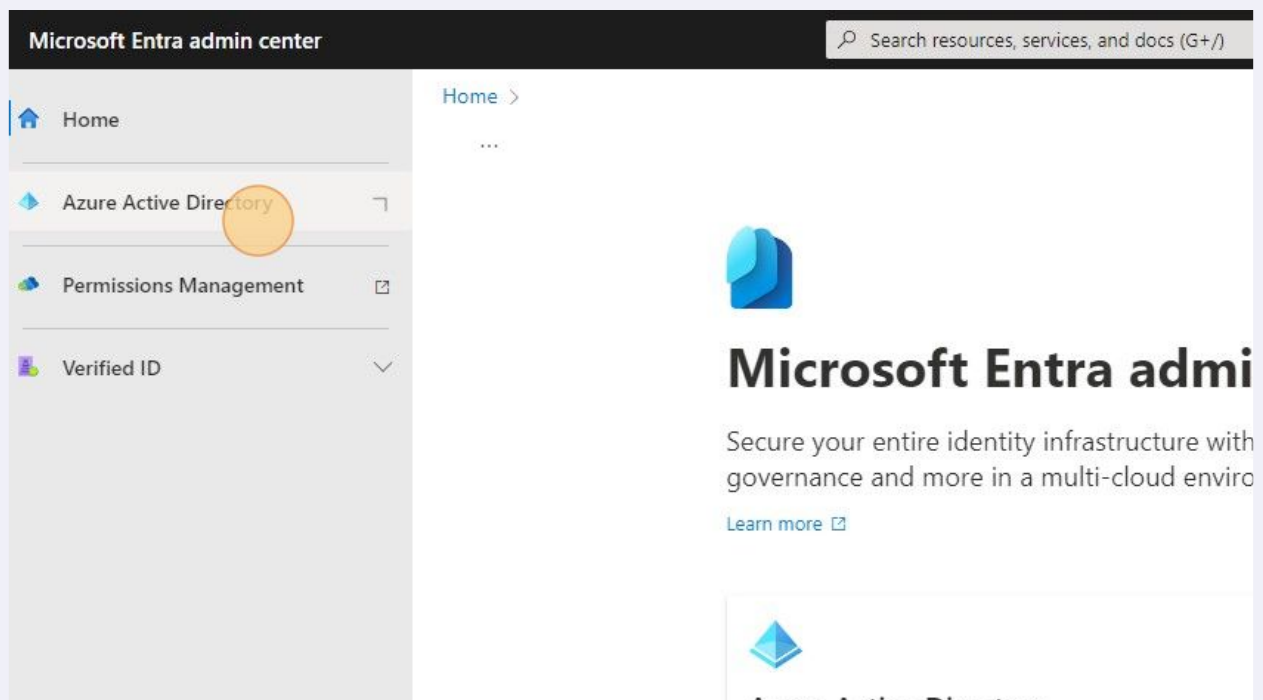


How to Disable Users from Granting Consent to Unreliable Applications

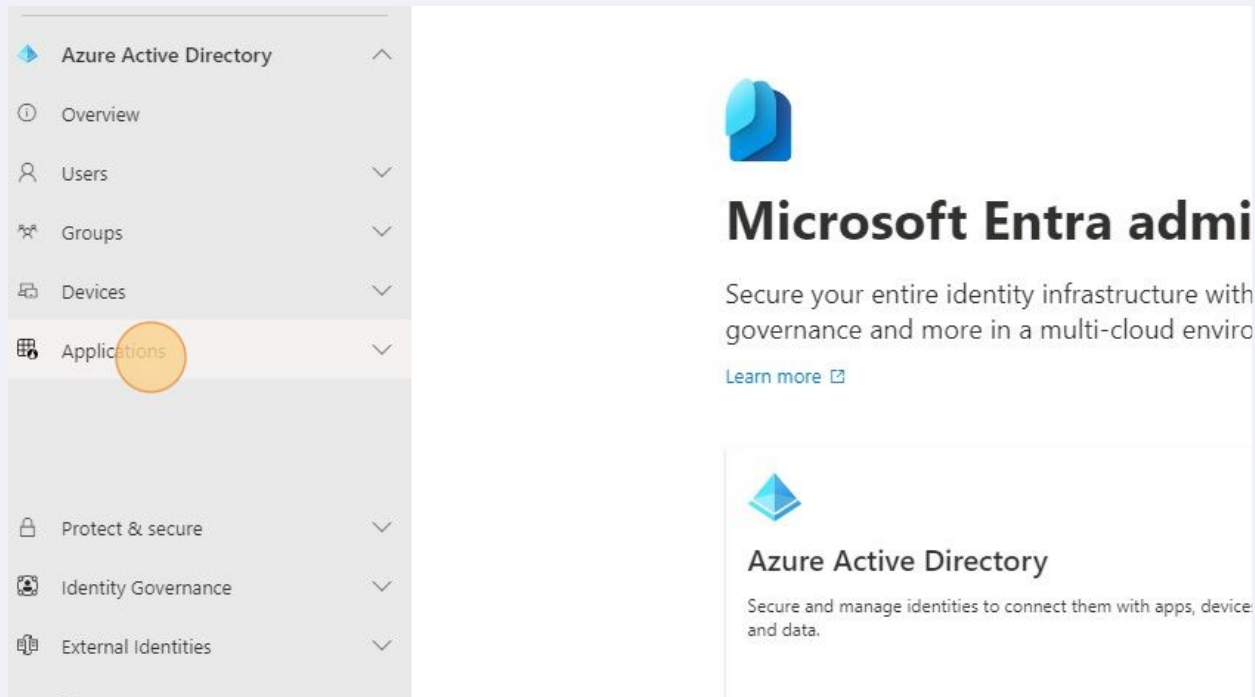
In this guide, we walk through configuring the setting controlling which types of applications users can grant consent to.

1 Navigate to entra.microsoft.com

2 Click "Azure Active Directory"

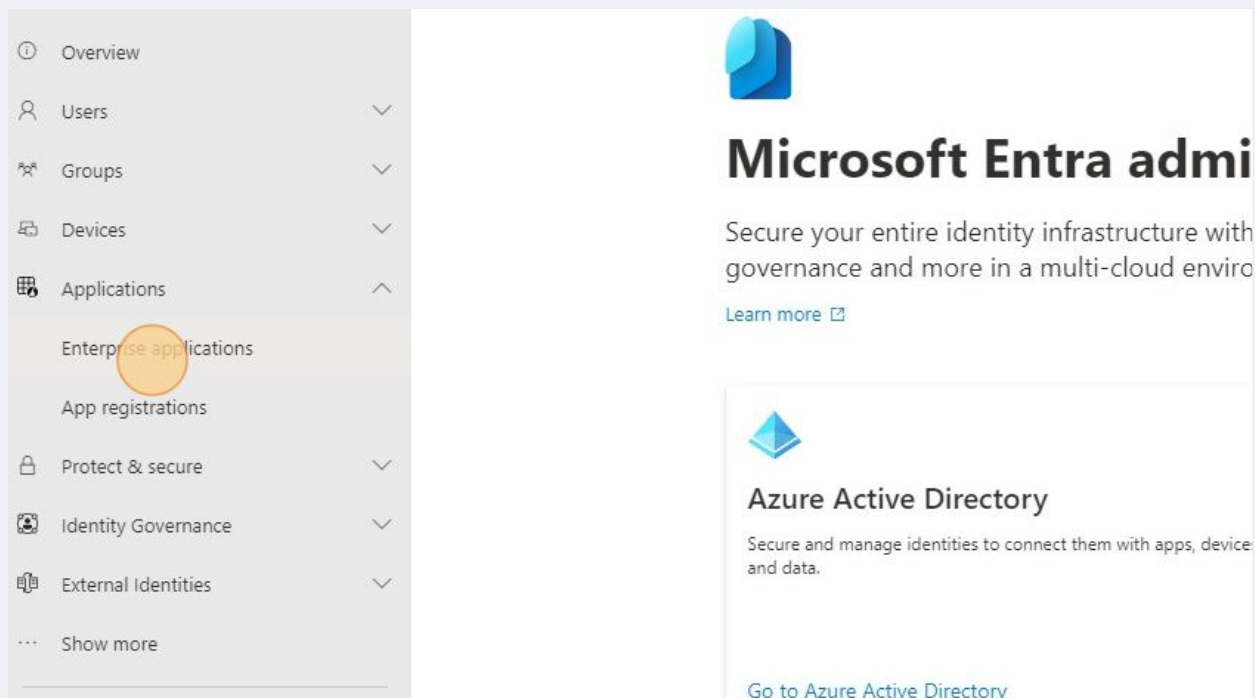


3 Click "Applications"



The screenshot shows the Microsoft Entra admin center interface. On the left, a navigation pane lists various sections: Azure Active Directory, Overview, Users, Groups, Devices, Applications, Protect & secure, Identity Governance, and External Identities. The 'Applications' item is highlighted with an orange circle. The main content area on the right features the Microsoft Entra admin center logo and title, followed by a description: 'Secure your entire identity infrastructure with governance and more in a multi-cloud environment'. Below this, there is a 'Learn more' link and a section for 'Azure Active Directory' with its own description and a 'Go to Azure Active Directory' link.

4 Click "Enterprise applications"



The screenshot shows the Microsoft Entra admin center interface. On the left, the 'Applications' section is expanded, and 'Enterprise applications' is highlighted with an orange circle. The main content area on the right features the Microsoft Entra admin center logo and title, followed by a description: 'Secure your entire identity infrastructure with governance and more in a multi-cloud environment'. Below this, there is a 'Learn more' link and a section for 'Azure Active Directory' with its own description and a 'Go to Azure Active Directory' link.

5 Click "Consent and permissions"

The screenshot shows the Microsoft Entra ID console. On the left, the 'Applications' menu is expanded, and 'Enterprise applications' is selected. In the center, the 'Consent and permissions' option is highlighted with an orange circle. On the right, a table lists 8 applications found.

Name	Object ID
FGLFW-MHT-VPN	3425888...
FGLFW-MHT-LAN	4dbb1cb...
FGLFW-DNV-Admin	792f4cf9...
Blackpoint Cloud Response	918301a...
FGLFW-MHT-Admin	a83431a...
FGLFW-DNV-VPN	c2c1e88...
Blackpoint Managed Defend...	c376a04...
FGLFW-DNV-LAN	f203c88...

6 Click "Allow user consent for apps from verified publishers, for selected permissions (Recommended)"

The screenshot shows the 'User consent settings' page in the Microsoft Entra ID console. The 'User consent settings' tab is selected. The page title is 'Control when end users and group owners are allowed to grant consent to applications, and when they require administrator review and approval. Allowing users to grant apps access to data helps them acquire useful information, but it 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 (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or for apps that are approved by the administrator.

[Select permissions to classify as low impact](#)

☐ Allow user consent for apps
All users can consent for any app to access the organization's data.

Information You have enabled limited user consent to apps, but users can still consent to apps accessing the groups they belong to. To prevent this, you can restrict user consent to group data below.

7 Click "Select permissions to classify as low impact"

Control when end users and group owners are allowed to grant consent to applications, and when they require administrator review and approval. Allowing users to grant apps access to data helps them acquire useful data, but it 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 (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or for apps that have been approved by your organization.

[Select permissions to classify as low impact](#)

☐ Allow user consent for apps
All users can consent for any app to access the organization's data.

You have enabled limited user consent to apps, but users can still consent to apps accessing the groups that they own. You can control this by enabling user consent to group data below.

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

8 Click "Add permissions"

Azure Active Directory

Manage

- User consent settings
- Admin consent settings
- Permission classifications

Classify permissions

Use permission classifications in consent policies to identify the set of permissions that you want to allow or deny.

Low Medium (Preview) High (Preview)

Define low-risk permissions here. Only delegated permissions that don't require administrator review and approval.

[+ Add permissions](#)

API used	Permissions
No delegated permissions found for classification 'low'	

[Get started by adding permissions](#)

9

Select:
User.Read
offline_access
openid
profile
email



Get started by adding the most used permission

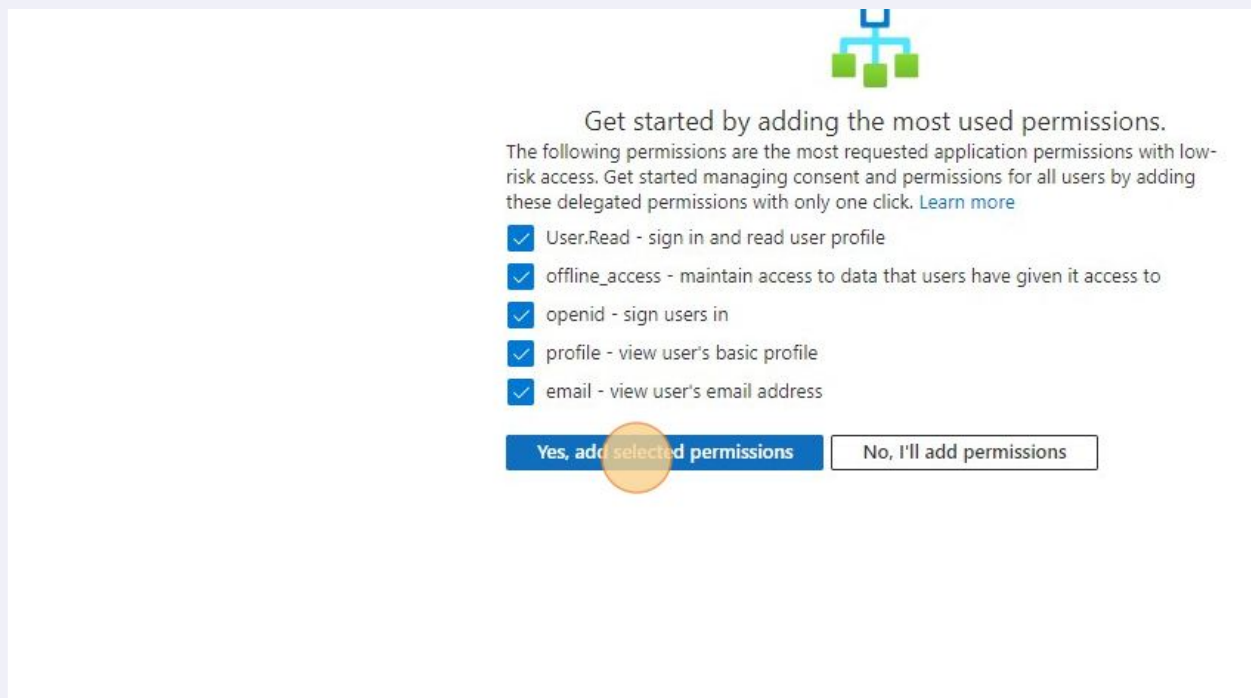
The following permissions are the most requested application permissions with low risk access. Get started managing consent and permissions for all users by adding these delegated permissions with only one click. [Learn more](#)

- ☒ User.Read - sign in and read user profile
- ☒ offline_access - maintain access to data that users have given it access to
- ☒ openid - sign users in
- ☒ profile - view user's basic profile
- ☒ email - view user's email address

Yes, add selected permissions

No, I'll add permissions

10 Click "Yes, add selected permissions"



11 After setting the permissions, click "Save"

