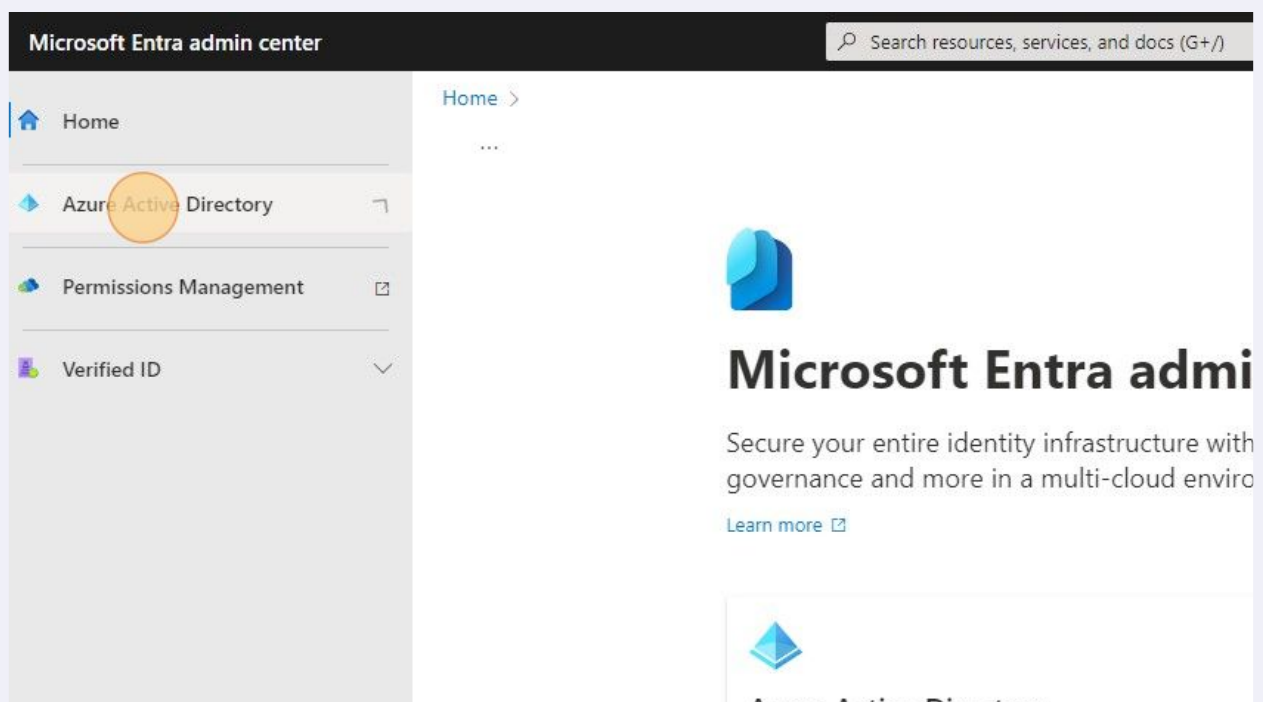


How to Configure Microsoft MFA Authentication Settings

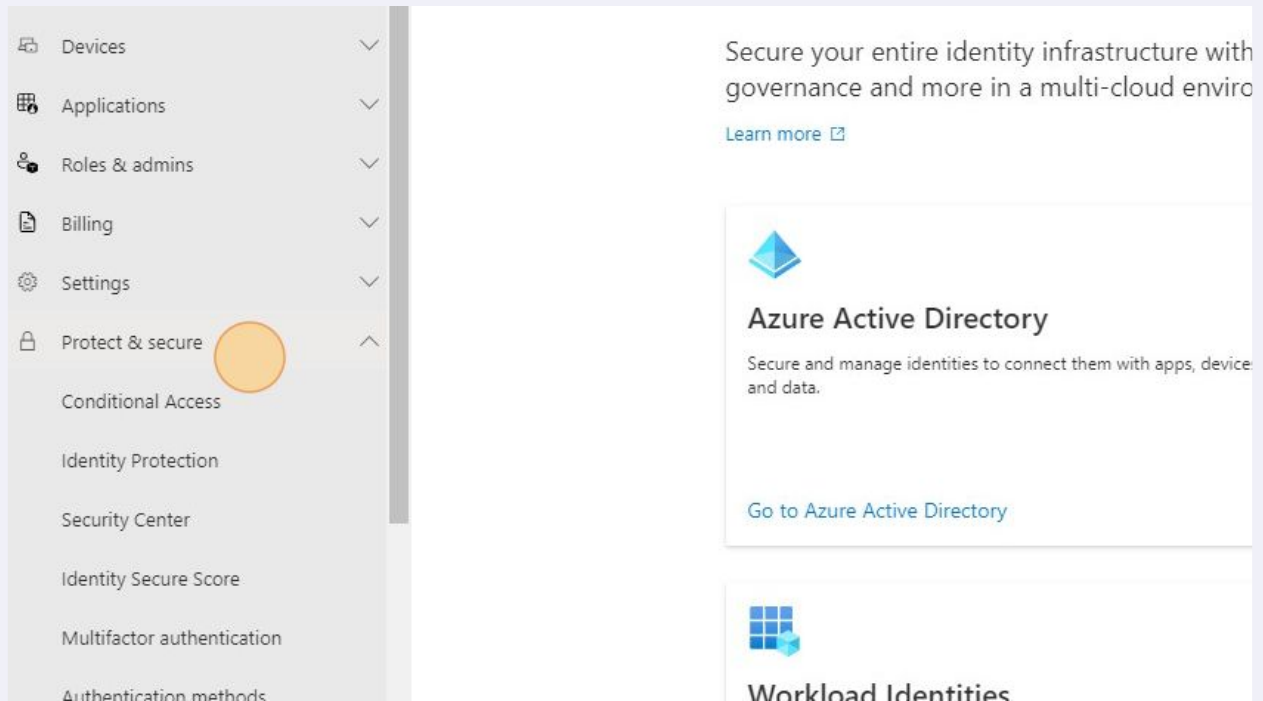
In this document, we cover how to configure the specific authentication settings available to us with the Microsoft MFA client.

- 1 Navigate to entra.microsoft.com

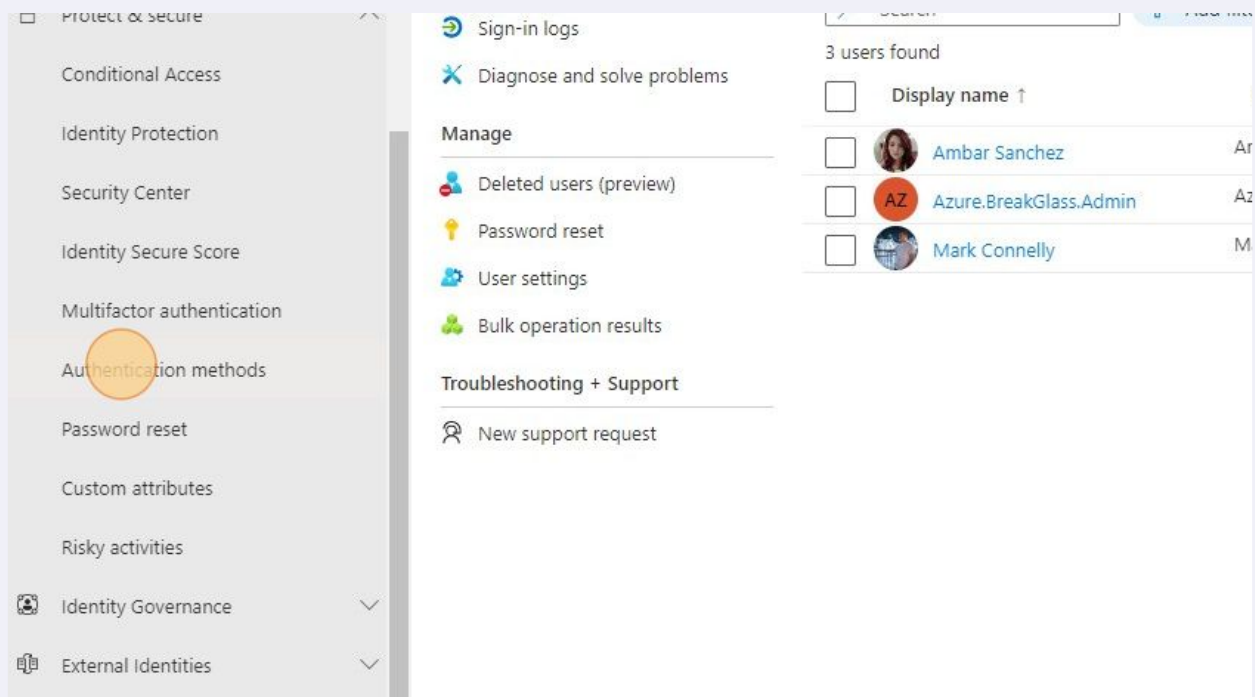
- 2 Click "Azure Active Directory"



3 Click "Protect & secure"



4 Click "Authentication methods"



5 Click "Microsoft Authenticator"

Password protection

Registration campaign

Authentication strengths (Preview)

Monitoring

- Activity
- User registration details
- Registration and reset events
- Bulk operation results

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 [Configure](#)

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 password-based authentication.

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 password-based authentication.

Enable and Target | Configure

Enable ☒

Exclude | Include

Target ☒ All users ☐ Select groups

Name	Type
All users	Group

9 Click "Add groups"

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 as a second factor.

Enable and Target Configure

Enable ☒

Include **Exclude**

[Add groups](#)

Name
No groups added yet.

10 Click "Microsoft Authenticator"

If your tenant doesn't yet use [combined security info registration](#), turn it on now – it's required for migration.

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	

11 Click "Exclude"

The screenshot shows the Microsoft Authenticator settings page. On the left, a navigation pane lists various settings categories. The 'Authentication methods' category is selected. The main content area displays the 'Enable and Target' section, which includes a toggle for 'Enable' (turned on), a tab for 'Exclude' (highlighted with an orange circle), and a 'Target' section with radio buttons for 'All users' (selected) and 'Select groups'. Below this is a table with columns 'Name' and 'Type'. The table contains one entry: 'All users' under 'Name' and 'Group' under 'Type'.

11 Click "Exclude"

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 password-based authentication.

Enable and Target Configure

Enable ☒

Include **Exclude**

Target ☒ All users ☐ Select groups

Name	Type
All users	Group

12 Click "Add groups"

The screenshot shows the Microsoft Authenticator settings page. On the left, a navigation pane lists various settings categories. The 'Authentication methods' category is selected. The main content area displays the 'Enable and Target' section, which includes a toggle for 'Enable' (turned on), a tab for 'Exclude' (selected), and an 'Add groups' button (highlighted with an orange circle). Below this is a table with columns 'Name' and 'Type'. The table contains one entry: 'No groups added yet.' under 'Name' and 'Group' under 'Type'.

12 Click "Add groups"

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 password-based authentication.

Enable and Target Configure

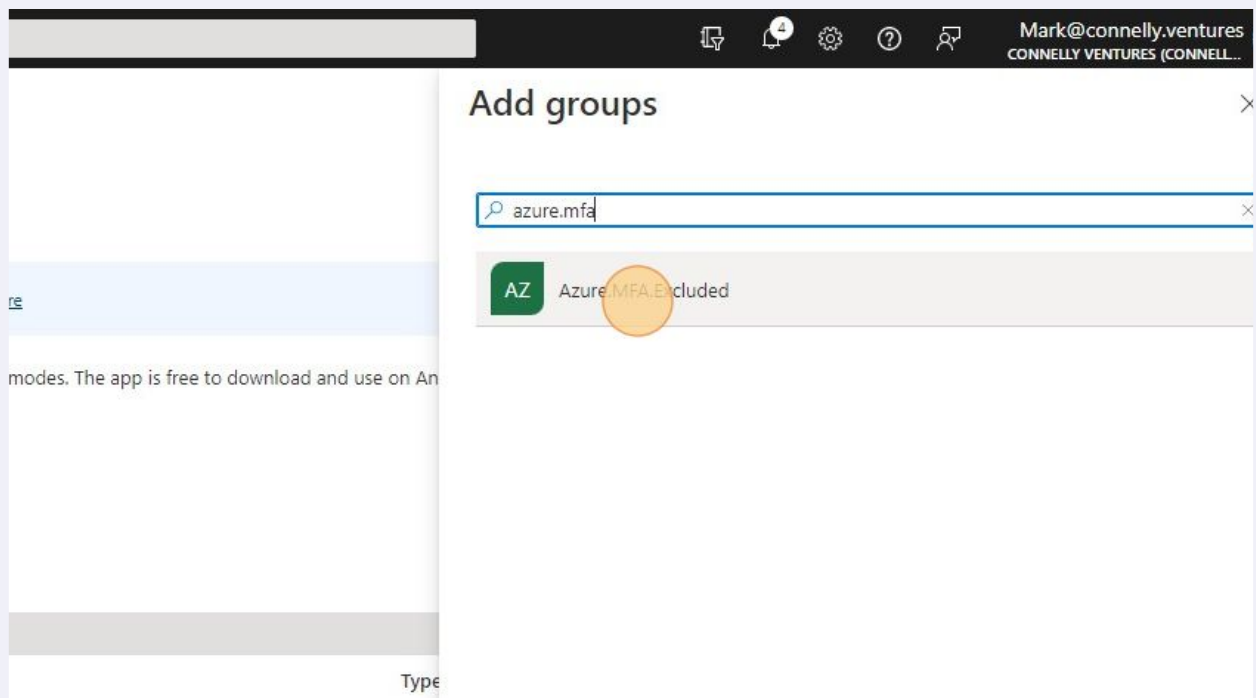
Enable ☒

Include **Exclude**

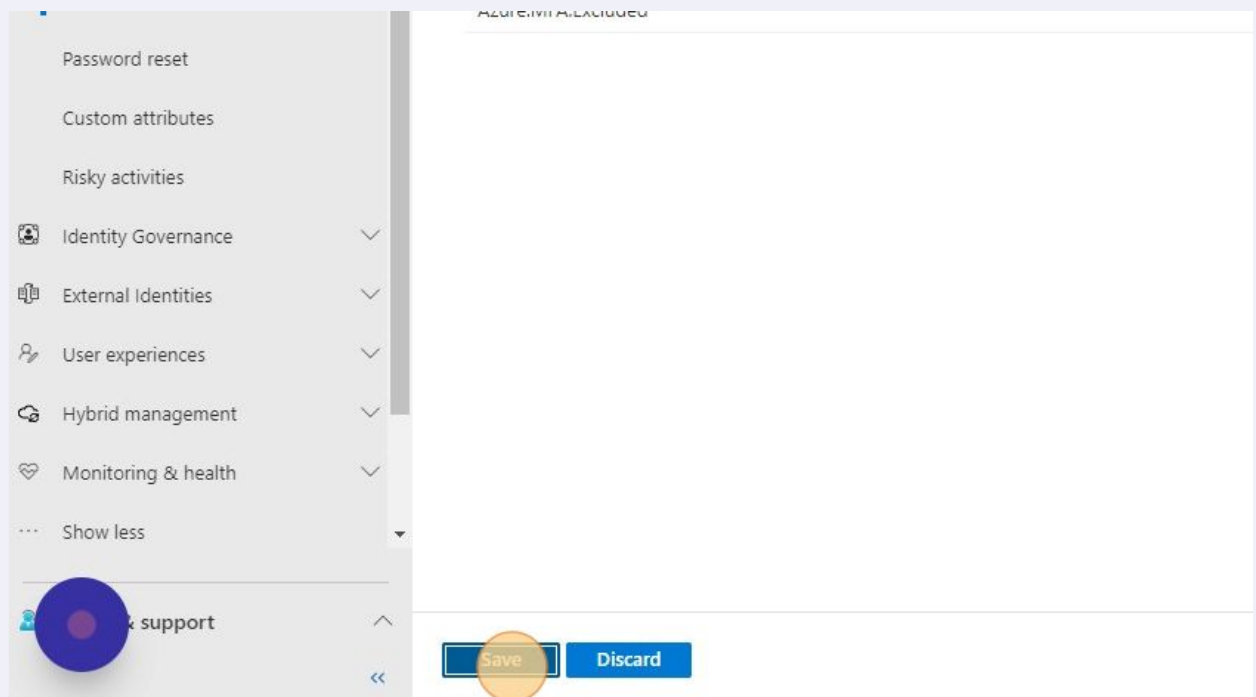
Add groups

Name	Type
No groups added yet.	Group

13 Click "Azure.MFA.Excluded"



14 Click "Save"



15 Click "Configure"

Applications

Users & admins

Settings

Protect & secure

Conditional Access

Identity Protection

Security Center

Identity Secure Score

Multifactor authentication

Authentication methods

Password reset

Microsoft Authenticator settings

Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting 27th c

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple p

Enable and Target **Configure**

Enable ☒

Include Exclude

Target ☒ All users ☐ Select groups

Name	Type
All users	Group

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

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

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 approp

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 approp

Status

Target ☒ All users

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

The screenshot shows the Microsoft Entra ID console with the left-hand navigation pane. The 'Authentication methods' section is expanded, and the 'Show application name in push and passwordless notifications' feature is selected. The feature status is set to 'Microsoft managed'. The 'Target' dropdown menu is open, showing 'Microsoft managed', 'Enabled', and 'Disabled'. The 'Enabled' option is highlighted with an orange circle. The 'Target' is set to 'All users'.

Security Center

Identity Secure Score

Multifactor authentication

Authentication methods

Password reset

Custom attributes

Risky activities

Identity Governance

External Identities

User experiences

Hybrid management

Monitoring & health

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: Microsoft managed ⓘ

Target: Microsoft managed ⓘ

Enabled

Disabled

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: Microsoft managed ⓘ

Target: Include Exclude

All users

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

The screenshot shows the Microsoft Entra ID console with the left-hand navigation pane. The 'Monitoring & health' section is expanded, and the 'Show geographic location in push and passwordless notifications' feature is selected. The feature status is set to 'Microsoft managed'. The 'Target' dropdown menu is open, showing 'Microsoft managed', 'Enabled', and 'Disabled'. The 'Enabled' option is highlighted with an orange circle. The 'Target' is set to 'All users'. The 'Save' and 'Discard' buttons are visible at the bottom.

Password reset

Custom attributes

Risky activities

Identity Governance

External Identities

User experiences

Hybrid management

Monitoring & health

Show less

Support

Target: Include Exclude

All users

Select group

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: Microsoft managed ⓘ

Target: Microsoft managed ⓘ

Enabled

Disabled

Save Discard

19 Click "Save"

Left sidebar navigation:

- Password reset
- Custom attributes
- Risky activities
- Identity Governance
- External Identities
- User experiences
- Hybrid management
- Monitoring & health
- Show less
- Help & support

Target settings:

Target: **Include** Exclude

☒ All users
☐ Select group

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 ap

Status: **Enabled**

Target: **Include** Exclude

☒ All users
☐ Select group

Buttons: **Save** **Discard**