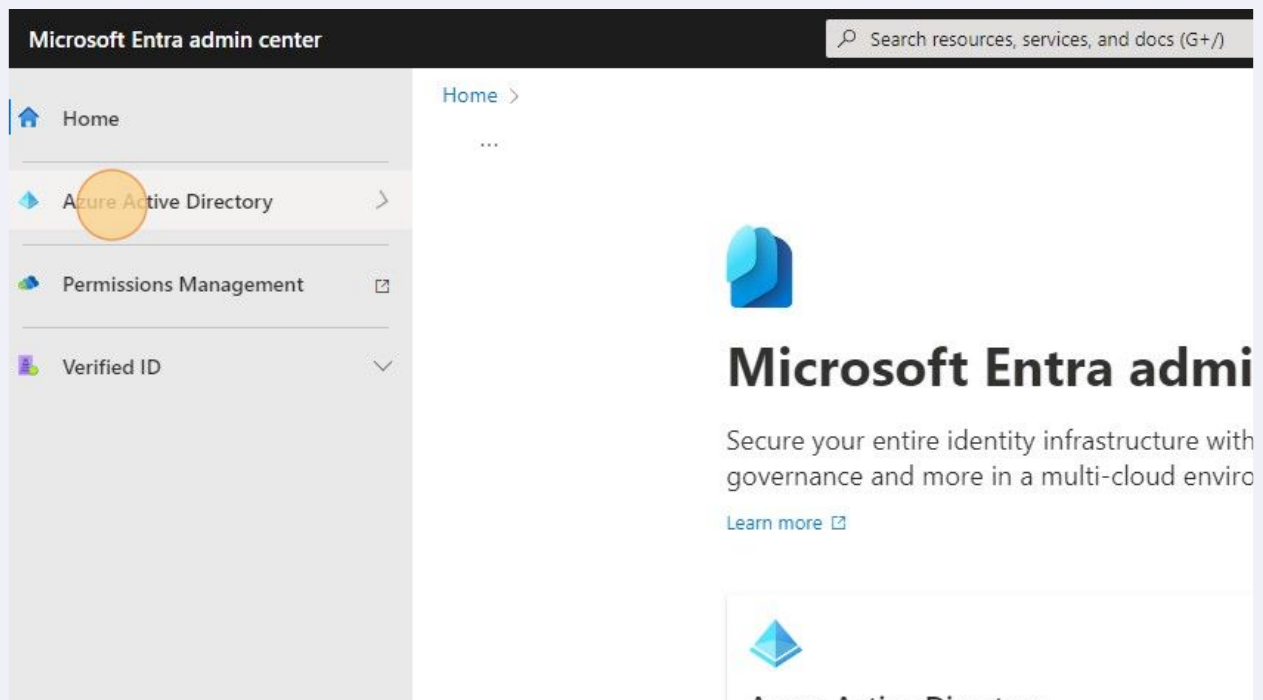


# How to Configure Password Protection

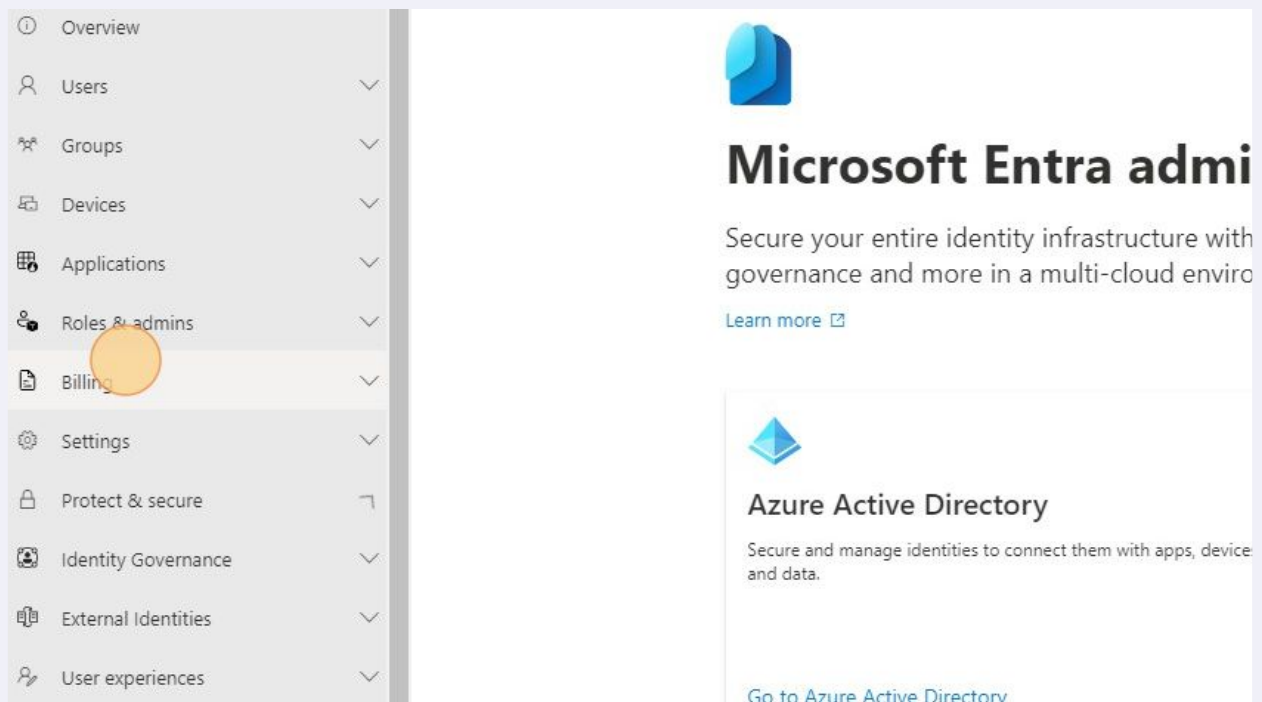
In this guide, we walk through our standard password protection settings.

- 1 Navigate to [entra.microsoft.com](https://entra.microsoft.com)

- 2 Click "Azure Active Directory"

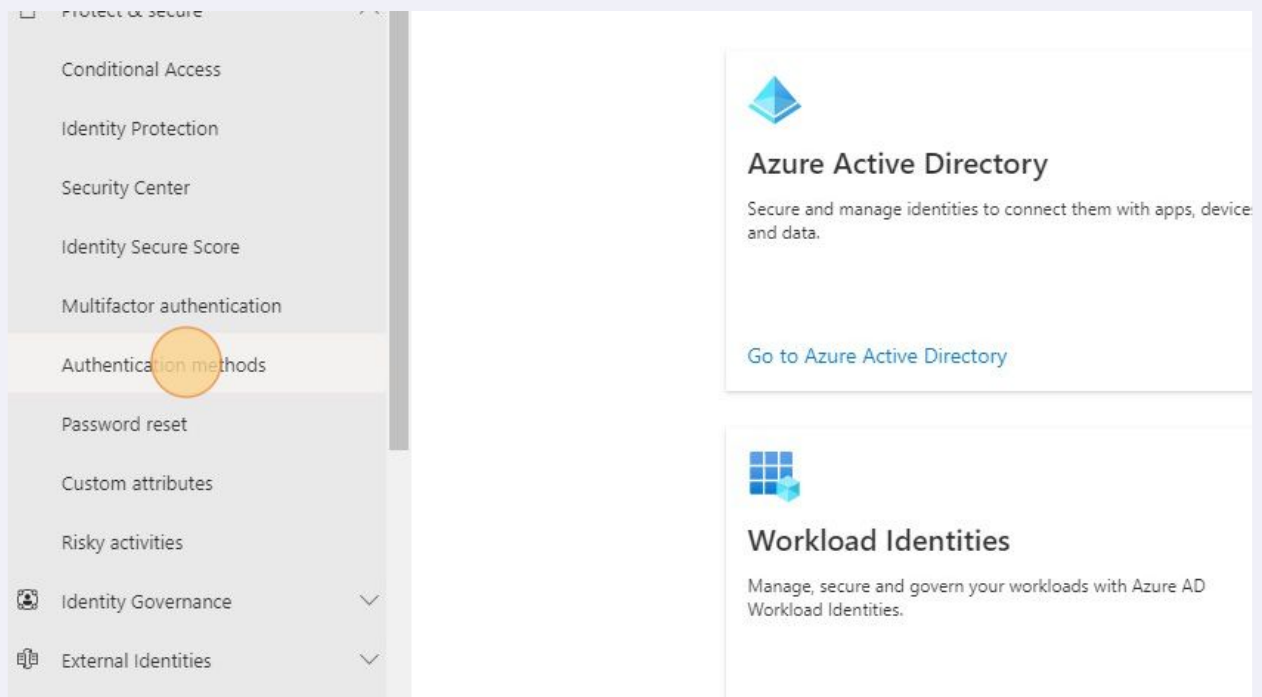


### 3 Click "Protect & secure"



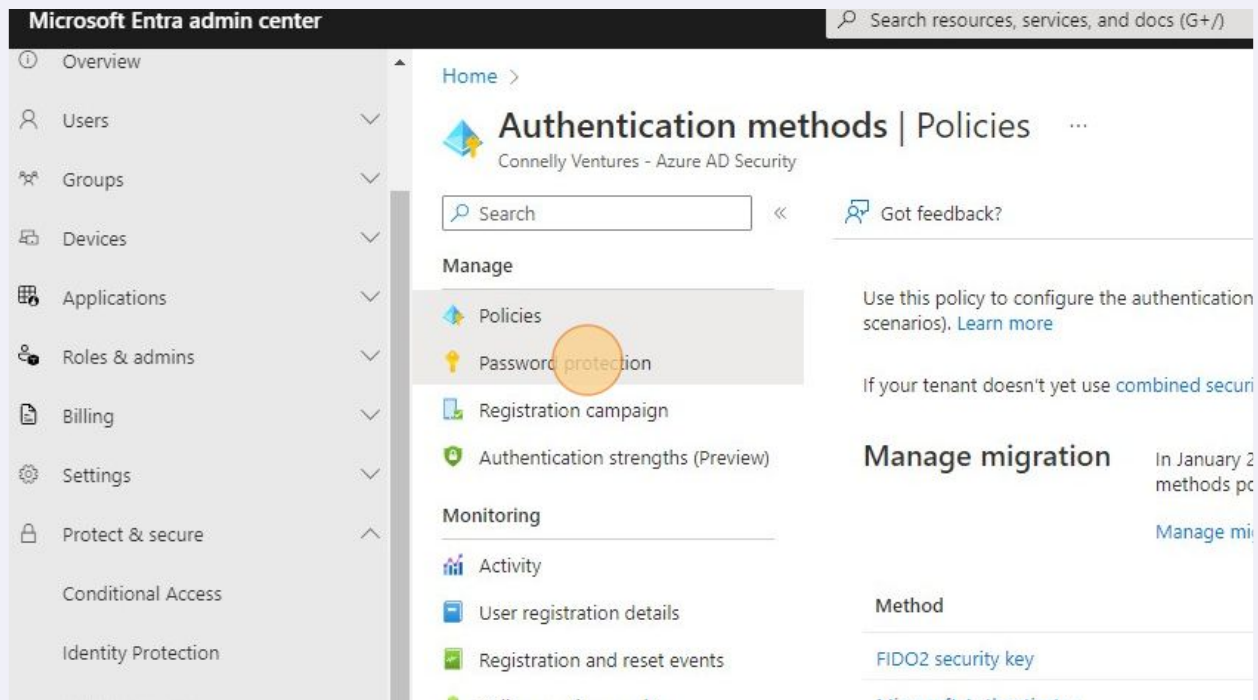
The screenshot shows the Microsoft Entra admin center interface. On the left, a navigation pane lists various sections: Overview, Users, Groups, Devices, Applications, Roles & admins, Billing, Settings, Protect & secure, Identity Governance, External Identities, and User experiences. The 'Protect & secure' 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 its logo and a description: 'Secure and manage identities to connect them with apps, devices, and data.' A 'Go to Azure Active Directory' link is also present.

### 4 Click "Authentication methods"

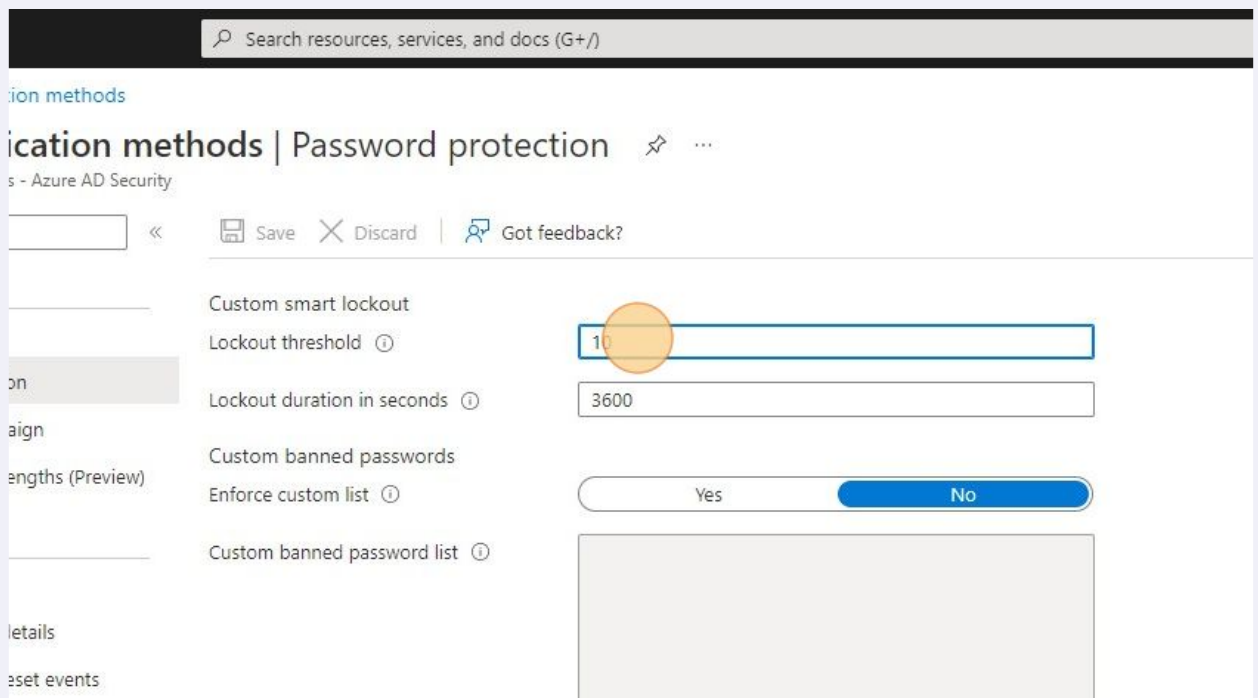


The screenshot shows the Microsoft Entra admin center interface with the 'Protect & secure' section expanded. The 'Authentication methods' option is highlighted with an orange circle. The main content area on the right displays the 'Azure Active Directory' section with its logo and description: 'Secure and manage identities to connect them with apps, devices, and data.' A 'Go to Azure Active Directory' link is visible. Below this, the 'Workload Identities' section is shown with its logo and description: 'Manage, secure and govern your workloads with Azure AD Workload Identities.'

5 Click "Password protection"



6 In the "Lockout threshold" field, type "3"



**7** In the "Lockout duration in seconds" field, type "5000"

The screenshot shows the 'Password protection' settings in the Windows AD Security console. The 'Lockout duration in seconds' field is highlighted with an orange circle and contains the value '3600'. The 'Lockout threshold' is set to '3'. The 'Enforce custom list' toggle is set to 'No'.

Methods | Password protection

Custom smart lockout

Lockout threshold ① 3 ✓

Lockout duration in seconds ① 3600

Custom banned passwords

Enforce custom list ① Yes No

Custom banned password list ①

**8** Select "Yes" for "Custom banned passwords: Enforce custom list"

The screenshot shows the 'Password protection' settings in the Windows AD Security console. The 'Enforce custom list' toggle is highlighted with an orange circle and is set to 'Yes'. The 'Lockout duration in seconds' field now contains the value '5000'. The 'Enable password protection on Windows Server Active Directory' toggle is also set to 'Yes'.

Methods | Password protection

Custom smart lockout

Lockout threshold ① 3 ✓

Lockout duration in seconds ① 5000 ✓

Custom banned passwords

Enforce custom list ① Yes No

Custom banned password list ①

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ① Yes No

9

Type in any keywords that you DO NOT want users to be able to use in their passwords.

The screenshot shows the 'Password Protection for Windows Server Active Directory' settings in Windows Security. The interface includes a top bar with 'Save', 'Discard', and 'Got feedback?' buttons. The settings are organized into sections: 'Custom smart lockout' with 'Lockout threshold' (3) and 'Lockout duration in seconds' (5000); 'Custom banned passwords' with 'Enforce custom list' (Yes) and 'Custom banned password list' (empty text box); and 'Password protection for Windows Server Active Directory' with 'Enable password protection on Windows Server Active Directory' (Yes) and 'Mode' (Enforced). A yellow circle highlights the 'Custom banned password list' text box.

Custom smart lockout

Lockout threshold ① 3 ✓

Lockout duration in seconds ① 5000 ✓

Custom banned passwords

Enforce custom list ① Yes No

Custom banned password list ①

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ① Yes No

Mode ① Enforced Audit



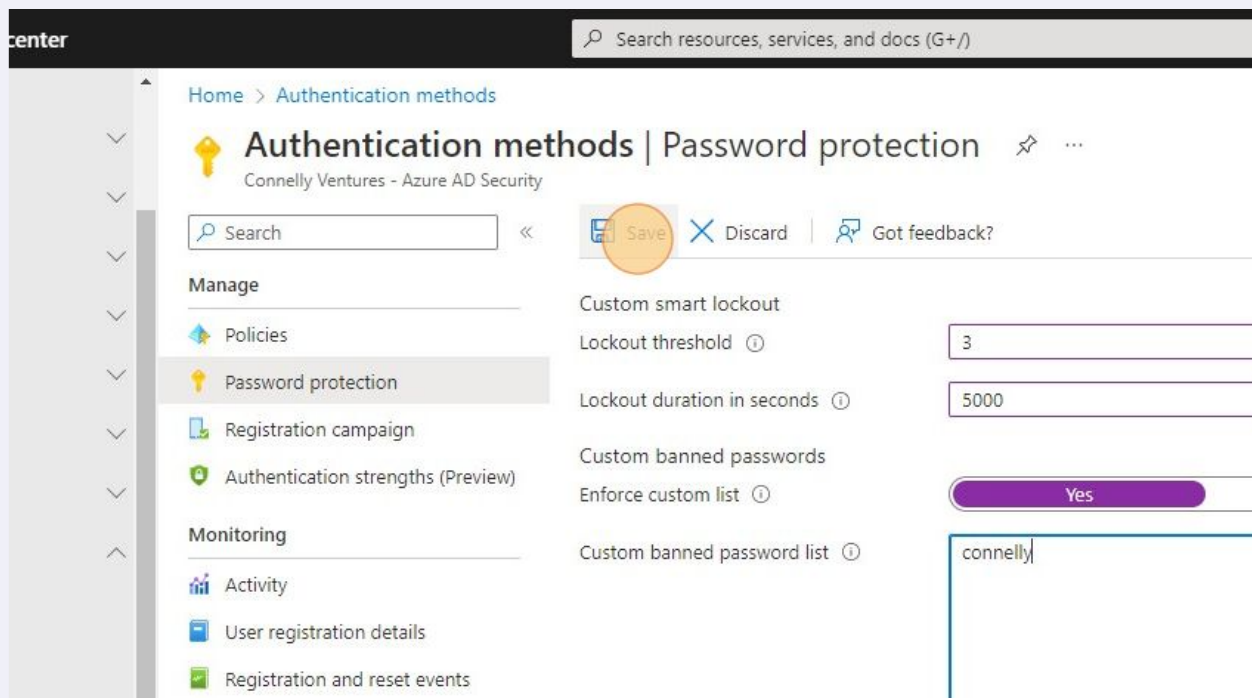
Alert!

Any word on the custom banned password list, will not be able to be used in any iteration.

See this link for details:

[learn.microsoft.com/en-us/azure/active-directory...](https://learn.microsoft.com/en-us/azure/active-directory...)

10 Click "Save"



11 You should see a notification that the settings were saved successfully.

