
Azure MFA
Jan Bakker

Microsoft® Most Valuable Professional

AKA.MS/JANBAKKER

SCAN ME

DUTCH MICROSOFT SECURITY MEETUP

Why this session?

MAKING AN INDICATOR FROM RED CABBAGE

The compounds that give red cabbage its colour can be extracted and used as a pH indicator solution. Here we look at the method and the colours!

MAKING THE INDICATOR

1. ROUGHLY CHOP THE CABBAGE

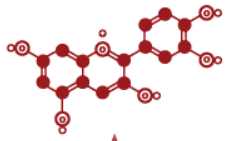
2. BOIL FOR A FEW MINUTES

3. STRAIN AND LET COOL

4. USE AS AN INDICATOR!

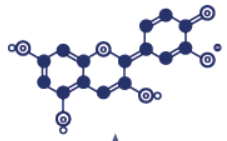
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14

ACIDIC — pH — ALKALINE

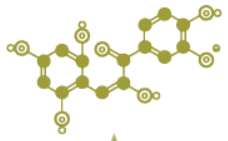


RED (pH <3)

VIOLET (pH 4–7)



BLUE (pH 7–8)



YELLOW GREEN (AT pH >8)

Hydrogens on carbon atoms implied; each carbon has 4 bonds.

The red cabbage extract can be used to determine whether substances are acidic or alkaline. The structures of the anthocyanin pigments which give the red cabbage its colour are subtly changed at varying pH. These different structures give a range of colours.

So, what does it cost?

Free for:

Azure AD Free
Office 365 (all versions)
Azure AD Premium P1
Azure AD Premium P2

What are you waiting for?

What are the options?

Security Defaults

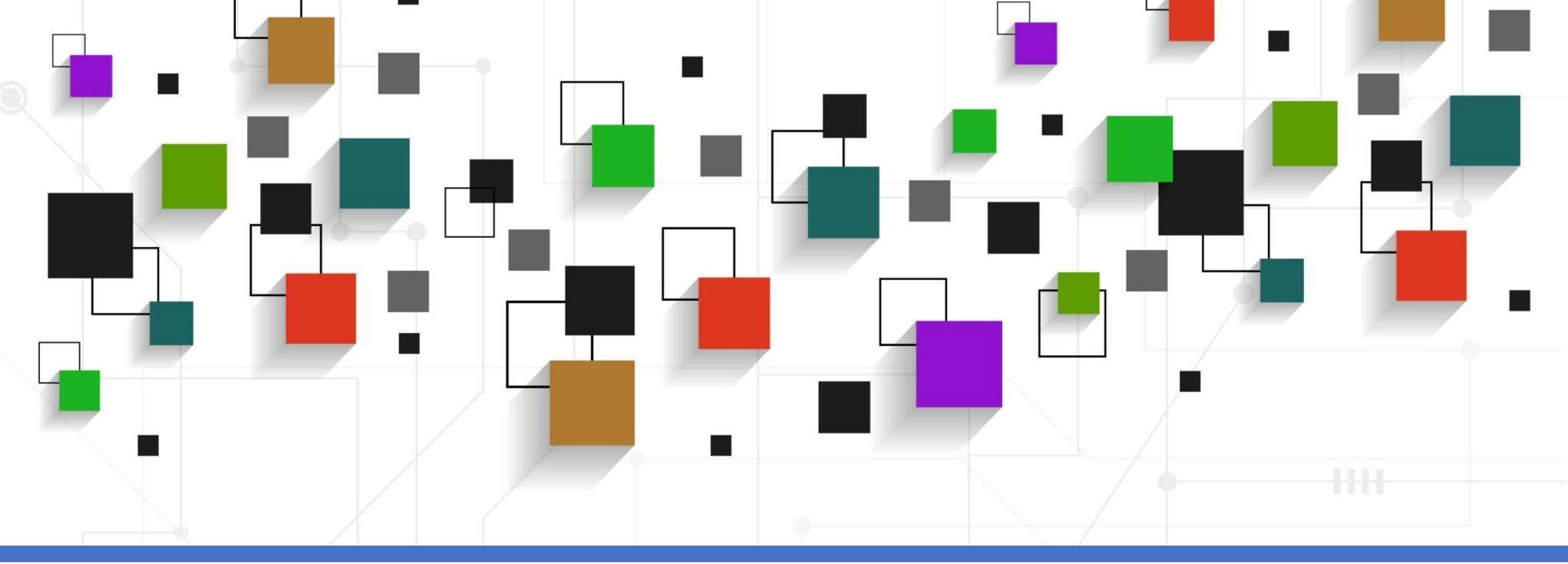
Per-user MFA

Conditional Access

Identity Protection

Conditional Access
+
Identity Protection

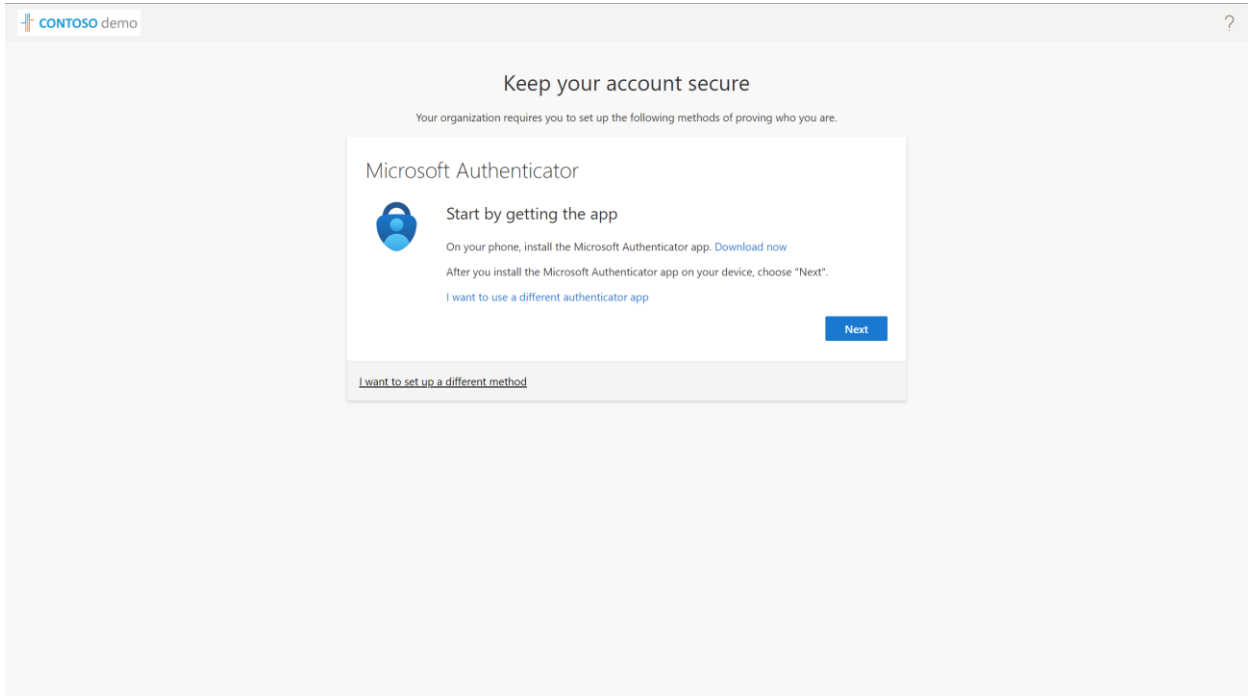
Privileged Identity Management

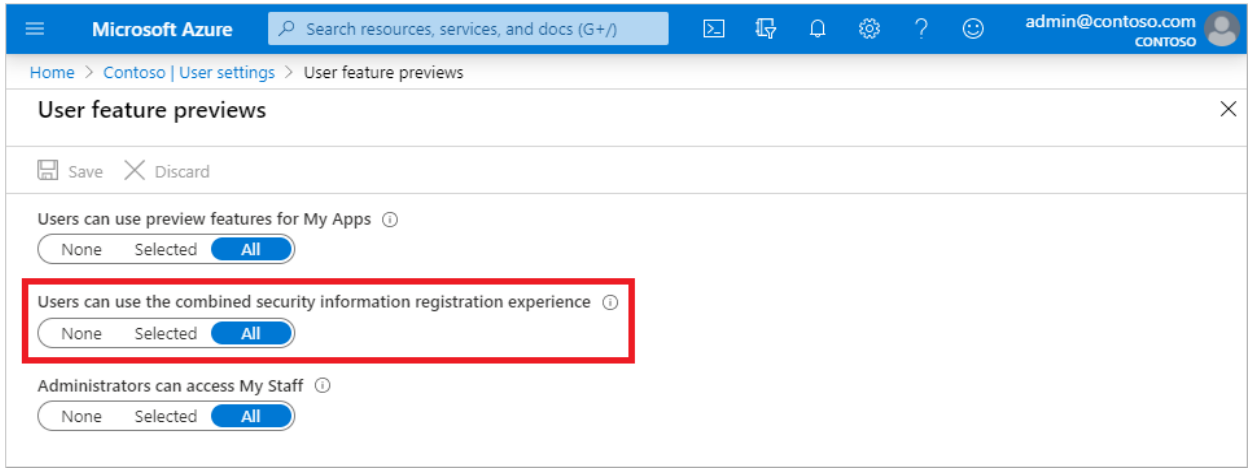


Enrollment

First things first

(I want to get rid of this slide)





Self Enrollment (manual)

aka.ms/mfasetup

aka.ms/setupsecurityinfo

multi-factor authentication

users service settings

Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users | Multi-Factor Auth status: Any | bulk update

DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
Adele Vance	AdeleV@M365x341716.OnMicrosoft.com	Disabled
Alex Wilber	AlexW@M365x341716.OnMicrosoft.com	Disabled
Allan Deyoung		
Automate Bot		
Bianca Pisani		
Brian Johnson (TA		
Cameron White		
Christian Horner		
Christie Cline		
Conf Room Adam		
Conf Room Baker	Baker@M365x341716.OnMicrosoft.com	Disabled
Conf Room Crystal	Crystal@M365x341716.OnMicrosoft.com	Disabled

Adele Vance

AdeleV@M365x341716.OnMicros
205 108th Ave. NE, Suite 400
T ANYTHING HERE

eps

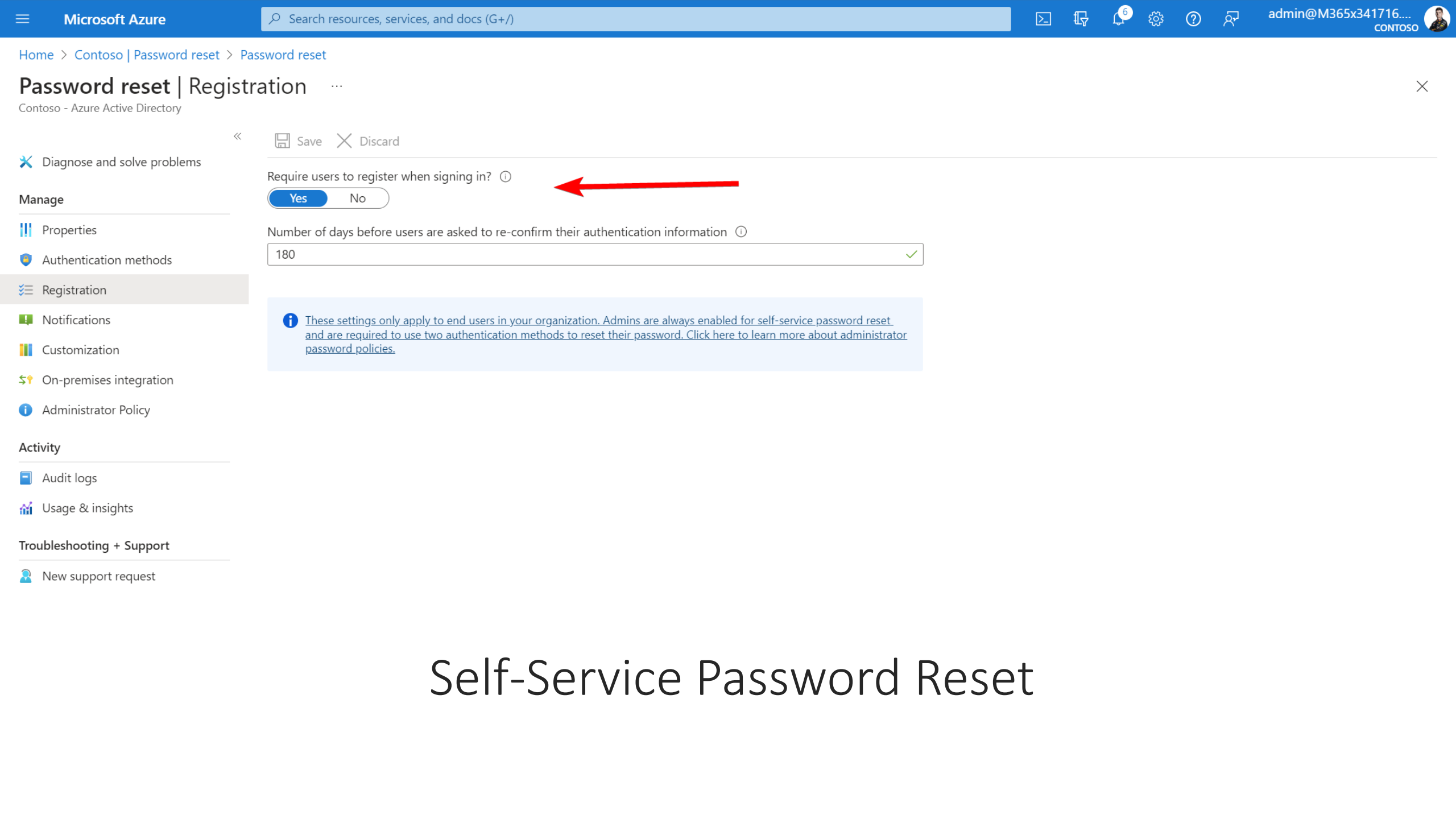
settings

About enabling multi-factor auth

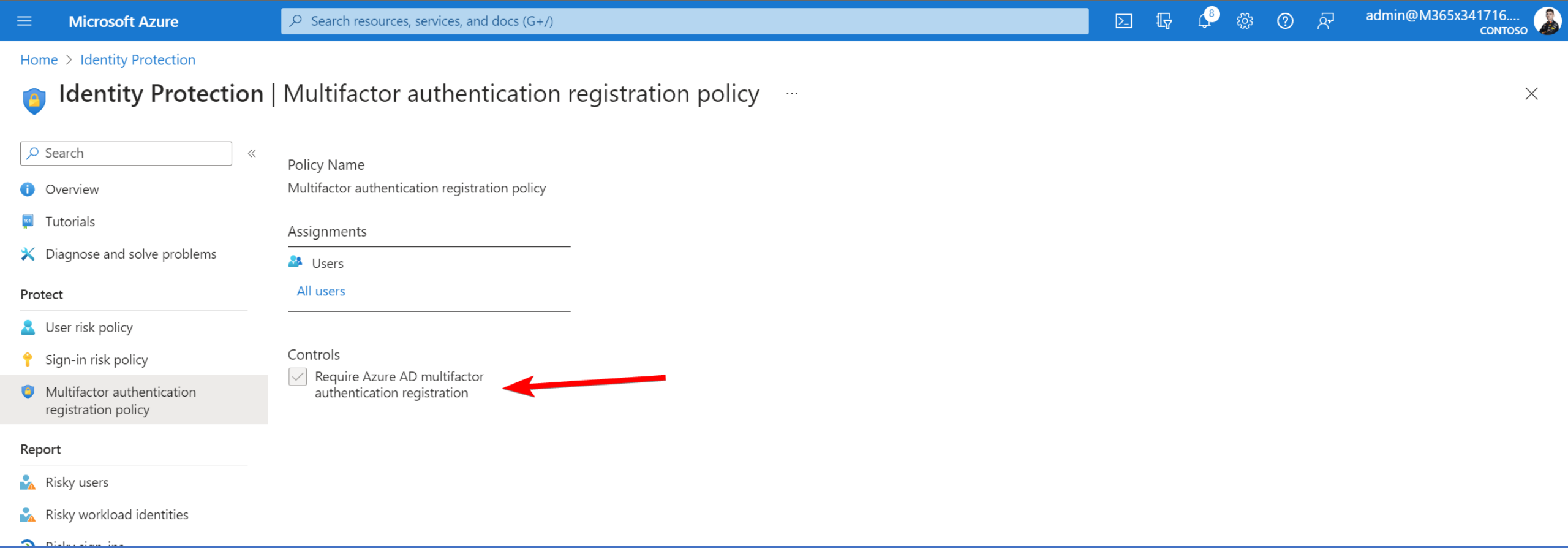
Please read the deployment guide if you haven't already.

If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: https://aka.ms/MFASetup

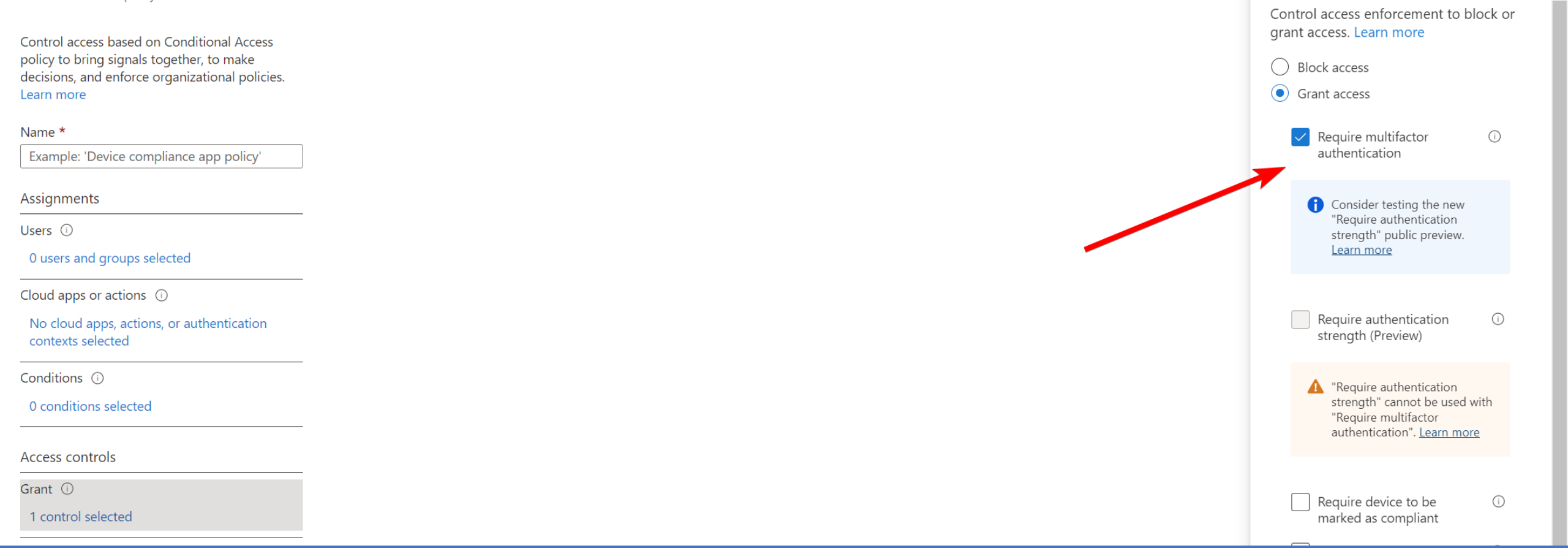
enable multi-factor auth | cancel



Self-Service Password Reset



Identity Protection



Conditional Access

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users

0 users and groups selected

Cloud apps or actions

1 user action included

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Session

Control access based on all or specific cloud apps or actions. Learn more

Select what this policy applies to

User actions

Select the action this policy will apply to

- [x] Register security information
- [ ] Register or join devices

Enable policy

Secure registration process

Secure MFA registration

Require known location
Require known device
Block specific regions
Require MFA

Require MFA for MFA registration?

Temporary Access Pass

Temporary Access Pass Manager

JANBAKKER.TECH
sharing is caring

Search User | Adele Vance | Clear

Create Temporary Access Pass

List/Get Temporary Access Pass

Delete Temporary Access Pass

Send Temporary Access Pass to mobile phone

Temporary Access Pass **A&Unj$#m**

ID	aa77cce2-98ca-420d-add5-488573a3dd01
Lifetime (minutes)	60
is Usable	true
is Usable Once	false
Created	Monday, August 9, 2021 10:10:40
Usability	EnabledByPolicy

+31643941043

AdeleV@M365x583104.OnMicrosoft.com

Bellevue

Method	Primary authentication	Secondary authentication
Windows Hello for Business	Yes	MFA*
Microsoft Authenticator app	Yes	MFA and SSPR
FIDO2 security key	Yes	MFA
Certificate-based authentication (preview)	Yes	No
OATH hardware tokens (preview)	No	MFA and SSPR
OATH software tokens	No	MFA and SSPR
SMS	Yes	MFA and SSPR
Voice call	No	MFA and SSPR
Password	Yes	

trusted ips (learn more)

- [ ] Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

192.168.1.0/27
192.168.1.0/27
192.168.1.0/27

verification options (learn more)

Methods available to users:

- [ ] Call to phone
- [ ] Text message to phone
- [ ] Notification through mobile app
- [ ] Verification code from mobile app or hardware token

remember multi-factor authentication on trusted device (learn more)

- [ ] Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)

Number of days users can trust devices for 90

NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes
risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,'
more days. Learn more about reauthentication prompts.

trusted ips (learn more)

Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

192.168.1.0/27
192.168.1.0/27
192.168.1.0/27

ve n options

Methods
Call to p
Text mes e
Notif ile app
V code fr app or hardware token

mber multi-factor tication on trusted device (learn more)

Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)

Number of days users can trust devices for 90

NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' more days. Learn more about reauthentication prompts.

Authentication methods | Policies

Contoso - Azure AD Security

Search

Got feedback?

Manage

- Policies
- Password protection
- Registration campaign
- Authentication strengths (Preview)
- Settings

Monitoring

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

Use this policy to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). Learn more

If your tenant doesn't yet use combined security info registration, turn it on now – it's required to use this policy.

Manage migration (Preview)

In January 2024, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy policies to the new unified policy. Learn more

Manage migration (Preview)

Method	Target	Enabled
FIDO2 security key	All users	Yes
Microsoft Authenticator	All users	Yes
SMS (Preview)	All users	Yes
Temporary Access Pass	All users	Yes
Third-party software OATH tokens (Preview)	All users	Yes
Voice call (Preview)		No
Email OTP (Preview)		No
Certificate-based authentication		No

Authentication methods policies

Irvin Sayers | Authentication methods

User

Search
Overview
Audit logs
Sign-in logs
Diagnose and solve problems

Manage
Custom security attributes (preview)
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods

Troubleshooting + Support
New support request

Add authentication method | Reset password | Require re-register multifactor authentication | Revoke multifactor authentication sessions | Got feedback?

Want to switch back to the old user authentication methods experience? Click here to go back. →

Authentication methods are the ways your users sign into Azure AD and perform SSPR.

Usable authentication methods

Authentication method	Detail
Phone number	Primary mobile: +31 649158615
FIDO2 security key	My FIDO key
Microsoft Authenticator	iPhone 13 Pro

Non-usable authentication methods

Authentication method	Detail
No non-usable methods.	

Manage migration

In January 2024, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy policies to the new unified policy.

Learn more

- ( ) Pre-migration:

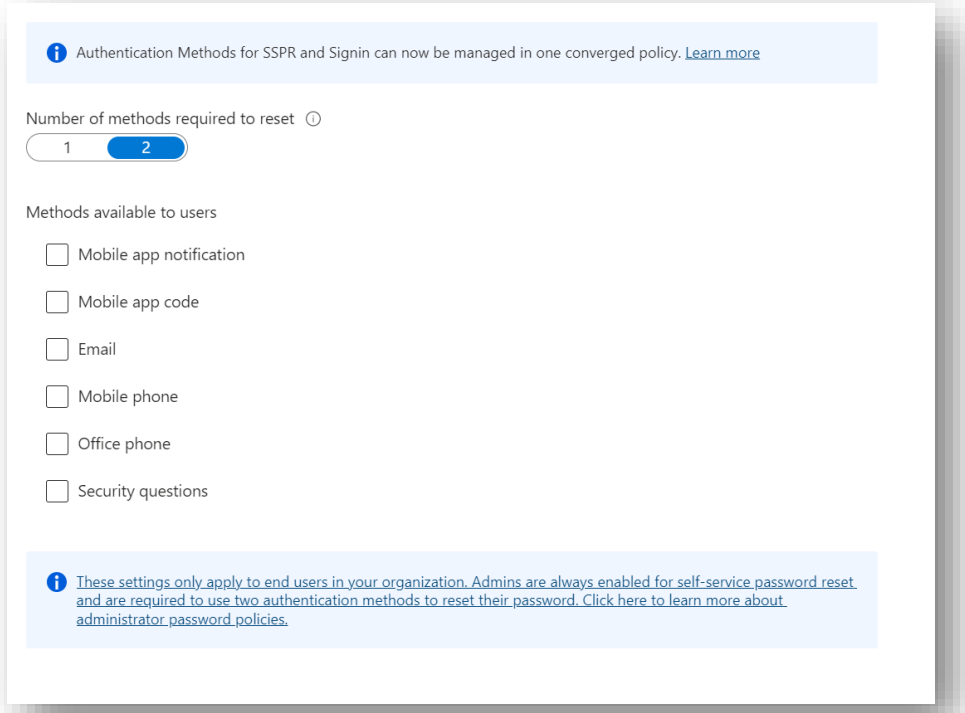
  Use policy for authentication only, respect legacy policies.

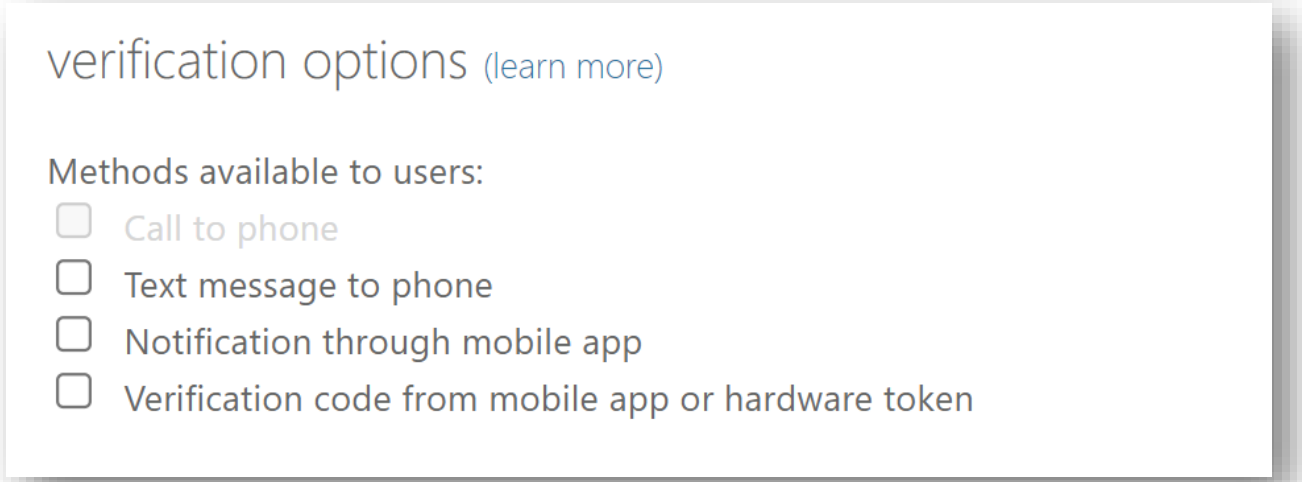
- (•) Migration In Progress:

  Use policy for authentication and SSPR, respect legacy policies.

- ( ) Migration Complete:

  Use policy for authentication and SSPR, ignore legacy policies.





[Goodbye legacy SSPR and MFA settings. Hello Authentication Methods Policies! - JanBakker.tech]

Manage migration (Preview)

In January 2024, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy policies to the new unified policy. Learn more

Manage migration (Preview)

Method	Target	Enabled
FIDO2 security key	All users	Yes
Microsoft Authenticator	All users	Yes
SMS (Preview)	All users	Yes
Temporary Access Pass	All users	Yes
Third-party software OATH tokens (Preview)	All users	Yes
Voice call (Preview)		No
Email OTP (Preview)		No
Certificate-based authentication		No

[Goodbye legacy SSPR and MFA settings. Hello Authentication Methods Policies! - JanBakker.tech]

How to handle previous registrations?

Authentication methods | Registration campaign

Contoso - Azure AD Security

Search

Manage

- Policies
- Password protection
- Registration campaign
- Authentication strengths (Preview)
- Settings

Monitoring

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

Got feedback?

Start a registration campaign that prompts users to set up more secure authentication methods.
Exclude users and groups from the entire campaign in the Settings section or include users and groups for each authentication method (currently limited to Microsoft Authenticator).
Learn more

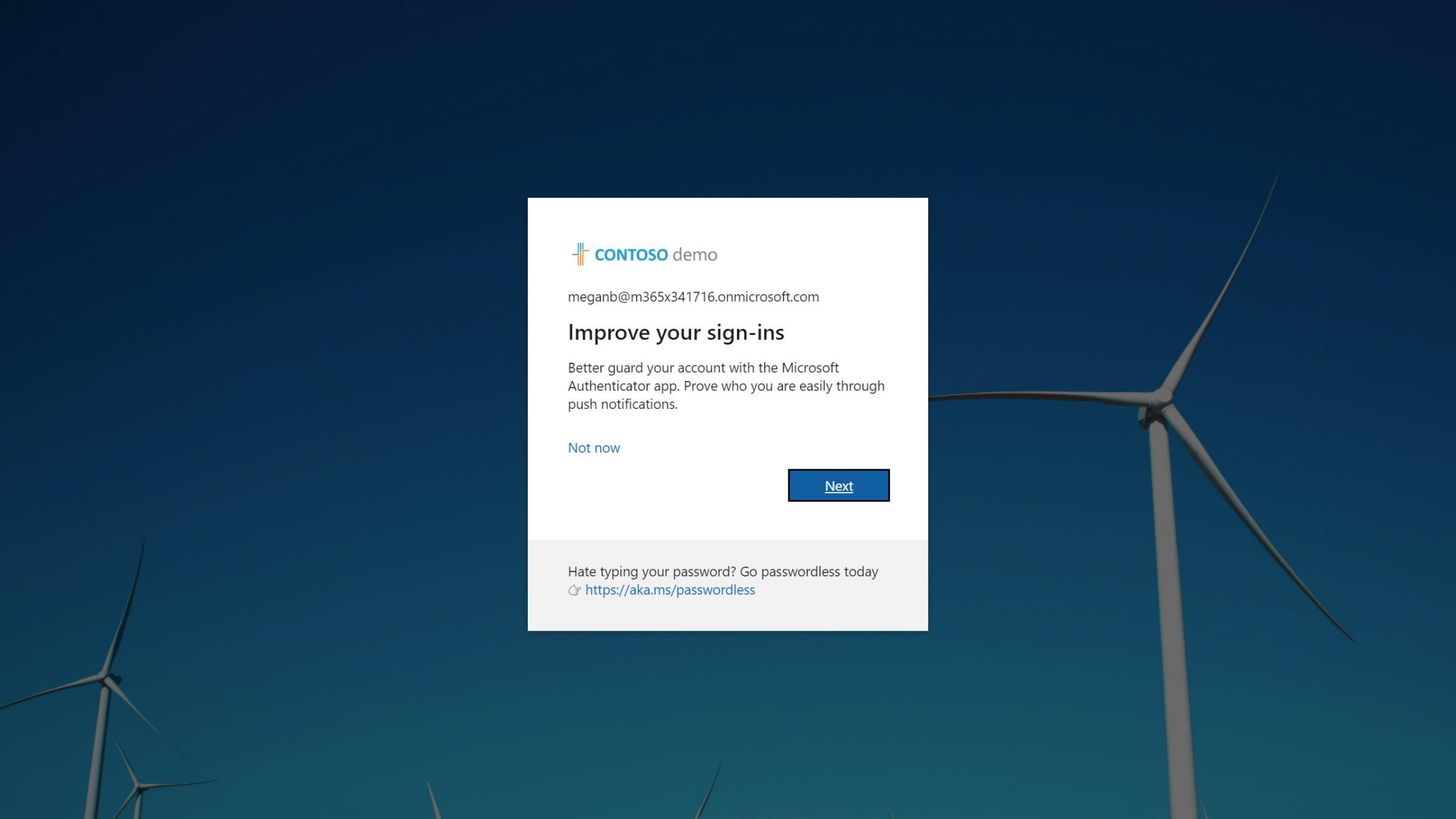
Settings Edit Discard

State	Enabled
Days allowed to snooze	1 day
Excluded users and groups	None selected
	Add users and groups

Authentication method

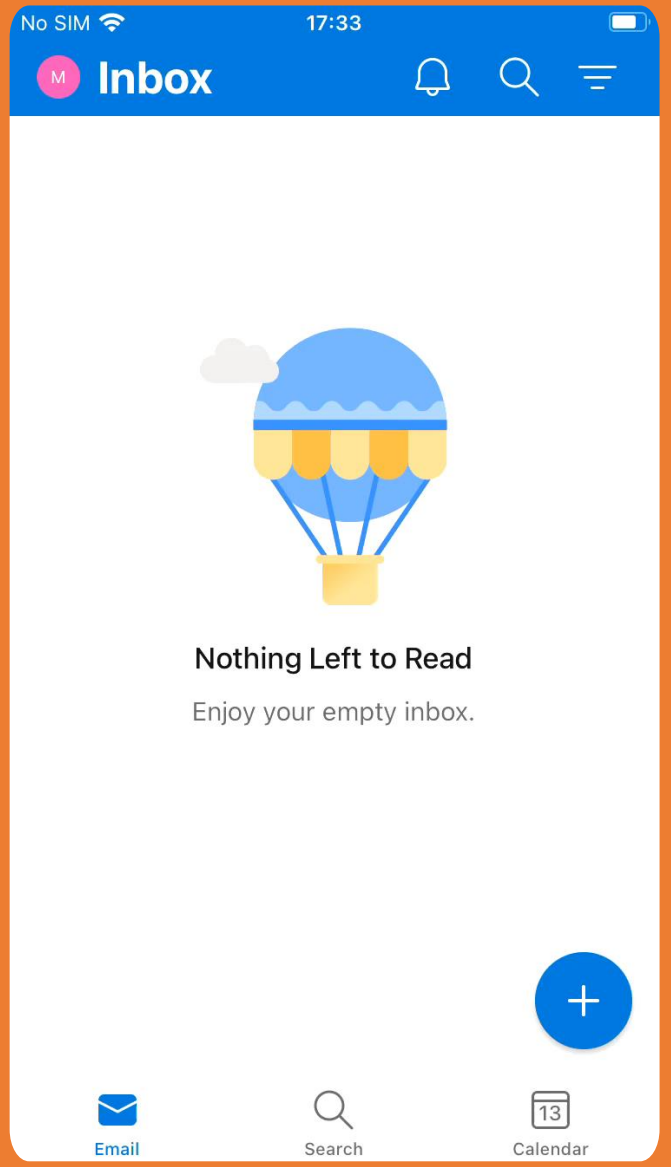
Method	Included users and groups
Microsoft Authenticator	All users

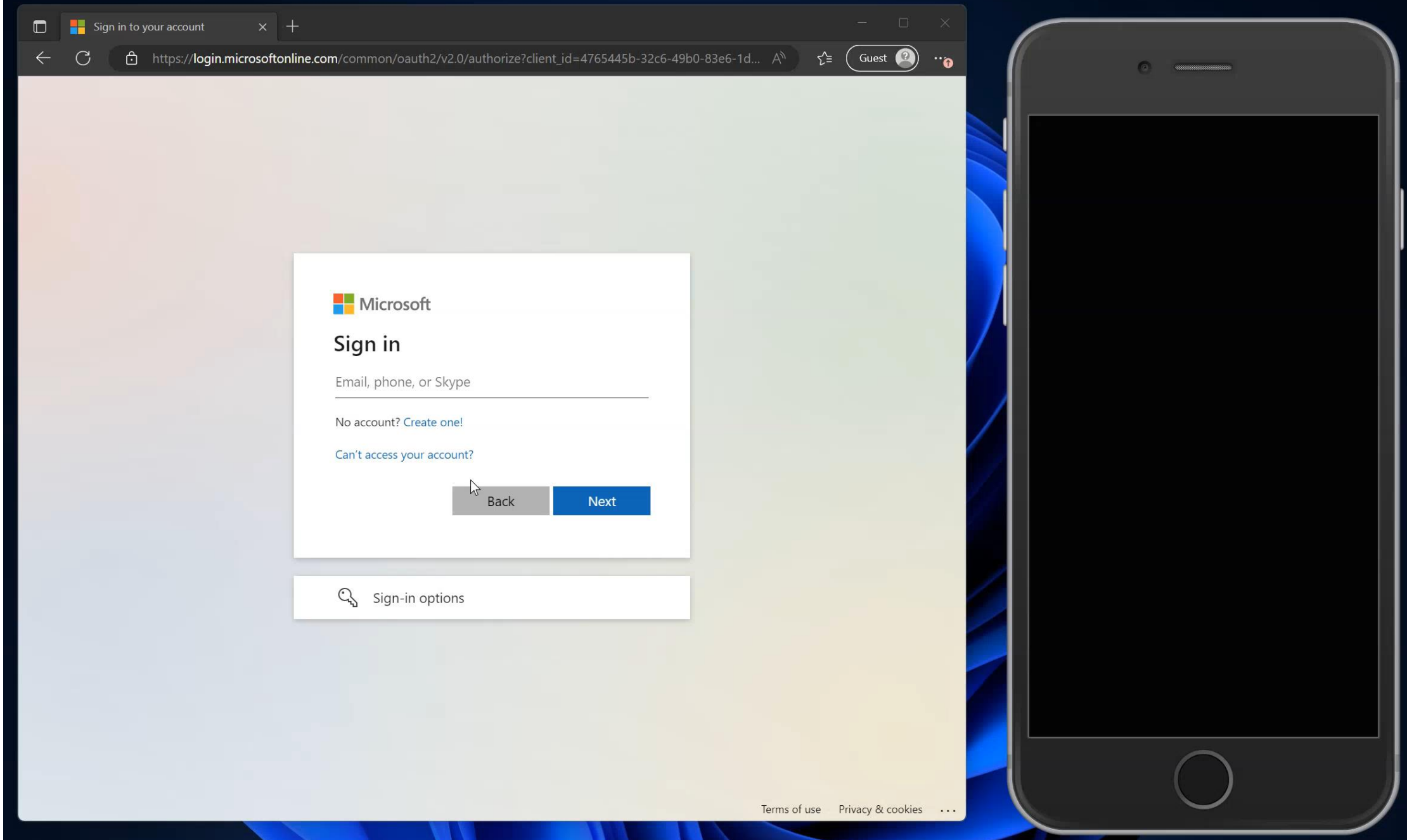
Registration campaign (Nudge)


CONTOSO demo
meganb@m365x341716.onmicrosoft.com
Improve your sign-ins
Better guard your account with the Microsoft Authenticator app. Prove who you are easily through push notifications.
Not now
Next
Hate typing your password? Go passwordless today
https://aka.ms/passwordless

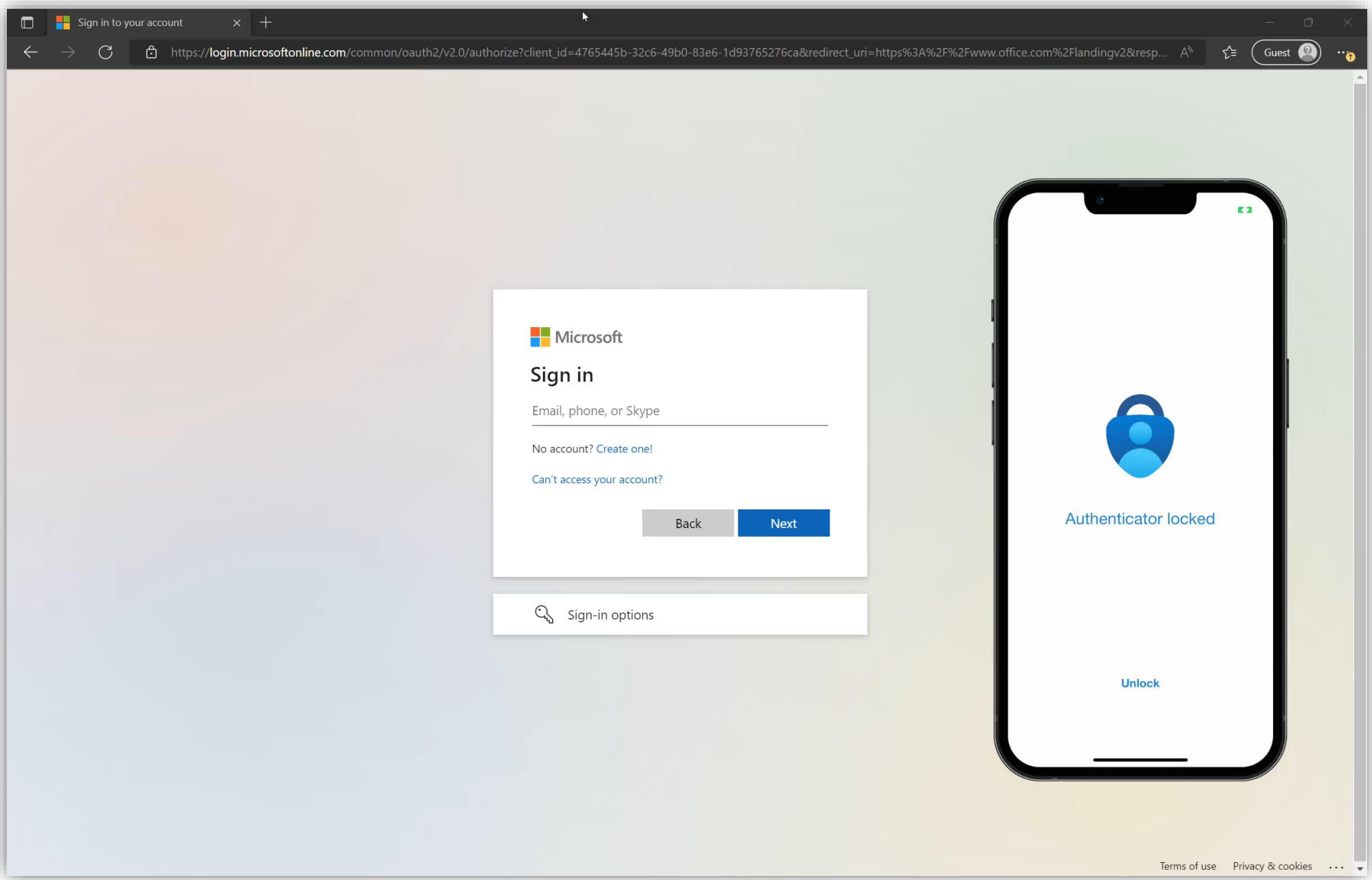

NO!

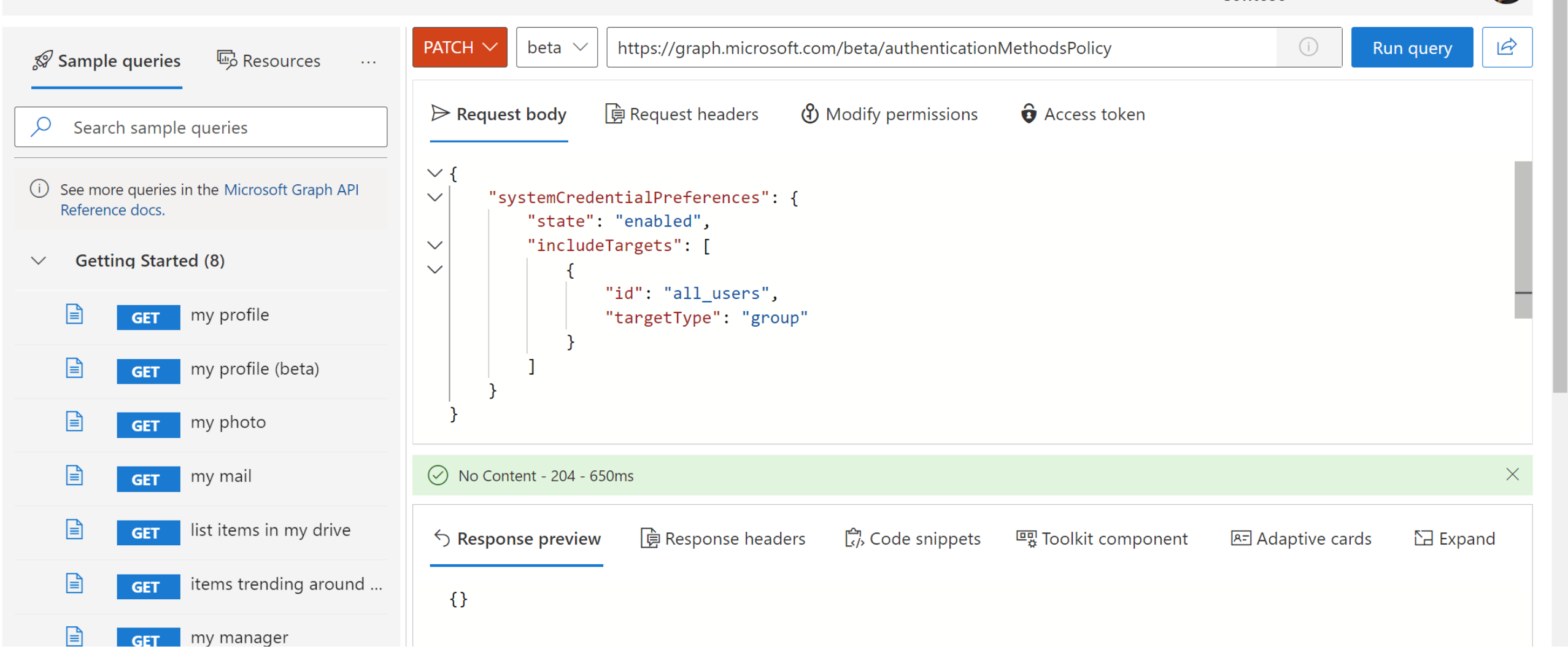
Authenticator Lite enrollment with TAP




Sign in to your account
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d...
Guest
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Back
Next
Sign-in options
Terms of use
Privacy & cookies

Microsoft Authenticator App features

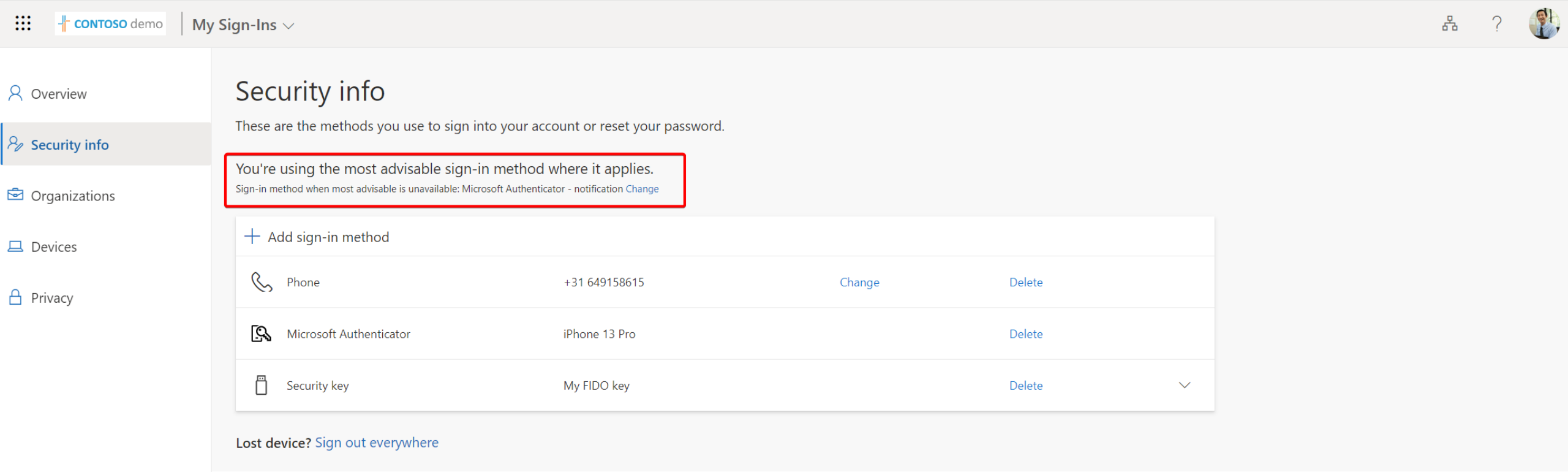

Sign in to your account
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fwww.office.com%2Flandingv2&resp...
Guest
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Back
Next
Sign-in options
Authenticator locked
Unlock
Terms of use
Privacy & cookies



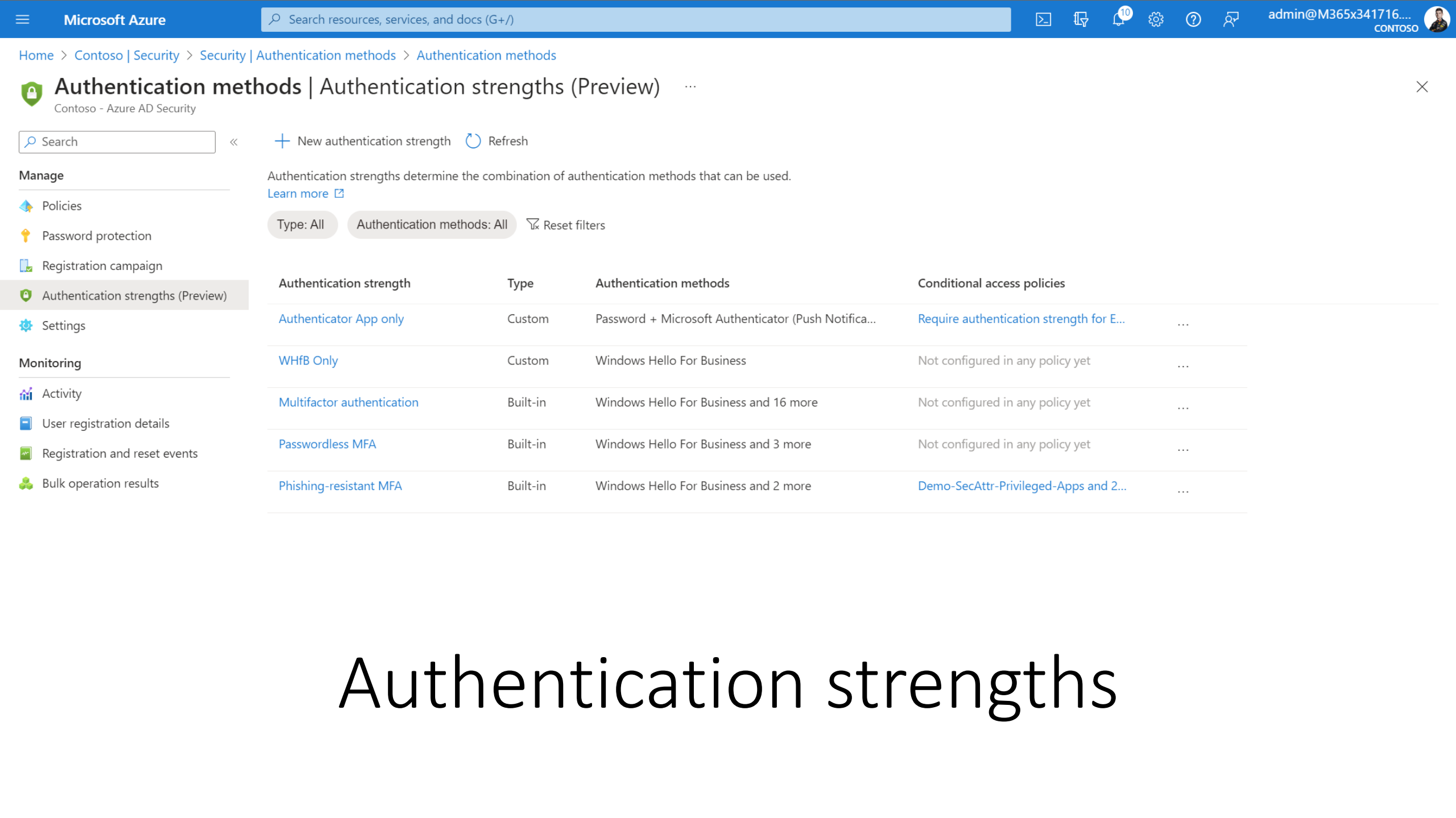
System preferred method

1. Temporary Access Pass
2. Certificate-based authentication
3. FIDO2 security key
4. Microsoft Authenticator notification
5. Companion app notification
6. Microsoft Authenticator time-based one-time password (TOTP)
7. Companion app TOTP
8. Hardware token based TOTP
9. Software token based TOTP
10. SMS over mobile
11. OnewayVoiceMobileOTP
12. OnewayVoiceAlternateMobileOTP
13. OnewayVoiceOfficeOTP
14. TwowayVoiceMobile
15. TwowayVoiceAlternateMobile
16. TwowayVoiceOffice
17. TwowaySMSOverMobile

The user is prompted to sign-in with the most secure method according to the following order.



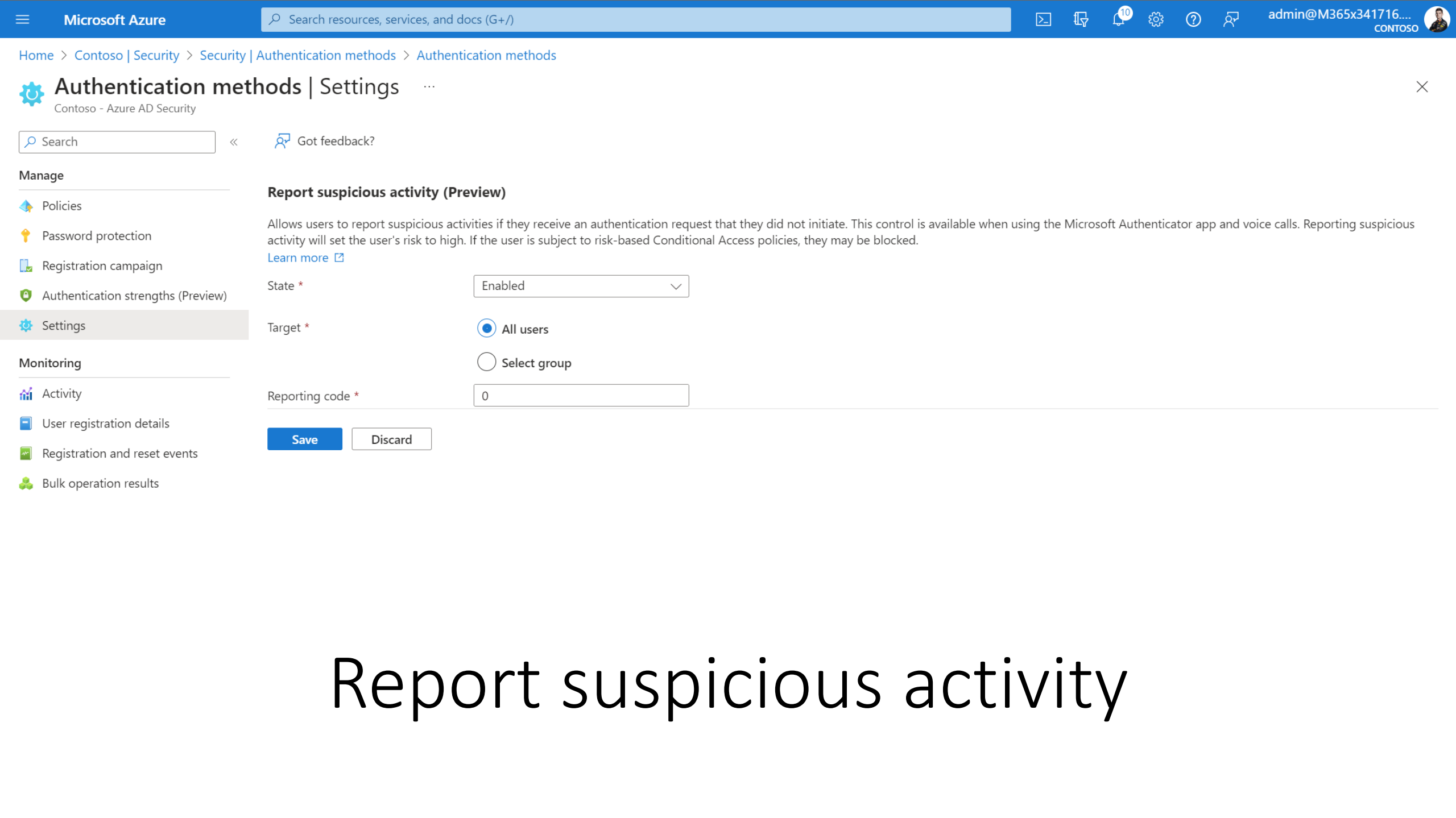
System preferred method – My Sign-ins



Authentication strengths

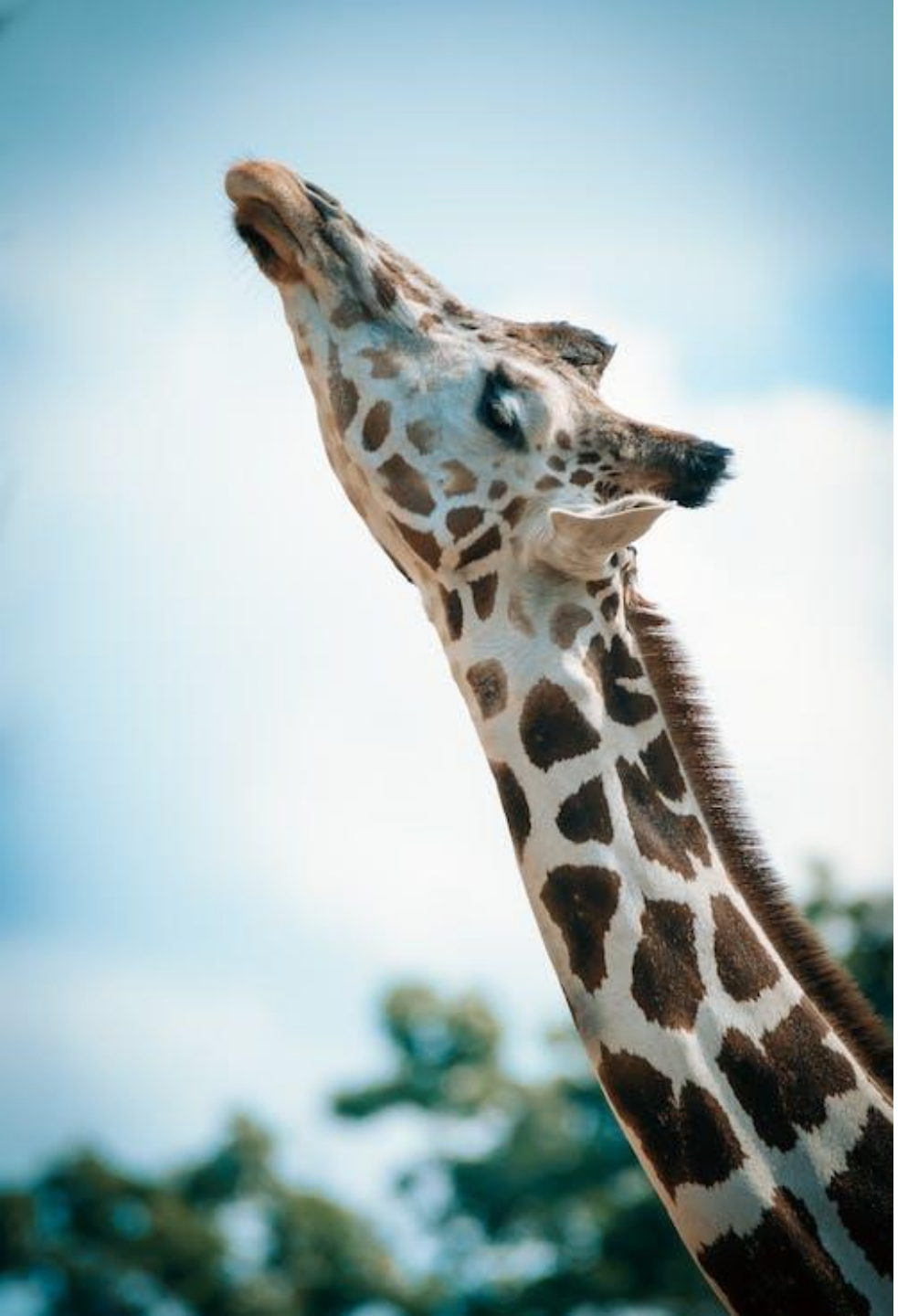
Built-in authentication strengths

Authentication method combination	MFA strength	Passwordless MFA strength	Phishing-resistant MFA strength
FIDO2 security key	✅	✅	✅
Windows Hello for Business	✅	✅	✅
Certificate-based authentication (Multi-Factor)	✅	✅	✅
Microsoft Authenticator (Phone Sign-in)	✅	✅	
Temporary Access Pass (One-time use AND Multi-use)	✅		
Password + something you have[1]	✅		
Federated single-factor + something you have[1]	✅		
Federated Multi-Factor	✅		
Certificate-based authentication (single-factor)			
SMS sign-in			
Password			
Federated single-factor			



Report suspicious activity

USER EXPERIENCE



Non managed =
non persistent, or:

less risk = longer
session duration

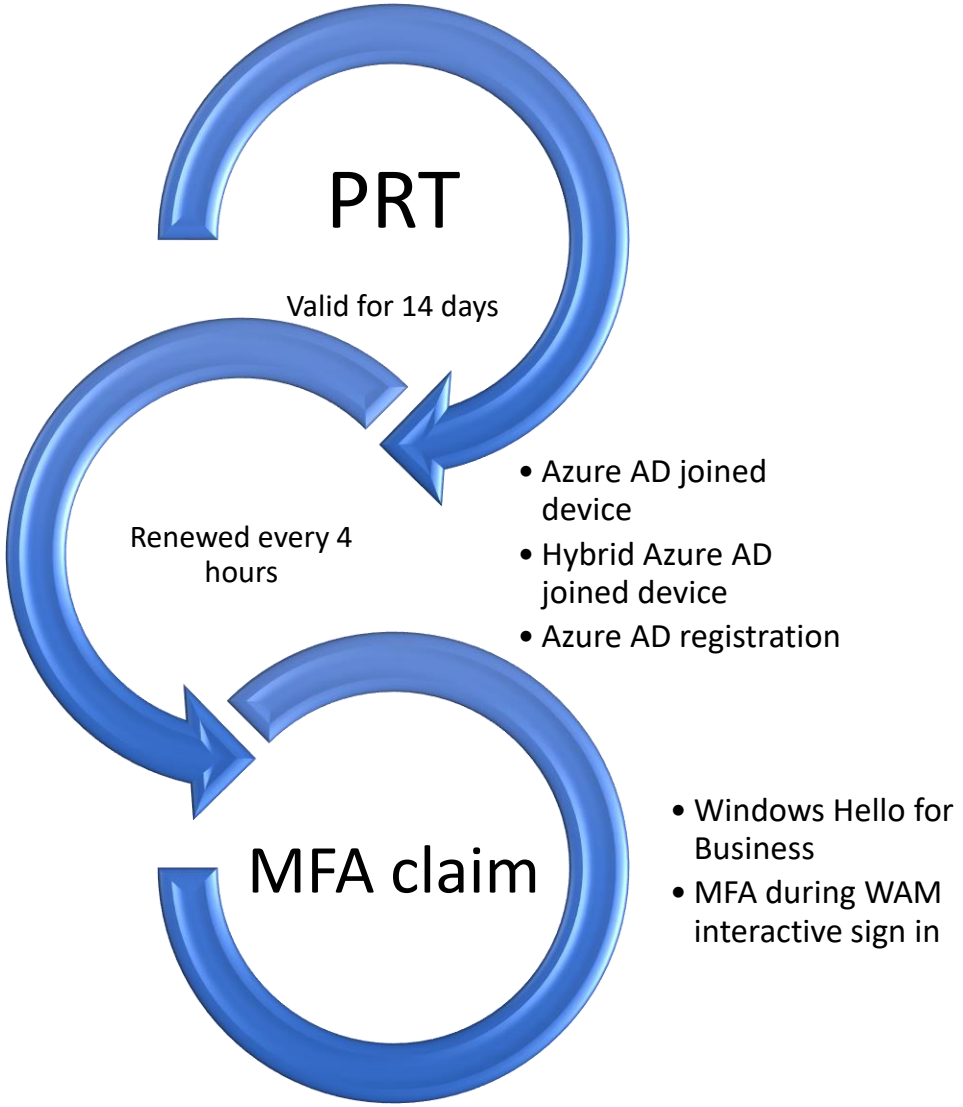
1 MFA prompt

Per user
Per device
Per password change

*if you don’t mess around too much with token lifetime and sign-in frequency

More prompts
eq
Bad user experience
eq
Bad security


In PRT we trust


PRT
Valid for 14 days
Renewed every 4 hours
• Azure AD joined device
• Hybrid Azure AD joined device
• Azure AD registration
MFA claim
• Windows Hello for Business
• MFA during WAM interactive sign in

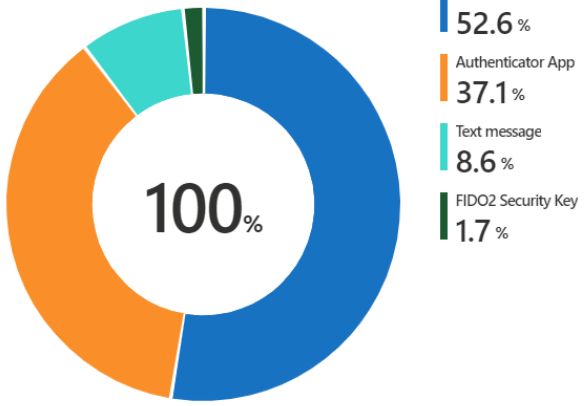
As Windows Hello for Business is considered multifactor authentication, the MFA claim is updated when the PRT itself is refreshed, so the MFA duration will continually extend when users sign in with Windows Hello for Business.

Visualize MFA fatigue

Authentication prompts by authentication method

To investigate methods causing the most prompts, filter this report by AuthMethod.

% Prompts by method



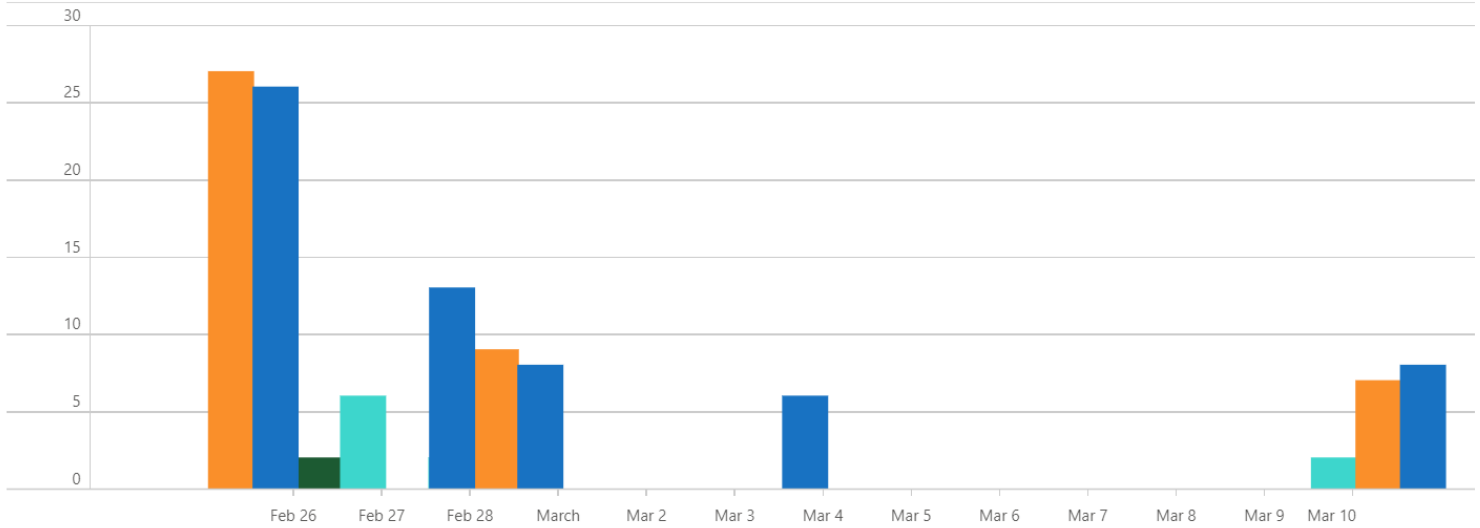
Password
52.6 %

Authenticator App
37.1 %

Text message
8.6 %

FIDO2 Security Key
1.7 %

Daily prompts by method



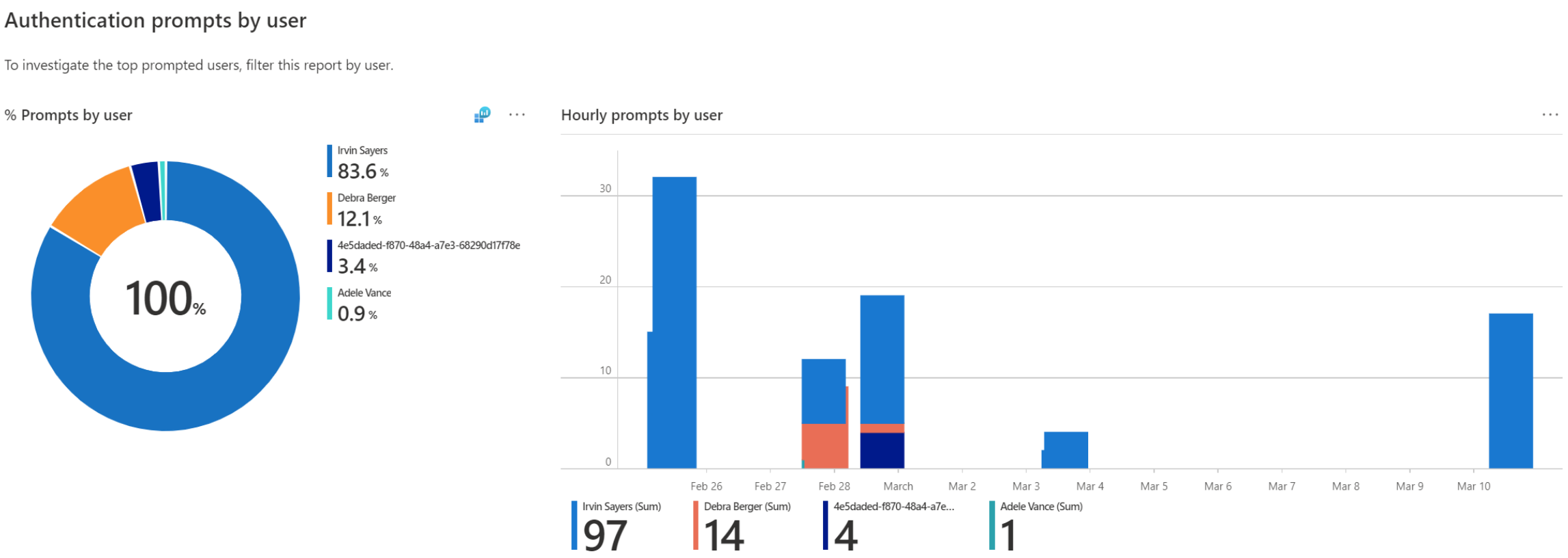
Password (Sum)
61

Authenticator App (Sum)
43

Text message (Sum)
10

FIDO2 security key (Sum)
2

Authentication Prompts Analysis



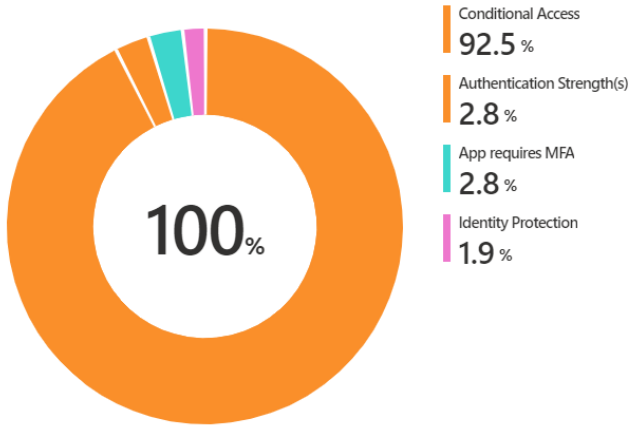
Authentication Prompts Analysis

Authentications prompts by policy

Authentication policies describe how MFA is enforced and can include Conditional Acces, Security Defaults, Per User MFA, App requires MFA, and others.

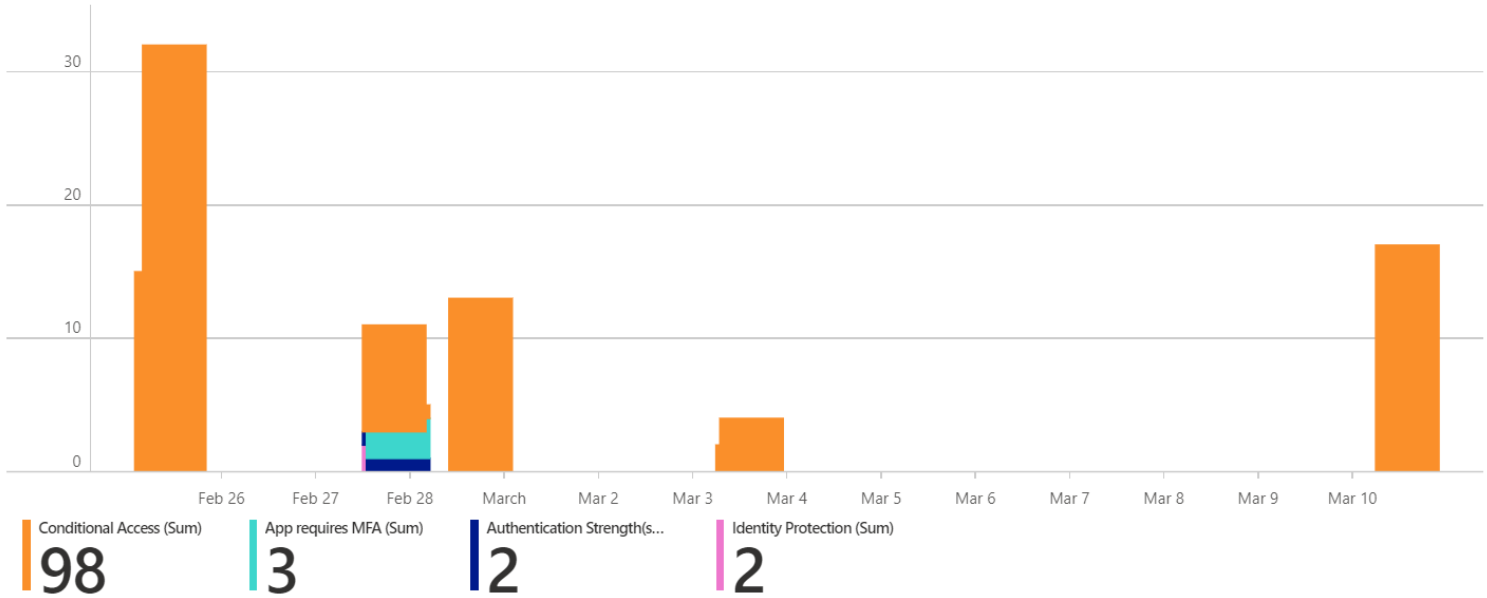
"App requires MFA" occurs when the application itself enforce the policy and requires a fresh MFA.

Prompts by authentication policy



- Conditional Access 92.5 %
- Authentication Strength(s) 2.8 %
- App requires MFA 2.8 %
- Identity Protection 1.9 %

Hourly prompts by authentication policy



- Conditional Access (Sum) 98
- App requires MFA (Sum) 3
- Authentication Strength(s... 2
- Identity Protection (Sum) 2

Authentication Prompts Analysis


Trusted IPs


Named Locations

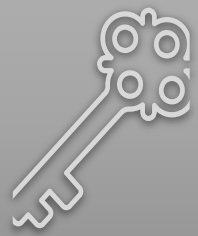

Keep Me Signed In

Sign-in Frequency

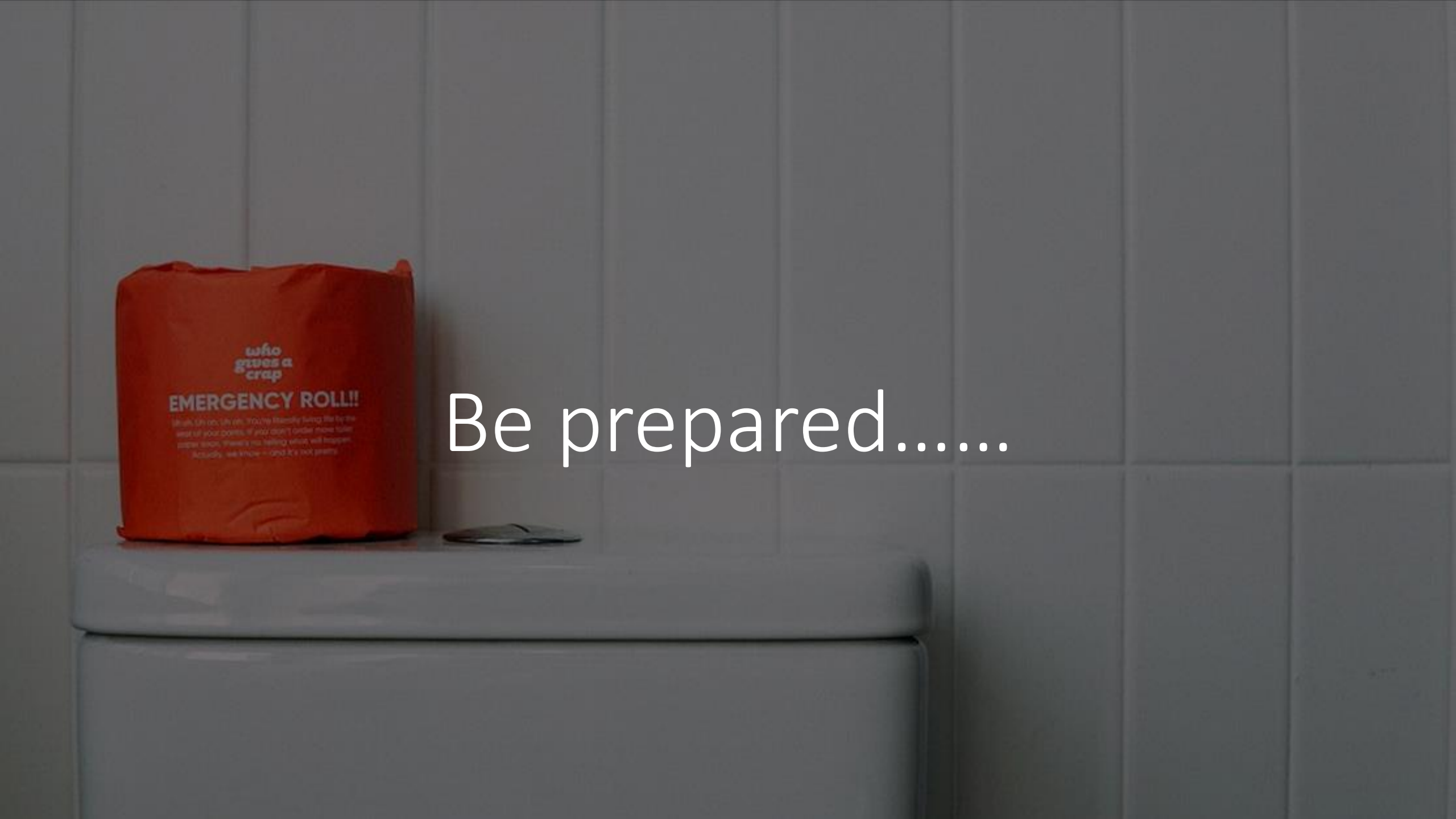
Provisioning

Phone number

Email



Temporary Access Pass



Be prepared……


FIDO to the rescue

To sum up

- Use Conditional Access where possible
- Mix with Identity Protection when possible
- Don’t use per-user MFA
- Migrate SSPR and legacy methods to auth methods policy
- Do not over-prompt end-users
- Use Window Hello (or FIDO2) where possible
- Always use the strongest method
- Enforce phishing resistant methods for administrators
- Have at least 2 break glass accounts
- Secure your security registration process
- Do not use legacy settings like KMSI or Trusted IP’s


Any questions?
non-cabbage related?

Stay safe!