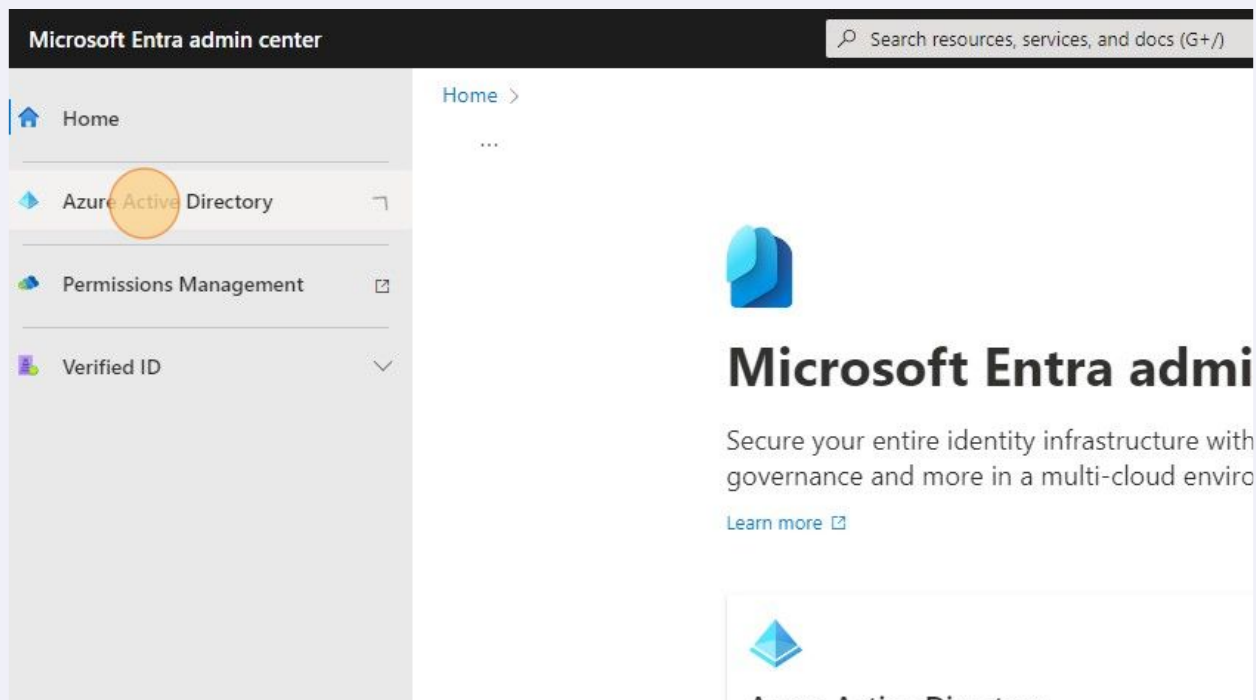


Configure Admin Consent Settings

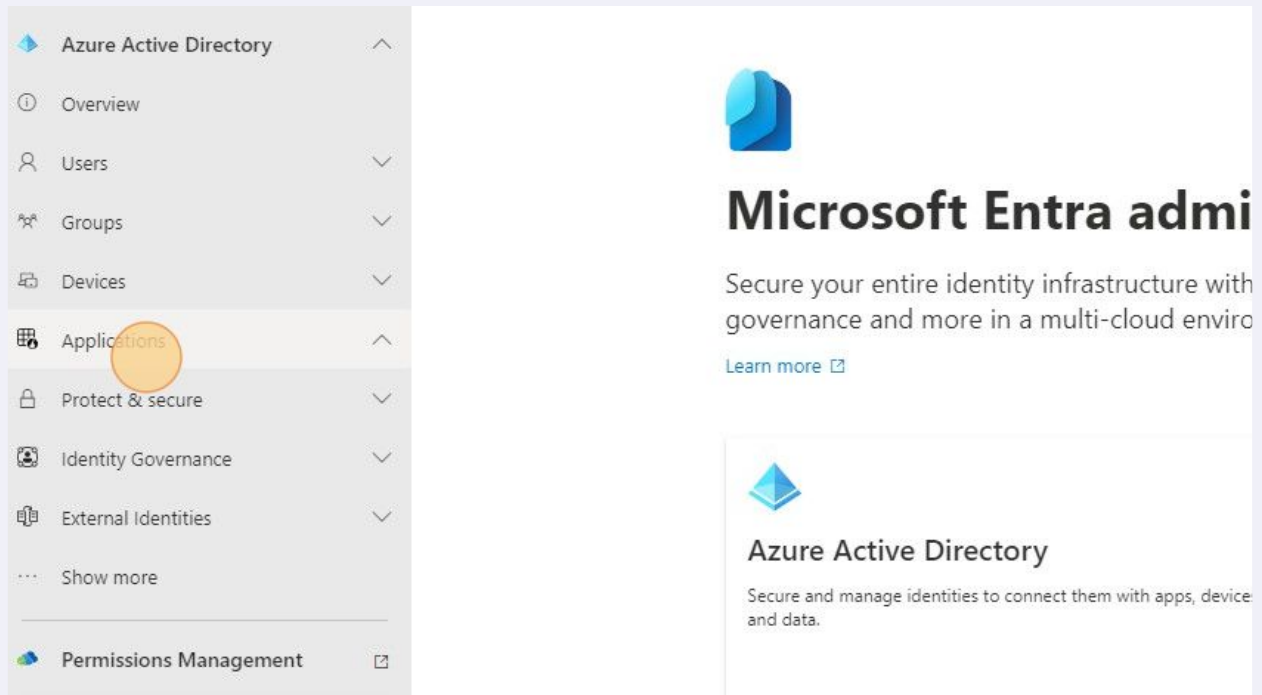
In this guide, we review how to restrict admin consent.

- 1 Navigate to entra.microsoft.com

- 2 Click "Azure Active Directory"

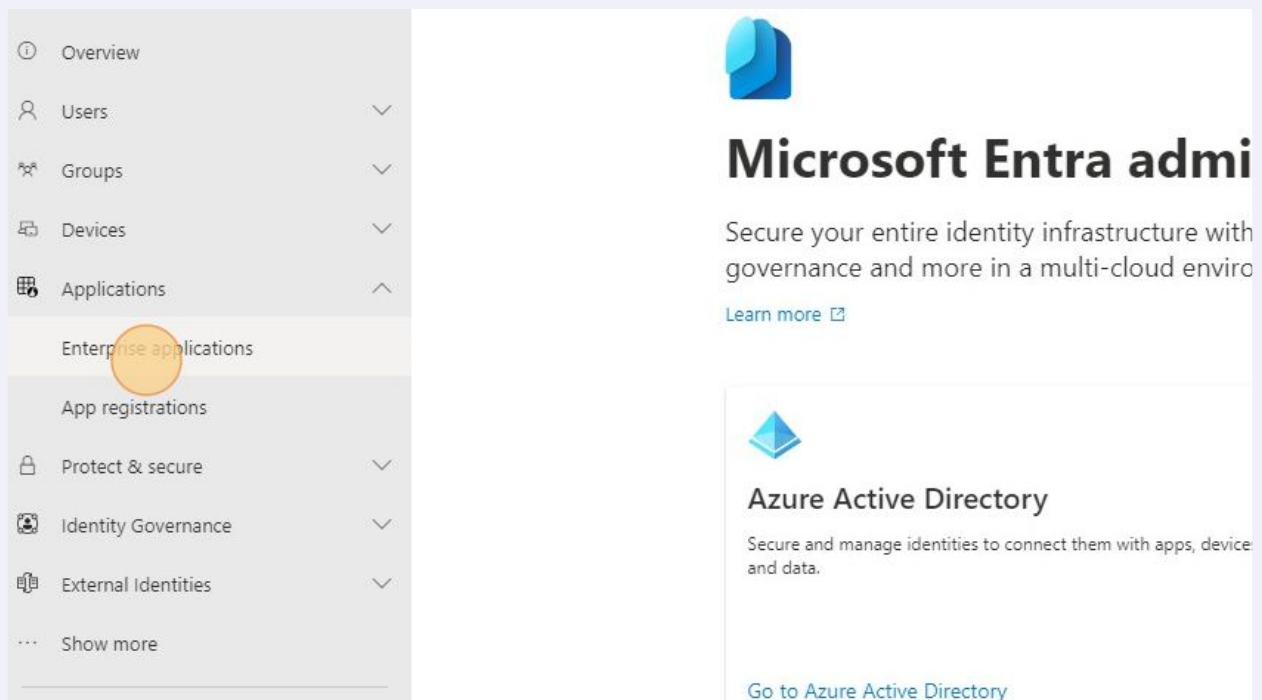


3 Click "Applications"



The screenshot shows the Microsoft Entra admin center interface. On the left, a navigation pane lists various management areas: Azure Active Directory, Overview, Users, Groups, Devices, Applications, Protect & secure, Identity Governance, External Identities, and Permissions Management. The 'Applications' item is highlighted with an orange circle. The main content area on the right features the Microsoft Entra logo and the heading 'Microsoft Entra admin center'. Below this, a description states: 'Secure your entire identity infrastructure with governance and more in a multi-cloud environment'. A 'Learn more' link is provided. Further down, there is a section for 'Azure Active Directory' with a description: 'Secure and manage identities to connect them with apps, devices, and data.'.

4 Click "Enterprise applications"



The screenshot shows the Microsoft Entra admin center interface. On the left, the 'Applications' menu is expanded, and 'Enterprise applications' is highlighted with an orange circle. The main content area on the right features the Microsoft Entra logo and the heading 'Microsoft Entra admin center'. Below this, a description states: 'Secure your entire identity infrastructure with governance and more in a multi-cloud environment'. A 'Learn more' link is provided. Further down, there is a section for 'Azure Active Directory' with a description: 'Secure and manage identities to connect them with apps, devices, and data.' and a 'Go to Azure Active Directory' link.

5 Click "Consent and permissions"

The screenshot shows the Microsoft Entra admin center interface. On the left, the 'Applications' menu is expanded, and 'Enterprise applications' is selected. The 'Manage' dropdown menu is open, and 'Consent and permissions' is highlighted with an orange circle. On the right, a search bar is visible, and 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 | c2c1e88b |
| Blackpoint Managed Defend... | c376a04a |
| FGLFW-DNV-LAN | f203c88b |

6 Click "Admin consent settings"

The screenshot shows the Microsoft Entra admin center interface. The left sidebar shows the 'Applications' menu expanded, and 'Enterprise applications' is selected. The 'Manage' dropdown menu is open, and 'Admin consent settings' is highlighted with an orange circle. The main content area shows the 'Consent and permissions | User consent settings' page, which includes a 'Manage' section with 'User consent settings', 'Admin consent settings', and 'Permission classifications'. The 'Admin consent settings' section is currently selected.

Consent and permissions | User consent settings

Control when end users and group owners are allowed to grant administrator review and approval. Allowing users to grant consent can represent a risk in some situations if it's not managed properly.

User consent for applications

Configure whether users are allowed to consent for applications.

☐ Do not allow user consent

An administrator will be required for all apps.

☒ Allow user consent for apps from verified publishers

All users can consent for permissions classified as low impact.

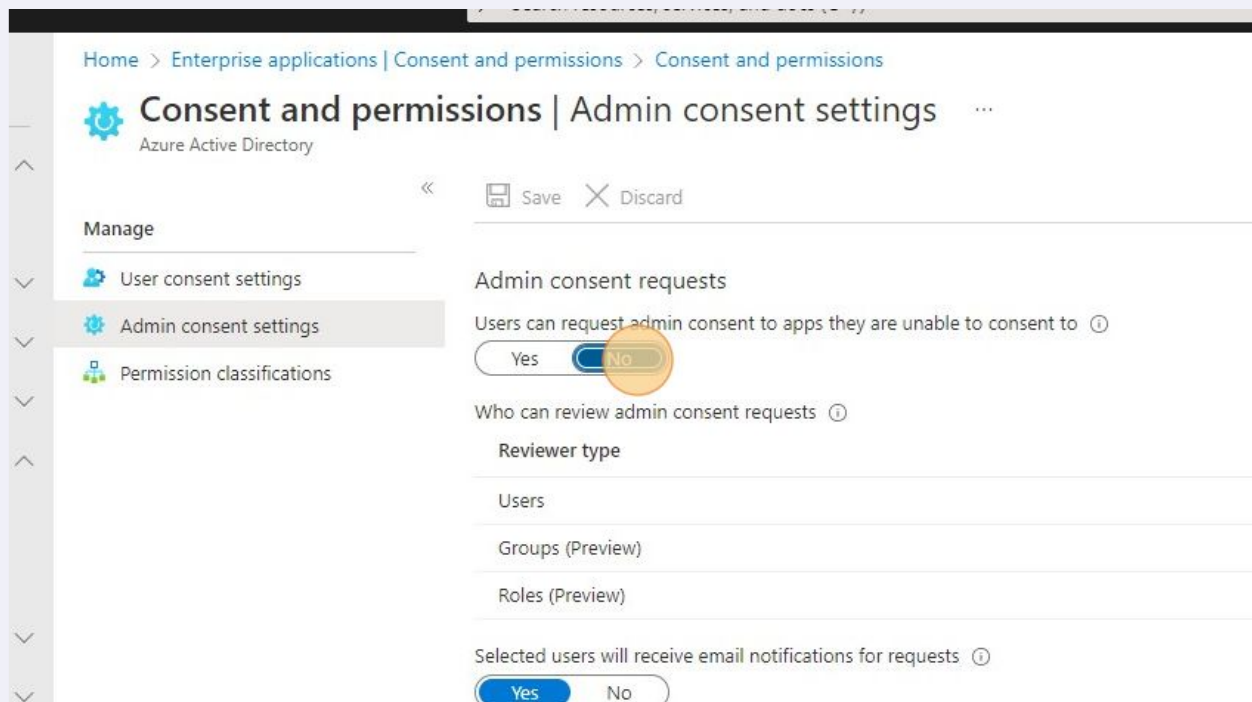
[5 permissions classified as low impact](#)

☐ Allow user consent for any app

All users can consent for any app to access their data.

7

Click "No" for "Users can request admin consent to apps they are unable to consent to"



8

Click "Save"

