the application a meaningful display **Name**. You can change the name later.

5. As the **Supported account type**, select **Single tenant only – <tenant>**.

6. As the **Redirect URI**, select 'Web' and enter 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`

7. Click **Register** to complete the initial app registration.

8. In the **Overview** pane that opens, copy the **Application (client) ID** and **Directory (tenant) ID**. You'll need to enter these later to create the Entra ID identity source in Application Workspace.

Add Client Secret

Next, you'll need to generate a client secret that facilitates communication between Application Workspace and Microsoft Entra ID.

To generate a client secret:

1. On the **App registrations** page, under **Manage**, click **Certificates & secrets**.

2. On the **Client secrets** tab, add a **New client secret**.

3. Add a client secret **Description**, choose when the secret **Expires**, and click **Add**.

   DO NOT navigate away from the page before completing the next step!

4. Copy the client secret value to a clipboard and save it to a secure location. You will not be able to see the client secret after navigating away from the page.

Add API Permissions for Application Workspace

Recast

Next, you need to add permissions to your app registration.

To add API permissions:

1. On the **App registrations** page, under **Manage**, click **API Permissions**.

2. Select **Add a permission**.

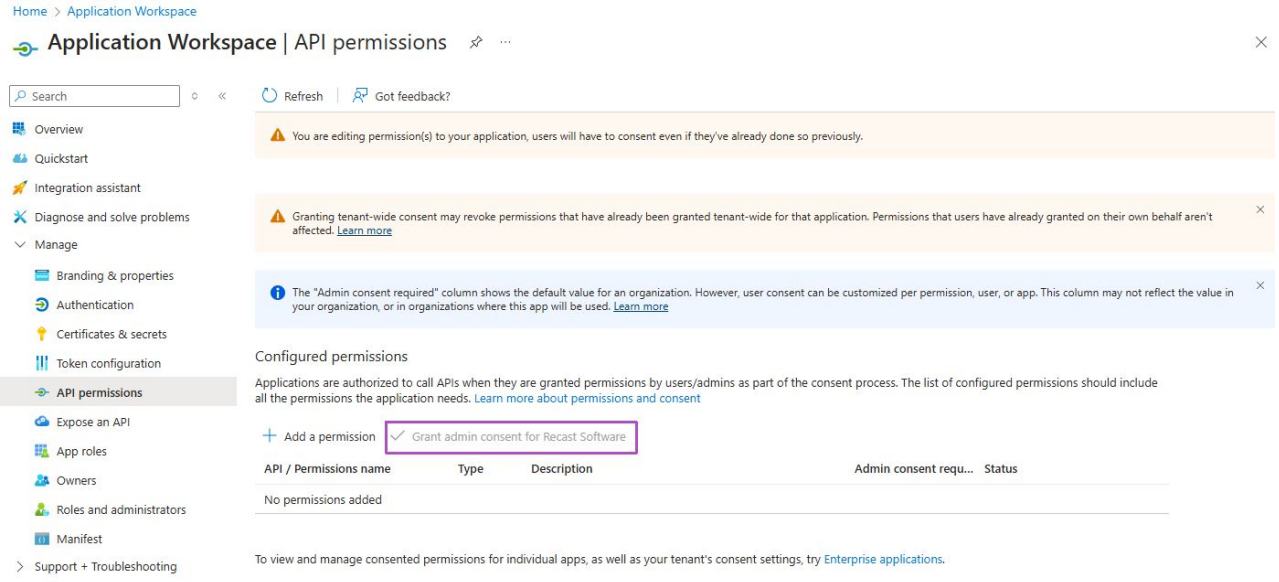
3. On the **Microsoft APIs** tab, click **Microsoft Graph**.

4. Add the following permissions:

Application permissions (require Admin consent)	Directory.Read.All	Allows Application Workspace to read data in your organization's directory, such as users, groups and apps
	User.Read.All (Optional)	Allows Application Workspace to read the user data and retrieve photos from Entra ID
	GroupMember.ReadWrite.All	Allows Application Workspace to modify group memberships
Delegated permissions	User.Read	Allows users to sign into Application Workspace

For more information, see Microsoft Graph permissions reference – Microsoft Graph | Microsoft Learn

5. Click **Grant admin consent for <Tenant Name>**. It can take up to an hour before these settings take effect in Entra ID.



Create the identity source in Application Workspace

As a last step to configuring single sign-on, create an Entra ID identity source within Application Workspace.

To create the identity source:

1. In Application Workspace, navigate to **Manage** > **Authentication** > **Identity Sources**.

2. Click **Create** in the table toolbar. The **Create identity source** dialog box opens.

3. In the **Create identity source** window that opens, select 'Microsoft Entra ID (Azure AD)' as the **Type**. Click **Next**.

4. On the **Overview** tab:
   - Enter a **Name** – We recommend using only letters without spaces. If you plan to use Kerberos/NTLM, use the NETBIOS name.
   - 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. Click **Next**.

6. On the **Settings** tab, select Application and Synchronization settings. For an explanation of all Entra ID identity source settings, see Microsoft Entra ID (Azure AD).

> You will need to enter the **Application (client) ID**, **Directory (tenant) ID**, and **Client secret** you copied down earlier.

7. After you finish entering all the necessary information, click **Next**.