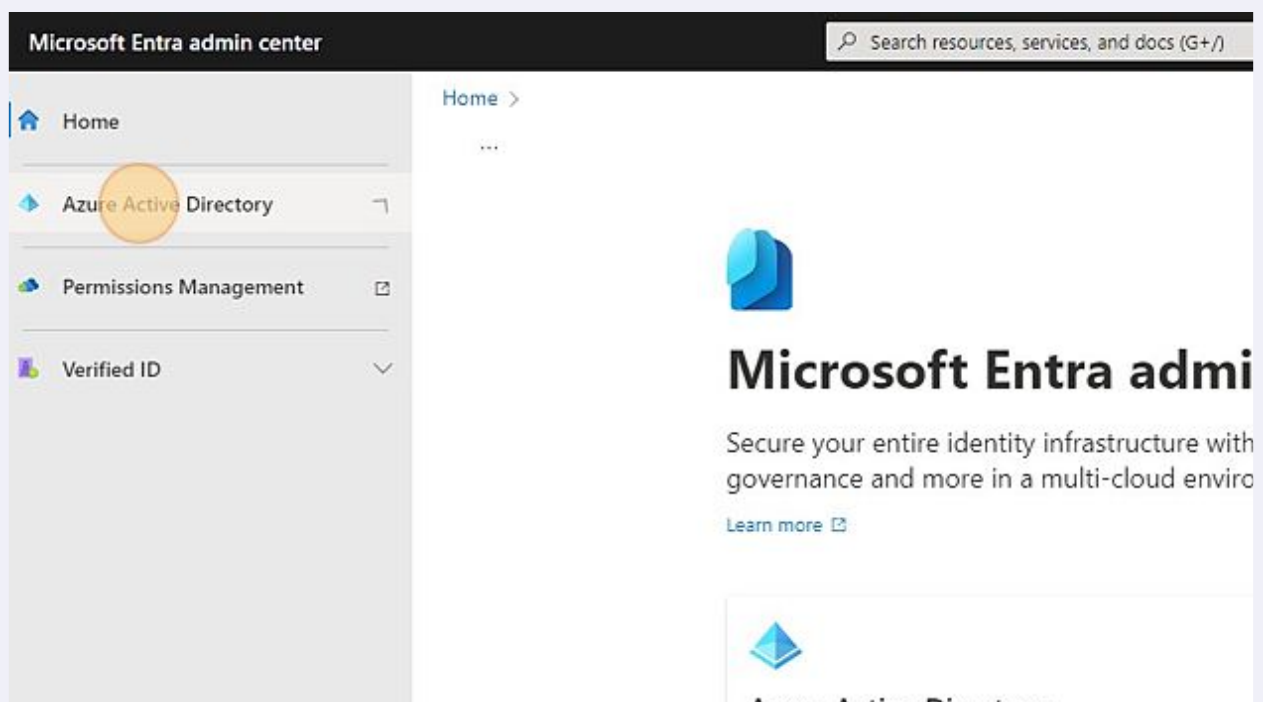


How to Configure Microsoft MFA Authentication Settings

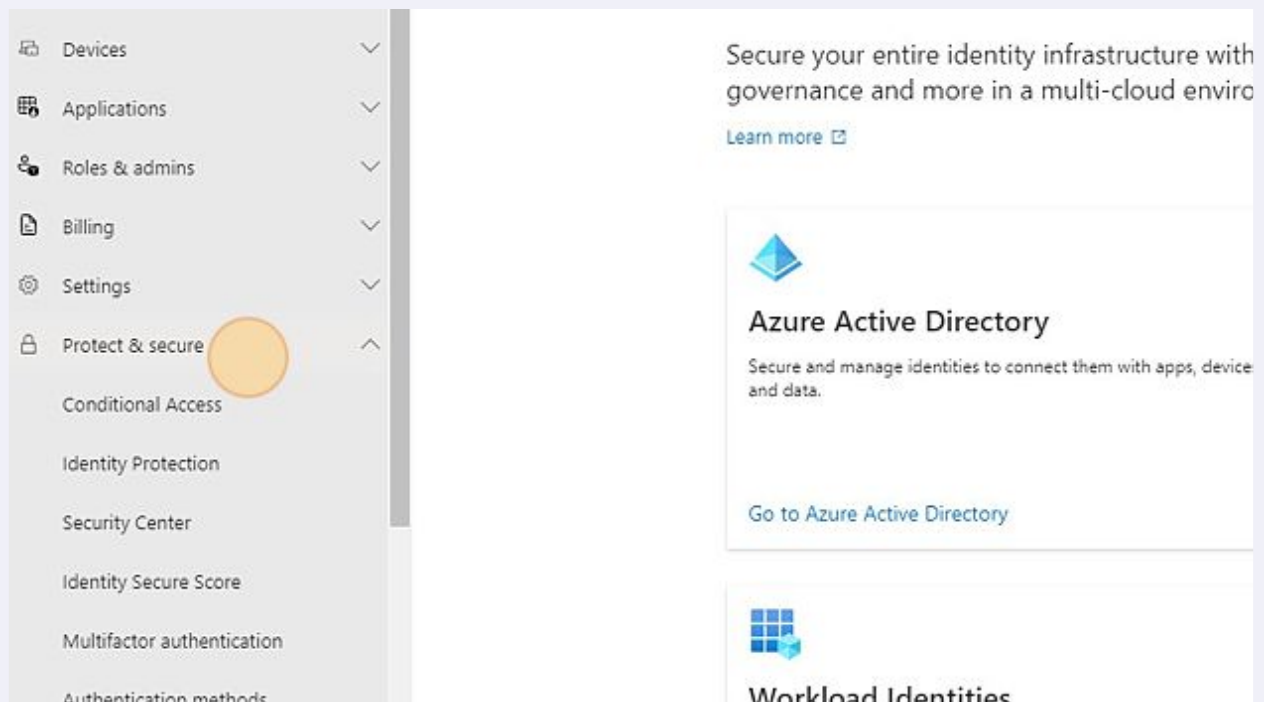
In this document, we cover how to configure the specific authentication settings available to us with the Microsoft MFA client.

- 1 Navigate to entra.microsoft.com

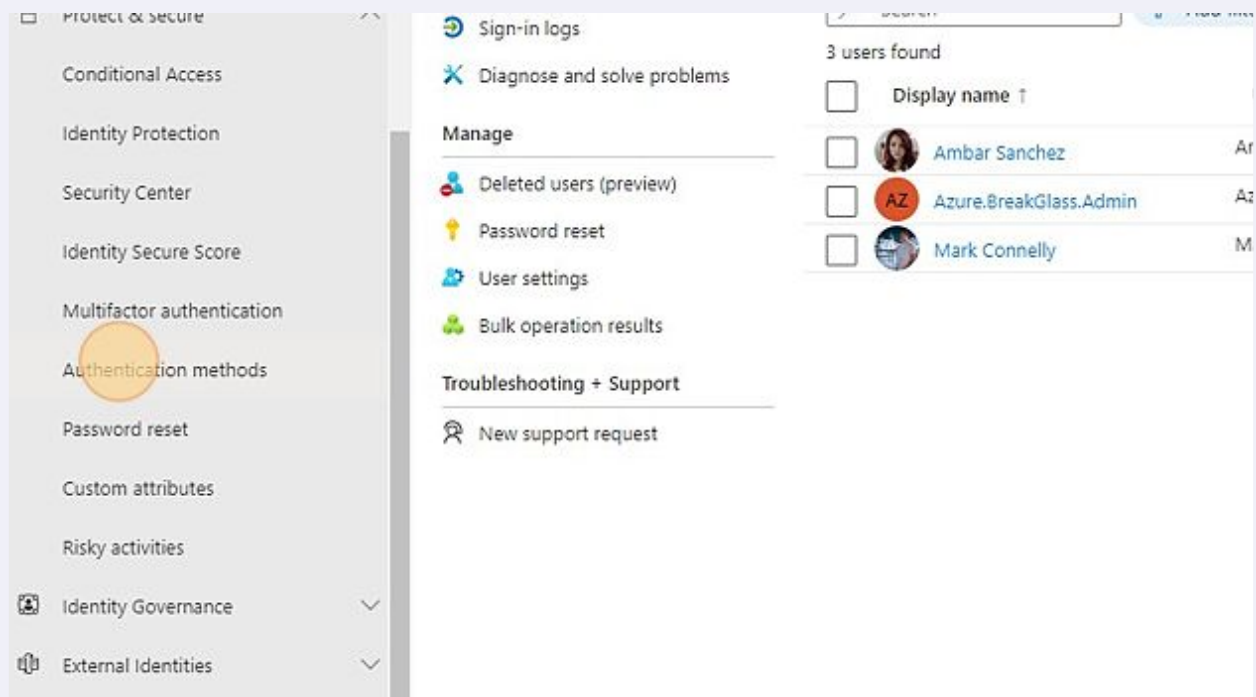
- 2 Click "Azure Active Directory"



3 Click "Protect & secure"



4 Click "Authentication methods"



5 Click "Microsoft Authenticator"

If your tenant doesn't yet use combined security info registration, turn it on now – it's

Manage migration

In January 2024, the legacy multifactor authentication methods policy. Use this control to manage your migration.

[Manage migration \(Preview\)](#)

Method	Target
FIDO2 security key	
Microsoft Authenticator	All users
SMS (preview)	
Temporary Access Pass	
Third-party software OATH tokens (preview)	
Voice call (preview)	
Email OTP (preview)	
Certificate-based authentication	

6 Click "Enable"

Microsoft Authenticator settings

Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting on 1/1/2024.

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or combined security info registration.

Enable and Target

Enable ☒

Include **Exclude**

Target ☒ All users ☐ Select groups

Name	Type
All users	Group

7 Target "All users"

Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting on 10/1/2023.

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or as a second factor.

Enable and Target | Configure

Enable ☒

Include | Exclude

Target ☒ All users ☐ Select groups

Name	Type
All users	Group

8 Click "Exclude" to switch to the exclusion tab.

Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting on 10/1/2023.

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or as a second factor.

Enable and Target | Configure

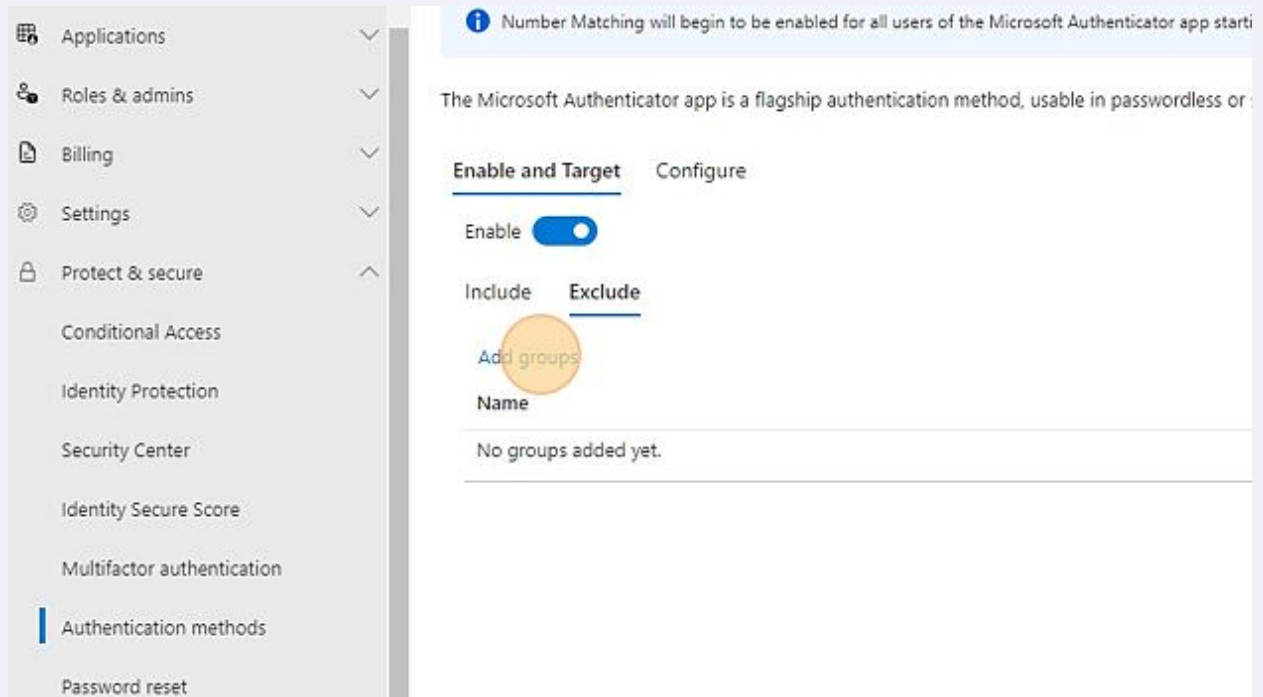
Enable ☒

Include | **Exclude**

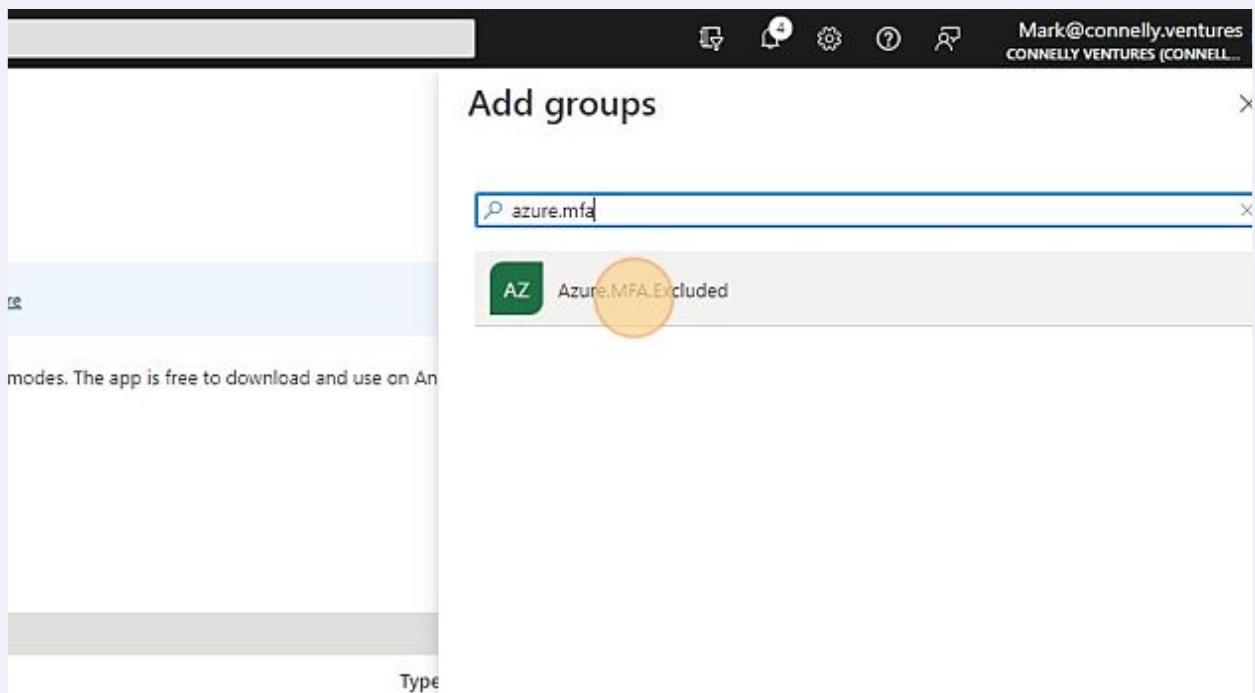
Target ☒ All users ☐ Select groups

Name	Type
All users	Group

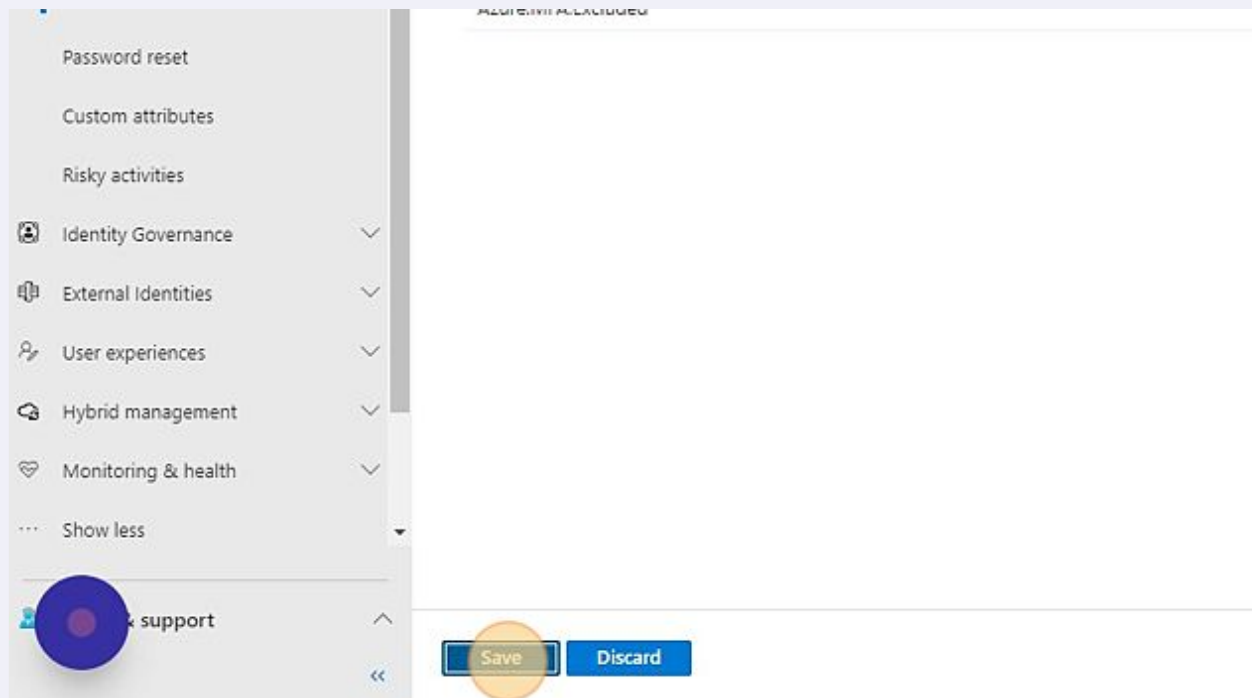
9 Click "Add groups"



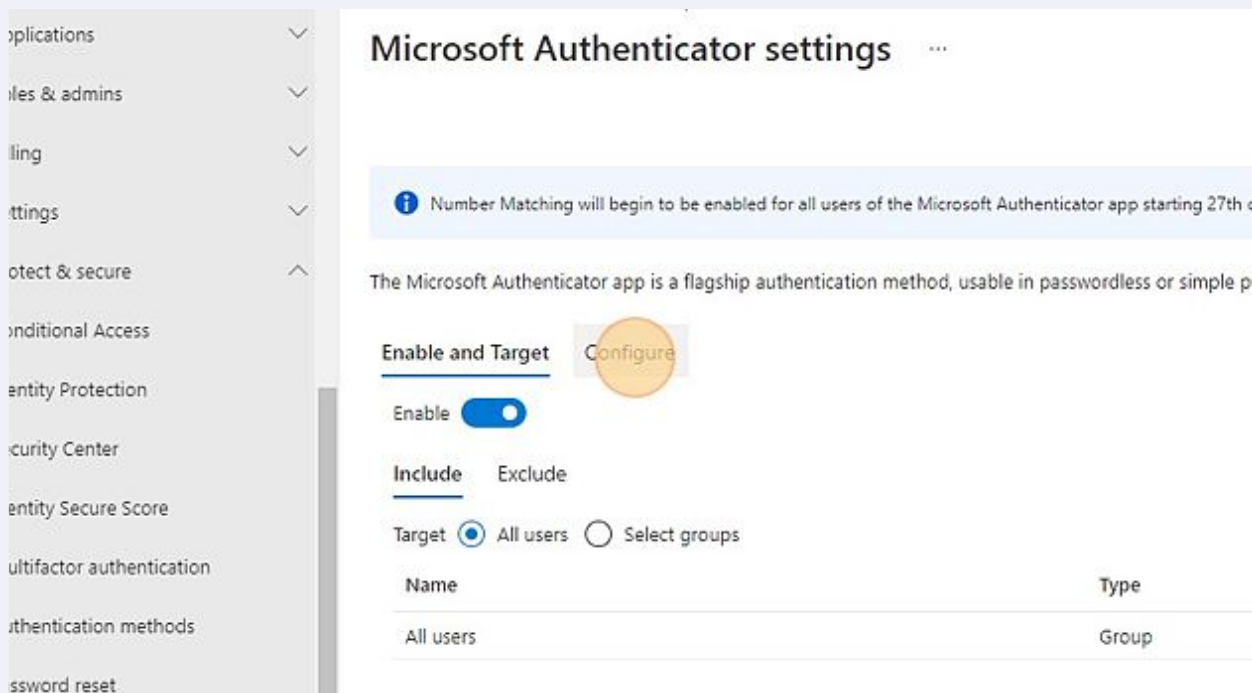
10 Click "Azure.MFA.Excluded"



11 Click "Save"



12 Click "Configure"



13 Set "Require number matching for push notifications" to "Enabled"

Note: Users must be included as part of the Microsoft Authenticator targeted groups under the policy.

GENERAL

Allow use of Microsoft Authenticator OTP ☐ Yes ☒ No

Require number matching for push notifications

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time.

Status

Target

Show application name in push and passwordless notifications

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time.

Status

Target

☒ All users

14 Set "Show application name in push and passwordless notifications" to "Enabled"

☒ All users
☐ Select group

Show application name in push and passwordless notifications

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time.

Status

Target

Show geographic location in push and passwordless notifications

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time.

Status

Target

☒ All users

15 Set "Show geographic location in push and passwordless notifications" to "Enabled"

The screenshot shows the Microsoft Entra ID console. On the left is a navigation pane with a search bar and a list of categories: Password reset, Custom attributes, Risky activities, Identity Governance, External Identities, User experiences, Hybrid management, Monitoring & health, and Show less. A blue circle highlights the 'Support' link at the bottom of the navigation pane. The main content area is titled 'Target' with tabs for 'Include' and 'Exclude'. Under the 'Include' tab, there are two radio buttons: 'All users' (selected) and 'Select group'. Below this is a section titled 'Show geographic location in push and passwordless notifications' with a note: 'Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time.' There are two dropdown menus: 'Status' and 'Target'. The 'Status' dropdown is currently set to 'Microsoft managed' and is highlighted with a blue circle. The 'Target' dropdown is currently set to 'Microsoft managed' and is also highlighted with a blue circle. At the bottom of the main content area are two buttons: 'Save' and 'Discard'.

16 Click "Save"

This screenshot is identical to the one above, showing the same configuration page. However, in this step, a blue circle highlights the 'Save' button at the bottom of the main content area, indicating the final action to be taken.