

Azure Active Directory admin center → Enterprise Applications → Manage/User Settings

[Dashboard](#) > [Enterprise applications](#)

Enterprise applications | User settings

« Save Discard Got feedback?

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications
- Application proxy
- User settings**

Security

- Conditional Access
- Consent and permissions

Activity

- Sign-ins
- Usage & insights (Preview)
- Audit logs
- Provisioning logs (Preview)
- Access reviews
- Admin consent requests (Preview)

Troubleshooting + Support

- Virtual assistant (Preview)
- New support request

Enterprise applications

Users can consent to apps accessing company data on their behalf Yes No

! You're using the public preview settings for managing end-user consent. Go to [Consent and permissions](#) to manage these settings.

Users can consent to apps accessing company data for the groups they own Yes No Limited

Users can add gallery apps to their Access Panel Yes No

Admin consent requests (Preview)

Users can request admin consent to apps they are unable to consent to Yes No

Select users to review admin consent requests * 1 admins selected

Selected users will receive email notifications for requests Yes No

Selected users will receive request expiration reminders Yes No

Consent request expires after (days)

Office 365 Settings

Users can only see Office 365 apps in the Office 365 portal Yes No

Azure Active Directory admin center → Enterprise Applications → Security → Consent and permissions → User consent settings

[Dashboard](#) > [Enterprise applications](#)

Consent and permissions | User consent settings

« Save Discard

Manage

- User consent settings**
- Permission classifications

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data. [Learn more about consent and permissions](#)

User consent for applications
Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)


- Do not allow user consent
An administrator will be required for all apps.
- Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
! 4 permissions classified as low impact
- Allow user consent for apps
All users can consent for any app to access the organization's data.

Group owner consent for apps accessing data
Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. [Learn more](#)

- Do not allow group owner consent
Group owners cannot allow applications to access data for the groups they own.
- Allow group owner consent for selected group owners
Only selected group owners can allow applications to access data for the groups they own.
- Allow group owner consent for all group owners
All group owners can allow applications to access data for the groups they own.


Azure Active Directory admin center → Enterprise Applications → Security → Consent and permissions → Permission classifications

[Dashboard](#) > [Enterprise applications](#) > [Consent and permissions](#)

 **Consent and permissions** | Permission classifications ...

Manage



 User consent settings

 **Permission classifications**

« [+ Add permissions](#)

Classify permissions

Choose which permissions are classified as "low risk". [Learn more](#)

API used	Permissions	Description	
Microsoft Graph	User.Read	Sign in and read user profile	
Microsoft Graph	openid	Sign users in	
Microsoft Graph	offline_access	Maintain access to data you have given it access to	
Microsoft Graph	profile	View users' basic profile	