

Last Modified on Thursday, 29-Jan-2026 17:05:57 GMT

Some organizations may choose to control the use of enterprise applications in Office 365 by restricting the ability for users to consent to third-party multi-tenant applications accessing user profile data in Azure Active Directory.

The screenshot displays the Microsoft Azure portal interface for managing users and groups. The left-hand navigation pane includes links to 'New', 'Dashboard', 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', and 'Azure Active Directory'. The main content area is titled 'Users and groups - User settings' and contains a sub-header 'Azure Active Directory'. Below this, there are tabs for 'Overview', 'MANAGE', and 'Groups'. The 'MANAGE' tab is active, showing a list of settings: 'All users', 'All groups', 'Password reset', 'Company branding', 'User settings', and 'Group settings'. The 'User settings' option is highlighted with a red box. To the right, the 'Enterprise applications' section is also highlighted with a red box. It contains a toggle switch for 'Users can consent to apps accessing company data on their behalf', which is currently set to 'No'. Below this, there is a link to 'Users can add gallery apps to their Access Panel' and another toggle switch, also set to 'No'. The 'App registrations' section is highlighted with a red box and contains a toggle switch for 'Users can register applications', which is also set to 'No'.

Given this configuration, two things may be done to allow users to access the Read&Write application:

- Navigate to Azure Admin Settings -> Azure Active Directory -> Enterprise Applications -> All Applications -> Read&Write.
- Select Users and Groups -> Add User/Group.

2 A Global Administrator must give consent on behalf of users

- Using an administrator account to sign-in to Office 365, the Administrator will need to copy the link below, replacing **{tenant}** with either the Primary domain or Tenant ID of their Azure Active Directory.

For Read&Write Mac v7.3 and above:

https://login.microsoftonline.com/%tenant%/v2.0/adminconsent?client_id=14d66fd9-3098-4e0f-8721-a35a3785d895&scope=https://graph.microsoft.com/User.Read%20https://graph.microsoft.com/email%20https://graph.microsoft.com/openid%20https://graph.microsoft.com/contacts%20https://graph.microsoft.com/calendars%20https://graph.microsoft.com/files.read%20https://graph.microsoft.com/groups.read%20https://graph.microsoft.com/me%20https://graph.microsoft.com/messages.read%20https://graph.microsoft.com/people.read%20https://graph.microsoft.com/sites.read%20https://graph.microsoft.com/user_impersonation

If you also have Read&Write for Windows, please see our [Windows support article here](#) for the Windows link to use.

- You will be prompted to consent for the read permissions that the Read&Write application needs. This information can be found in Azure Portal, in the Overview section of Azure Active Directory.
- After consenting, you'll be directed to the Read&Write login page <https://idp.texthelp.com>. Please allow a short period of time for the Read&Write Application to be added to your catalog.

After completing these steps, non-admin users should be able to access!