

<https://learn.microsoft.com/en-en/entra/identity/enterprise-apps/configure-admin-consent-workflow>

Microsoft Entra Admin Center → Entra ID → Enterprise Apps → Consent and Permission → Admin Consent Settings

Home > Enterprise applications | Consent and permissions > Consent and permissions

Consent and permissions | Admin consent settings

« Save Discard

Manage

- User consent settings
- Admin consent settings**
- Permission classifications

Admin consent requests

Users can request admin consent to apps they are unable to consent to [?](#)

☒ Yes ☐ No

Who can review admin consent requests [?](#)

Reviewer type	Reviewers
Users	2 users selected.
Groups (Preview)	1 group selected.
Roles (Preview)	+ Add roles

Selected users will receive email notifications for requests [?](#)

☒ Yes ☐ No

Selected users will receive request expiration reminders [?](#)

☒ Yes ☐ No

Consent request expires after (days) [?](#)

30

Microsoft Entra Admin Center → Entra ID → Enterprise Apps → Consent and Permission → User Consent Settings

Home > Enterprise applications | Consent and permissions >

Consent and permissions | User consent settings

« Save Discard Got feedback?

Manage

- User consent settings**
- Admin consent settings
- Permission classifications

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

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
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](#)

☐ Let Microsoft manage your consent settings (Recommended)
Automatically update your organization to Microsoft's current user consent guidelines. [Learn more](#)

Microsoft Entra Admin Center → Entra ID → Enterprise Apps → Consent and Permission → Permission Classifications

Home > Enterprise applications | Consent and permissions > Consent and permissions

Consent and permissions | Permission classifications

...

«

Got feedback?

Manage

User consent settings

Admin consent settings

Permission classifications

Classify permissions

Use permission classifications in consent policies to identify the set of permissions that users are allowed to consent to. [Learn more](#)

Low

Medium (Preview)

High (Preview)

Define low-risk permissions here. Only delegated permissions that don't require admin consent are supported.

+ Add permissions

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