



# AzureMFA

Jan Bakker

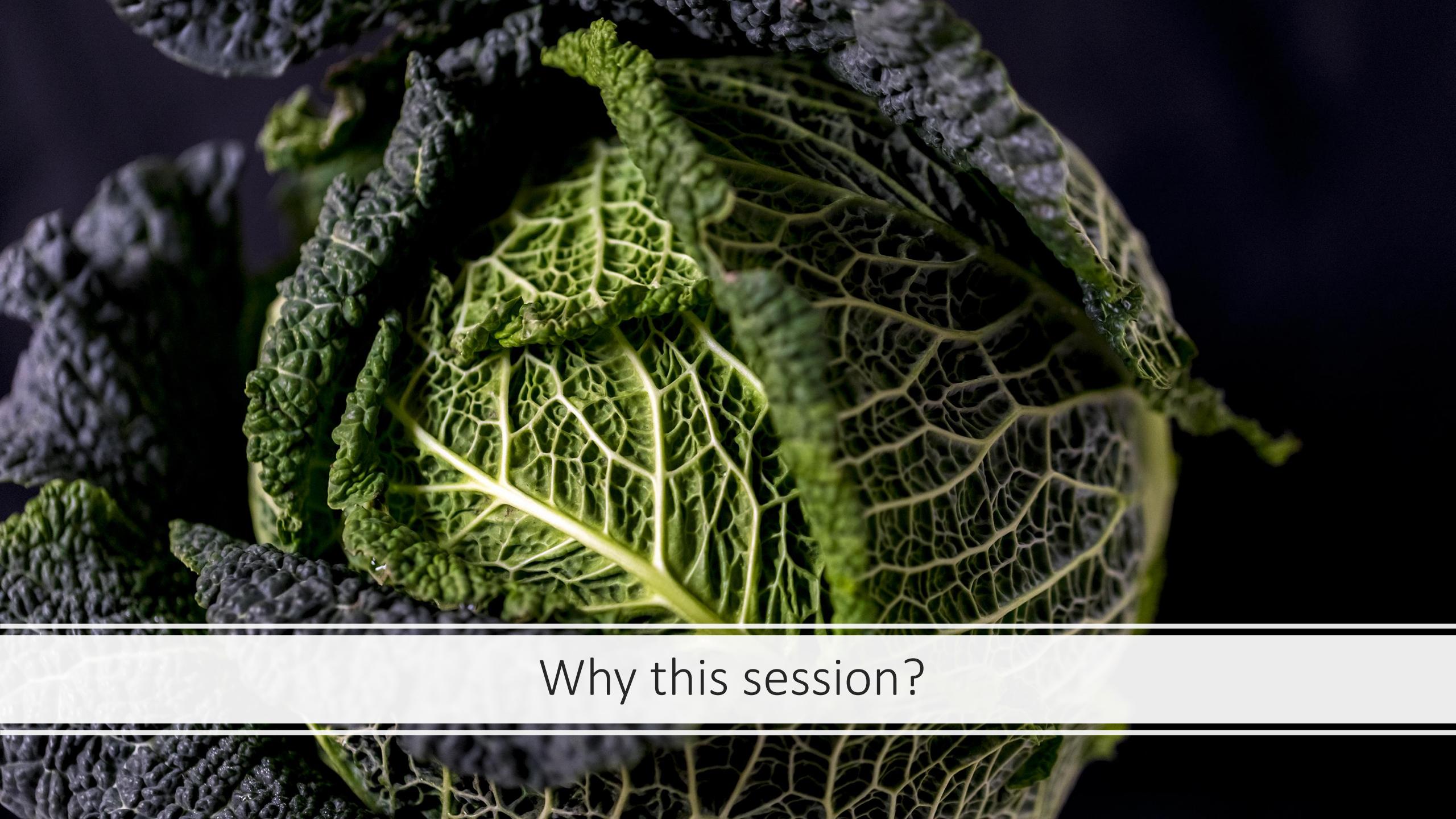


**Microsoft®**  
Most Valuable  
Professional



AKA.MS/JANBAKKER





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.



© Andy Brunning/Compound Interest 2017 - [www.compoundchem.com](http://www.compoundchem.com) | Twitter: @compoundchem | FB: [www.facebook.com/compoundchem](https://www.facebook.com/compoundchem)

This graphic is shared under a Creative Commons Attribution-NonCommercial-NoDerivatives licence.





So, what does it cost?

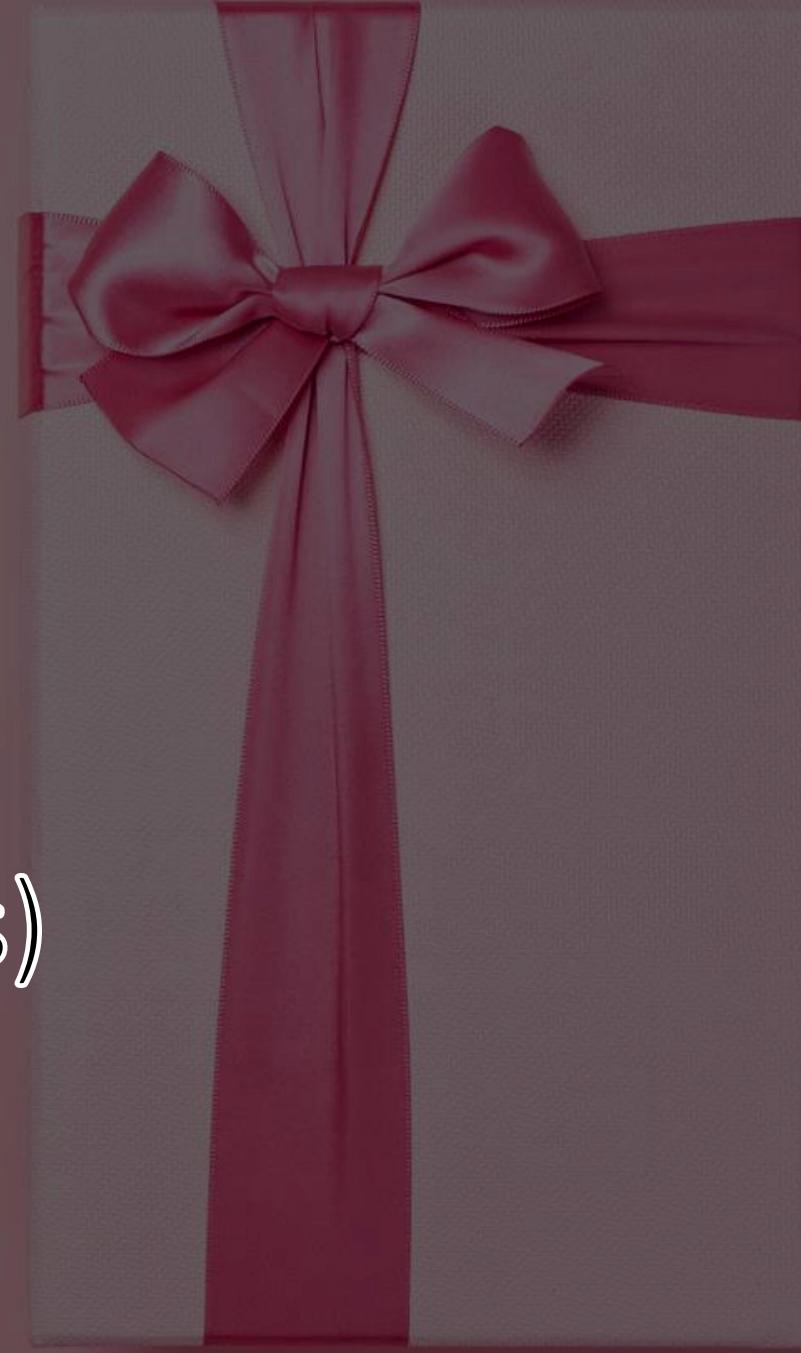
Free for:

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

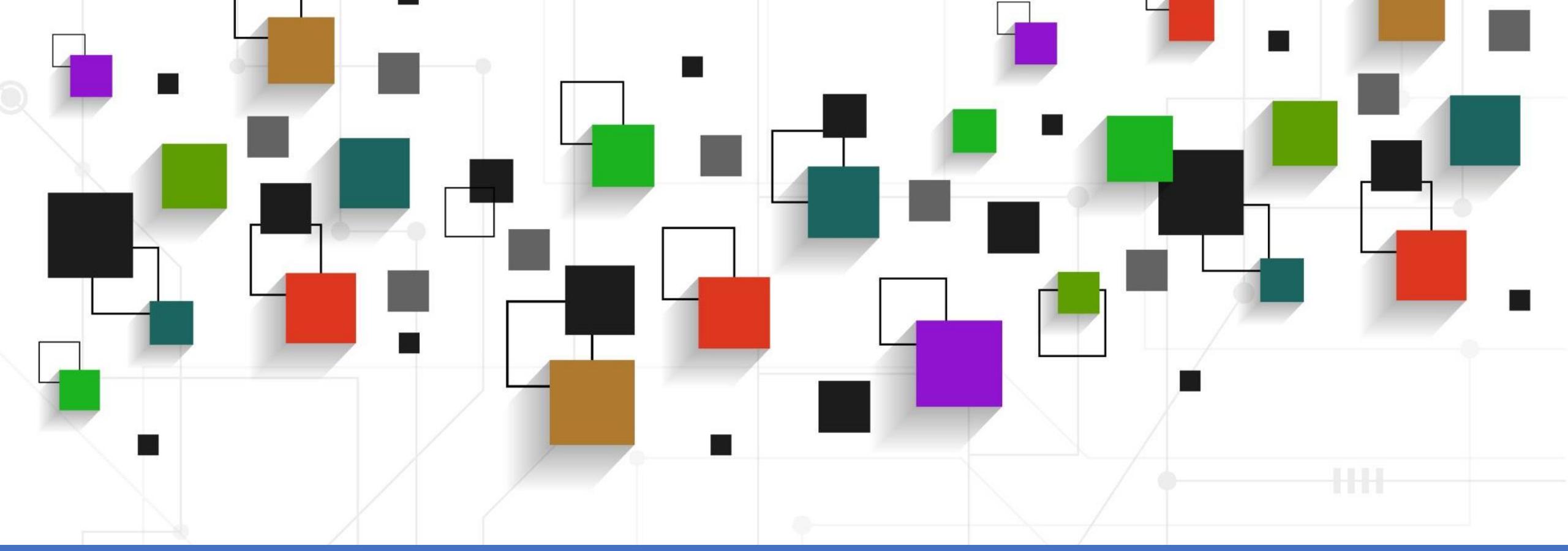
# Identity Protection

# Conditional Access

+

# Identity Protection

# Privileged Identity Management



# Enrollment

# First things first

(I want to get rid of this slide)

The image contains two side-by-side screenshots from Microsoft services.

**Top Screenshot:** A screenshot of a Microsoft Authenticator setup page titled "Keep your account secure". It instructs the user to install the Microsoft Authenticator app on their phone and then choose "Next". A "Next" button is visible at the bottom right. Below the main text, there is a link "I want to set up a different method".

**Bottom Screenshot:** A screenshot of the Microsoft Azure portal showing "User feature previews". The top navigation bar includes "Microsoft Azure", a search bar, and a user profile for "admin@contoso.com". The main content area shows three preview features:

- "Users can use preview features for My Apps" (status: All selected)
- "Users can use the combined security information registration experience" (status: All selected, highlighted with a red box)
- "Administrators can access My Staff" (status: All selected)



# Self Enrollment (manual)

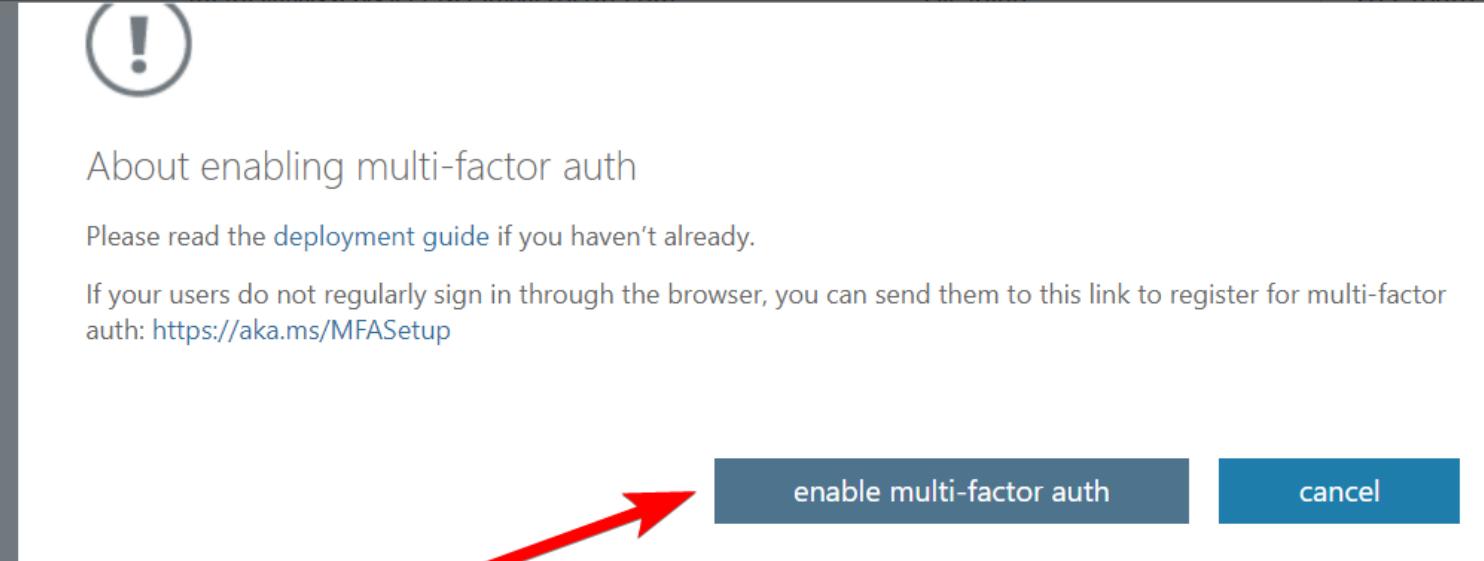
[aka.ms/mfasetup](https://aka.ms/mfasetup)

[aka.ms/setupsecurityinfo](https://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
<input type="checkbox"/>	DISPLAY NAME ▾	USER NAME	MULTI-FACTOR AUTH STATUS	
<input checked="" type="checkbox"/>	Adele Vance	AdeleV@M365x341716.OnMicrosoft.com	Disabled	<p>Adele Vance</p> <p>AdeleV@M365x341716.OnMicrosoft.com</p> <p>205 108th Ave. NE, Suite 400</p> <p>NOT ANYTHING HERE</p> <p>! About enabling multi-factor auth</p> <p>Please read the <a href="#">deployment guide</a> if you haven't already.</p> <p>If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: <a href="https://aka.ms/MFASetup">https://aka.ms/MFASetup</a></p> <p><input type="button" value="enable multi-factor auth"/> <input type="button" value="cancel"/></p> 
<input type="checkbox"/>	Alex Wilber	AlexW@M365x341716.OnMicrosoft.com	Disabled	
<input type="checkbox"/>	Allan Deyoung	AllanD@M365x341716.OnMicrosoft.com	Disabled	
<input type="checkbox"/>	Automate Bot			
<input type="checkbox"/>	Bianca Pisani			
<input type="checkbox"/>	Brian Johnson (TA)			
<input type="checkbox"/>	Cameron White			
<input type="checkbox"/>	Christian Horner			
<input type="checkbox"/>	Christie Cline			
<input type="checkbox"/>	Conf Room Adam			
<input type="checkbox"/>	Conf Room Baker	Baker@M365x341716.OnMicrosoft.com	Disabled	
<input type="checkbox"/>	Conf Room Crystal	Crystal@M365x341716.OnMicrosoft.com	Disabled	

## Password reset | Registration ...

Contoso - Azure Active Directory

&lt;&lt;

Save Discard

Require users to register when signing in?

 Yes  No

Number of days before users are asked to re-confirm their authentication information

180



These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

Diagnose and solve problems

## Manage

Properties

Authentication methods

## Registration

Notifications

Customization

On-premises integration

Administrator Policy

## Activity

Audit logs

Usage &amp; insights

## Troubleshooting + Support

New support request

## Self-Service Password Reset

Home &gt; Identity Protection



## Identity Protection | Multifactor authentication registration policy



Search

&lt;&lt;

Policy Name

Multifactor authentication registration policy

 Overview Tutorials Diagnose and solve problems

## Protect

 User risk policy Sign-in risk policy Multifactor authentication  
registration policy

## Report

 Risky users Risky workload identities Risk detection

Assignments

 Users

All users

Controls

 Require Azure AD multifactor  
authentication registration

# Identity Protection

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 ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Control access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multifactor authentication

ⓘ

**i** Consider testing the new "Require authentication strength" public preview. [Learn more](#)

Require authentication strength (Preview)

ⓘ

**⚠** "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

Require device to be marked as compliant

ⓘ

# Conditional Access



Home &gt; Conditional Access | Policies &gt;

## 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 \*

### 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

0 controls selected

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to



Select the action this policy will apply to

 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

Search User    

## Temporary Access Pass

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

 Create Temporary Access Pass

 List/Get Temporary Access Pass

 Delete Temporary Access Pass

 Send Temporary Access Pass to mobile phone

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

NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes for risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' it's recommended to extend the session lifetime by 30 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

[View options](#) ([learn more](#))

Methods

- Call to phone  
 Text message to phone  
 Notification to mobile app  
 Verify 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

NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes for risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' it's recommended to extend the number of days. [Learn more about reauthentication prompts.](#)

Home &gt;

## 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

Home &gt; Irvin Sayers

## Irvin Sayers | Authentication methods



Irvin Sayers

User

[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	...

### Nonusable authentication methods

Authentication method	Detail	
No nonusable methods.		



### 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](#)

# Manage migration

X

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.

 Authentication Methods for SSPR and Signin can now be managed in one converged policy. [Learn more](#)

Number of methods required to reset ⓘ

1

2

Methods available to users

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

 These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

## 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

## 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
<a href="#">FIDO2 security key</a>	All users	Yes
<a href="#">Microsoft Authenticator</a>	All users	Yes
<a href="#">SMS (Preview)</a>	All users	Yes
<a href="#">Temporary Access Pass</a>	All users	Yes
<a href="#">Third-party software OATH tokens (Preview)</a>	All users	Yes
<a href="#">Voice call (Preview)</a>		No
<a href="#">Email OTP (Preview)</a>		No
<a href="#">Certificate-based authentication</a>		No



How to  
handle  
previous  
registrations?

## Authentication methods | Registration campaign

Contoso - Azure AD Security

[Got feedback?](#)**Manage**[Policies](#)[Password protection](#)[Registration campaign](#)[Authentication strengths \(Preview\)](#)[Settings](#)**Monitoring**[Activity](#)[User registration details](#)[Registration and reset events](#)[Bulk operation results](#)**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)



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](#)

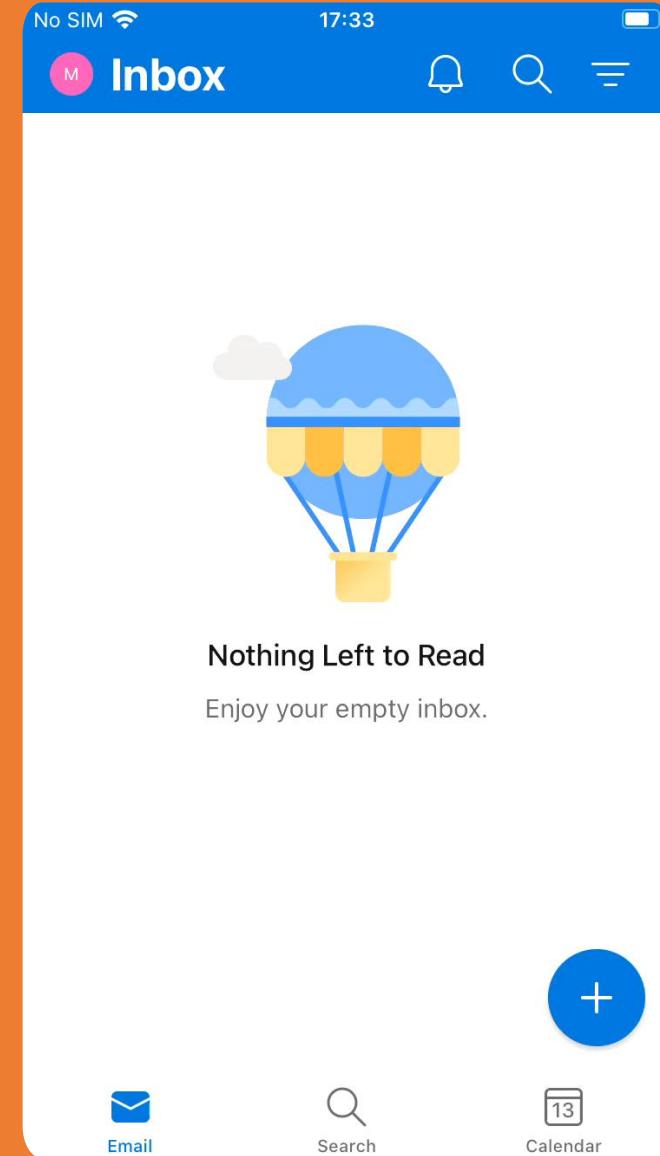
[Next](#)

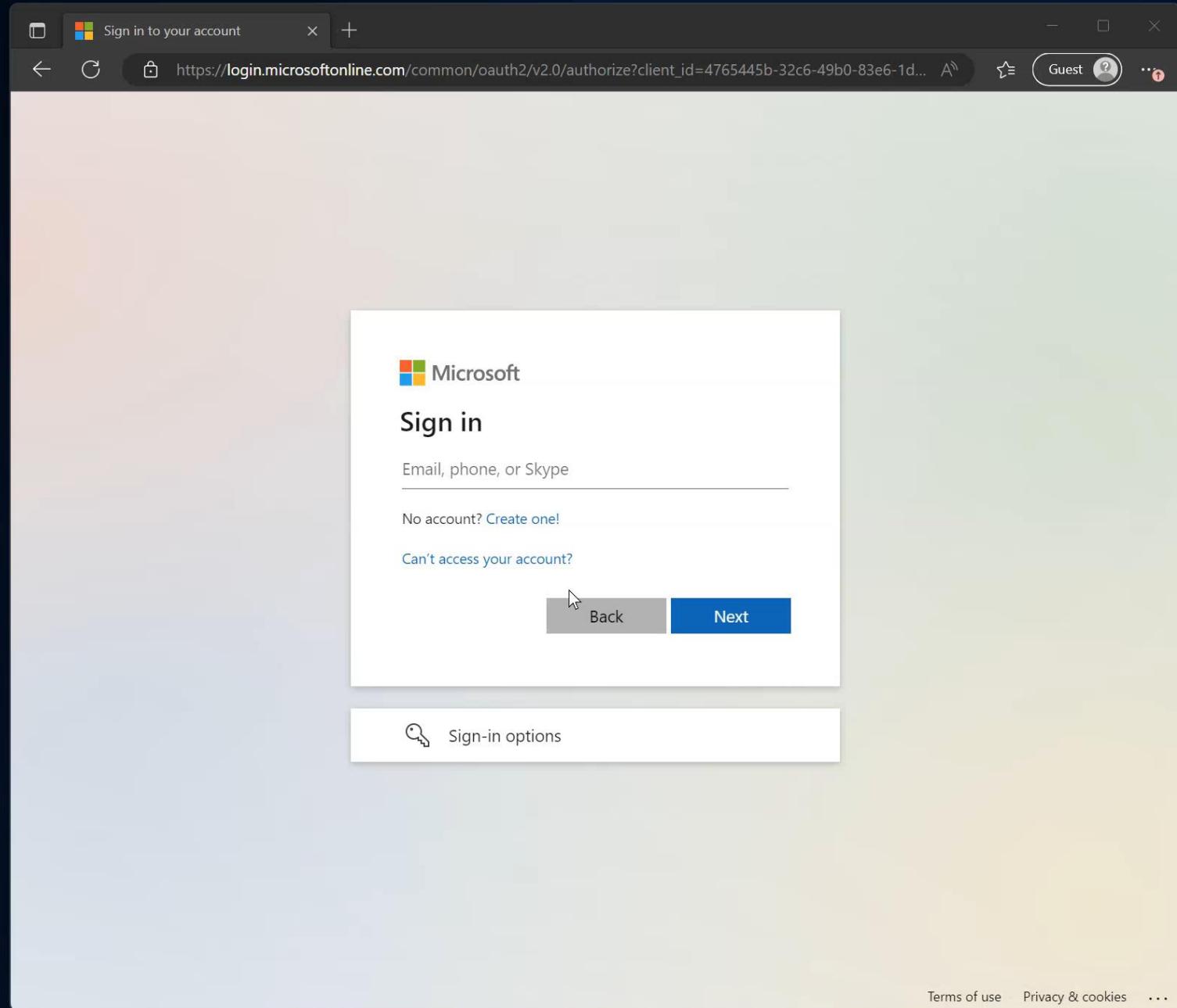
Hate typing your password? Go passwordless today  
 <https://aka.ms/passwordless>

A close-up photograph of a person's hand holding a red marker, writing the word "NO" in large, bold letters on a transparent or light-colored surface. The background is blurred, showing a woman with long brown hair looking down at the writing. The lighting is dramatic, with strong highlights on the red marker and the letters.

NO

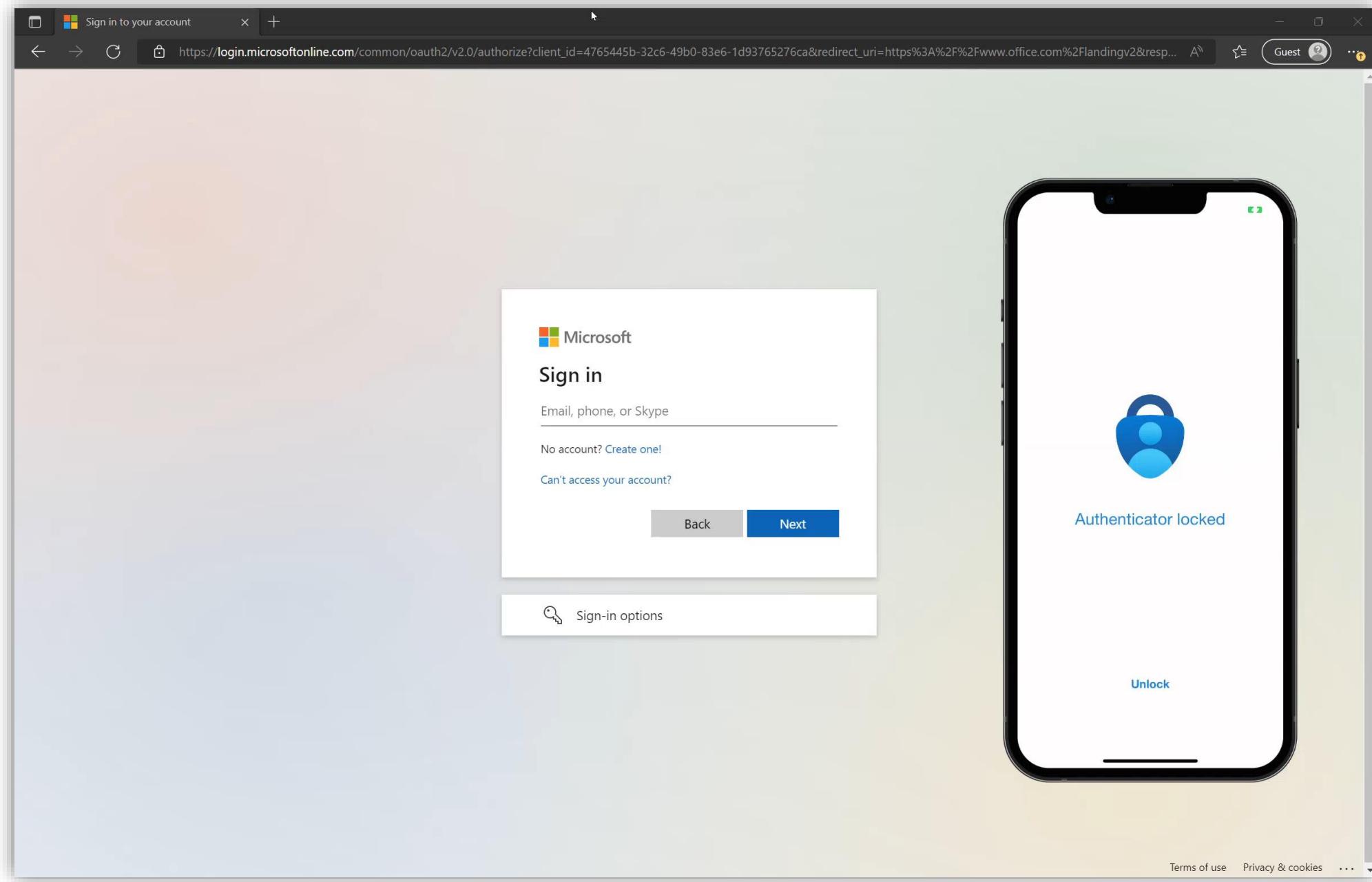
# Authenticator Lite enrollment with TAP





# Microsoft Authenticator App features







[Sample queries](#)[Resources](#)

...

PATCH ▾

beta ▾

https://graph.microsoft.com/beta/authenticationMethodsPolicy



Run query



Search sample queries

ⓘ See more queries in the [Microsoft Graph API Reference docs](#).

Getting Started (8)

**GET** my profile

**GET** my profile (beta)

**GET** my photo

**GET** my mail

**GET** list items in my drive

**GET** items trending around ...

**GET** my manager

Request body

Request headers

Modify permissions

Access token

```
▽ {  
  ▽ "systemCredentialPreferences": {  
    "state": "enabled",  
    "includeTargets": [  
      {  
        "id": "all_users",  
        "targetType": "group"  
      }  
    ]  
  }  
}
```

✓ No Content - 204 - 650ms X

Response preview

Response headers

Code snippets

Toolkit component

Adaptive cards

Expand

{}

# 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.

Overview

Security info

Organizations

Devices

Privacy

## Security info

These are the methods you use to sign into your account or reset your password.

You're using the most advisable sign-in method where it applies.

Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification [Change](#)

Add sign-in method

	Phone	+31 649158615	<a href="#">Change</a>	<a href="#">Delete</a>
	Microsoft Authenticator	iPhone 13 Pro	<a href="#">Change</a>	<a href="#">Delete</a>
	Security key	My FIDO key	<a href="#">Change</a>	<a href="#">Delete</a>

Lost device? [Sign out everywhere](#)

# System preferred method – My Sign-ins

 **Authentication methods** | Authentication strengths (Preview)  
Contoso - Azure AD Security Search

&lt;&lt;

[+ New authentication strength](#) 

...

X

**Manage** Policies Password protection Registration campaign Authentication strengths (Preview) Settings**Monitoring** Activity User registration details Registration and reset events Bulk operation results

Authentication strengths determine the combination of authentication methods that can be used.  
[Learn more](#)

Type: All

Authentication methods: All

 Reset filters

Authentication strength	Type	Authentication methods	Conditional access policies	...
<a href="#">Authenticator App only</a>	Custom	Password + Microsoft Authenticator (Push Notifica...)	<a href="#">Require authentication strength for E...</a>	...
<a href="#">WHfB Only</a>	Custom	Windows Hello For Business	Not configured in any policy yet	...
<a href="#">Multifactor authentication</a>	Built-in	Windows Hello For Business and 16 more	Not configured in any policy yet	...
<a href="#">Passwordless MFA</a>	Built-in	Windows Hello For Business and 3 more	Not configured in any policy yet	...
<a href="#">Phishing-resistant MFA</a>	Built-in	Windows Hello For Business and 2 more	<a href="#">Demo-SecAttr-Privileged-Apps and 2...</a>	...

# 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 <sup>1</sup>	✓		
Federated single-factor + something you have <sup>1</sup>	✓		
Federated Multi-Factor	✓		
Certificate-based authentication (single-factor)			
SMS sign-in			
Password			
Federated single-factor			

## Authentication methods | Settings

Contoso - Azure AD Security



Search



Got feedback?

### Report suspicious activity (Preview)

Allows users to report suspicious activities if they receive an authentication request that they did not initiate. This control is available when using the Microsoft Authenticator app and voice calls. Reporting suspicious activity will set the user's risk to high. If the user is subject to risk-based Conditional Access policies, they may be blocked.

[Learn more](#)

State \*

Enabled



Target \*

 All users Select group

Reporting code \*

0

[Save](#)[Discard](#)

# 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

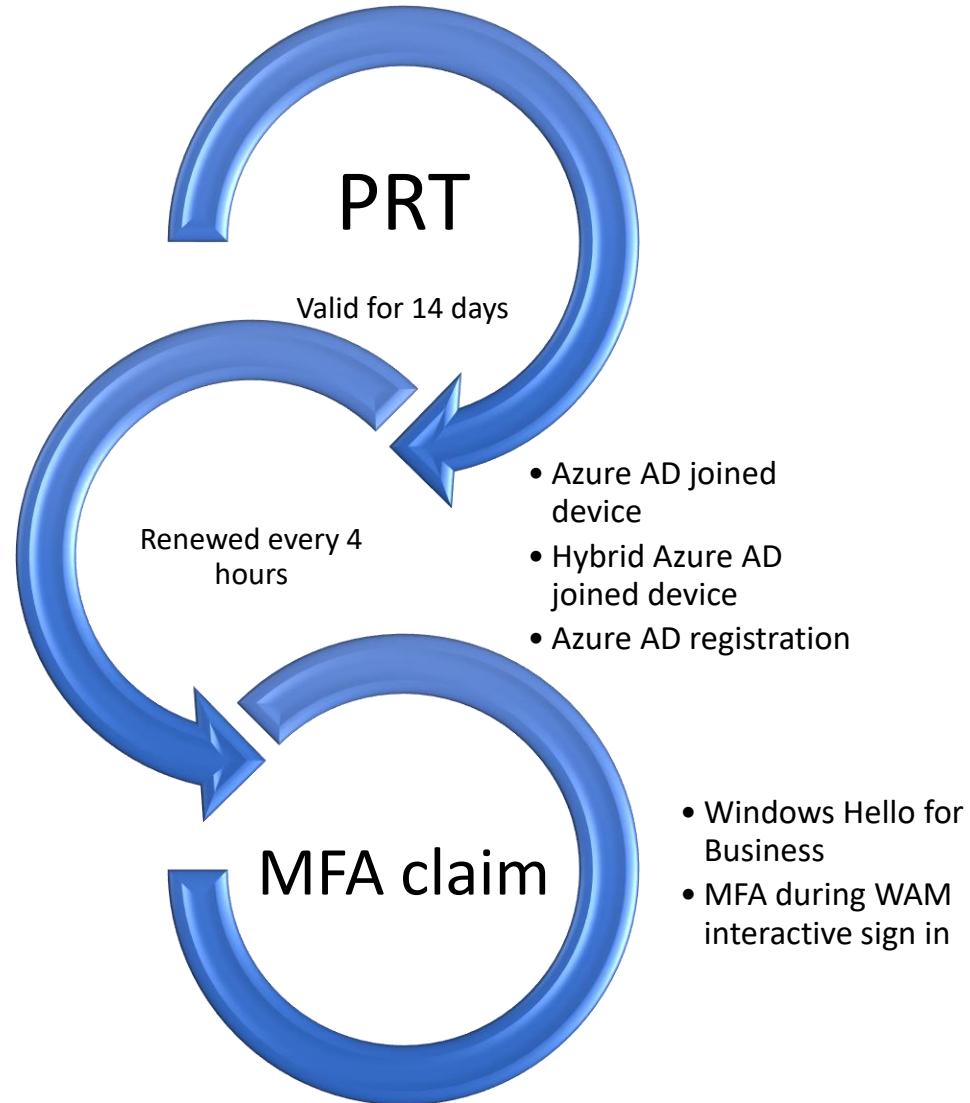
Bad user experience

eq  
Bad security



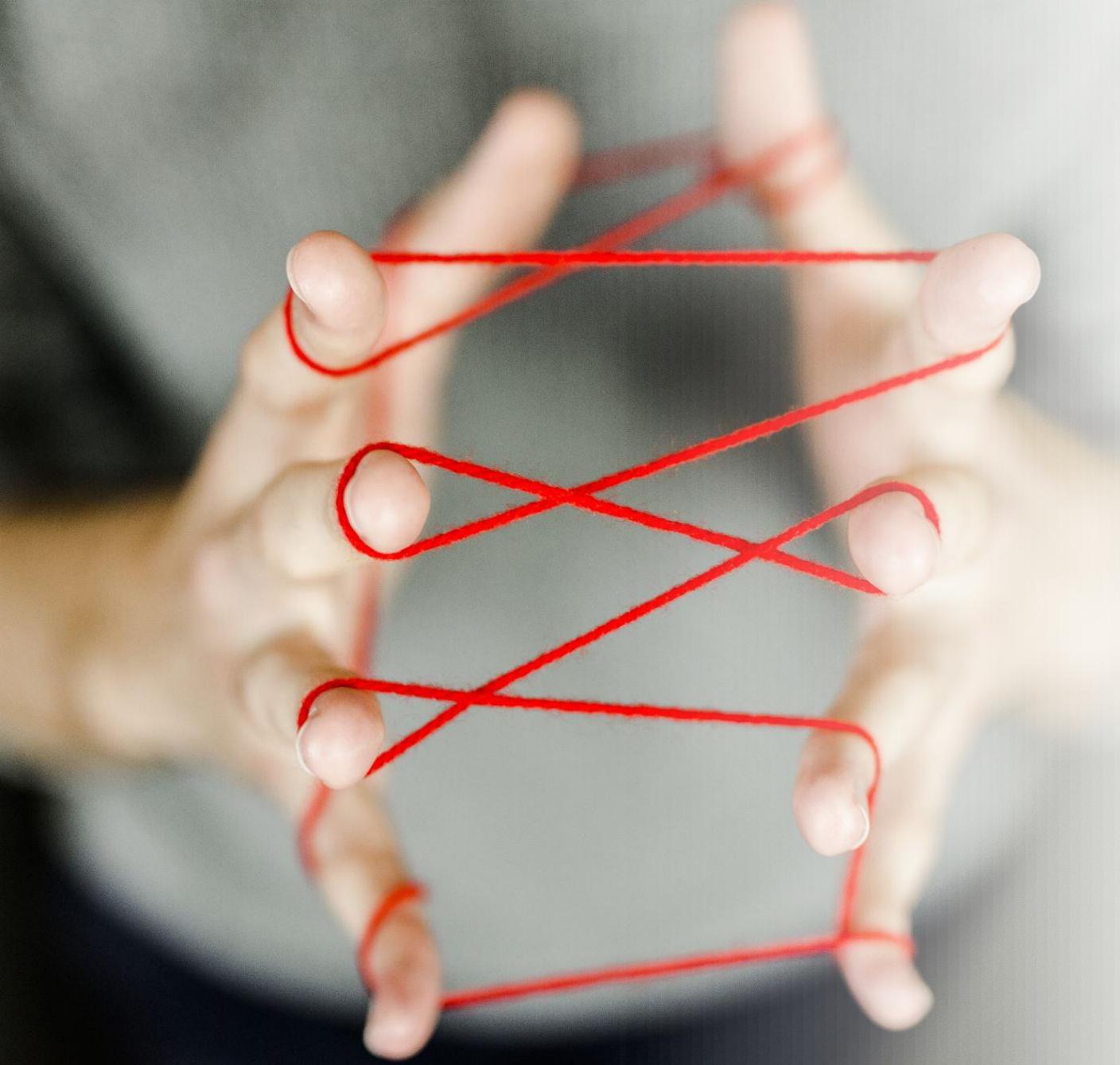
In PRT we trust





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.





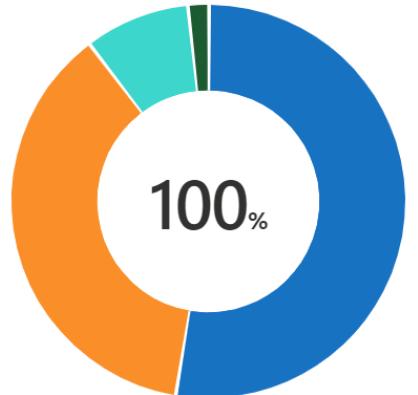
Visualize MFA  
fatigue

---

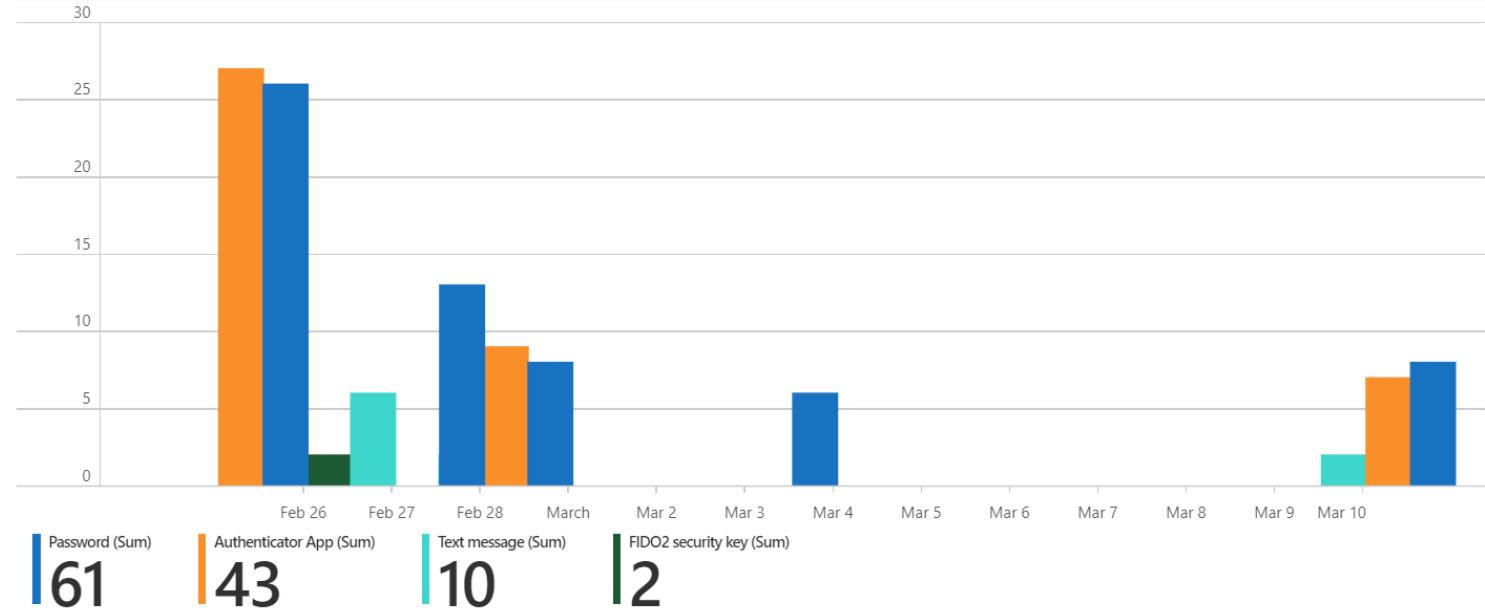
## Authentication prompts by authentication method

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

% Prompts by method



Daily prompts by method

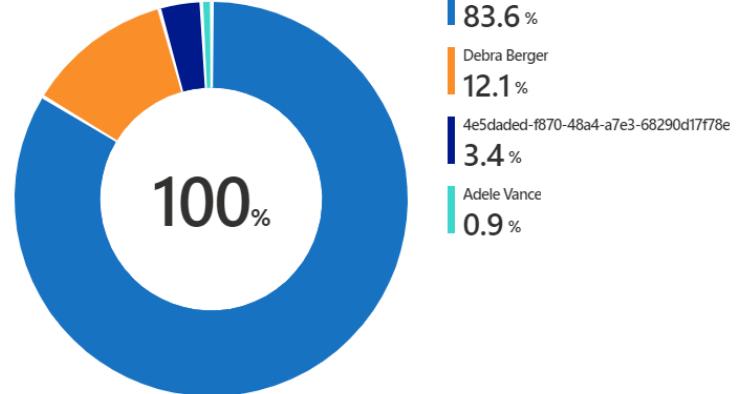


# Authentication Prompts Analysis

## Authentication prompts by user

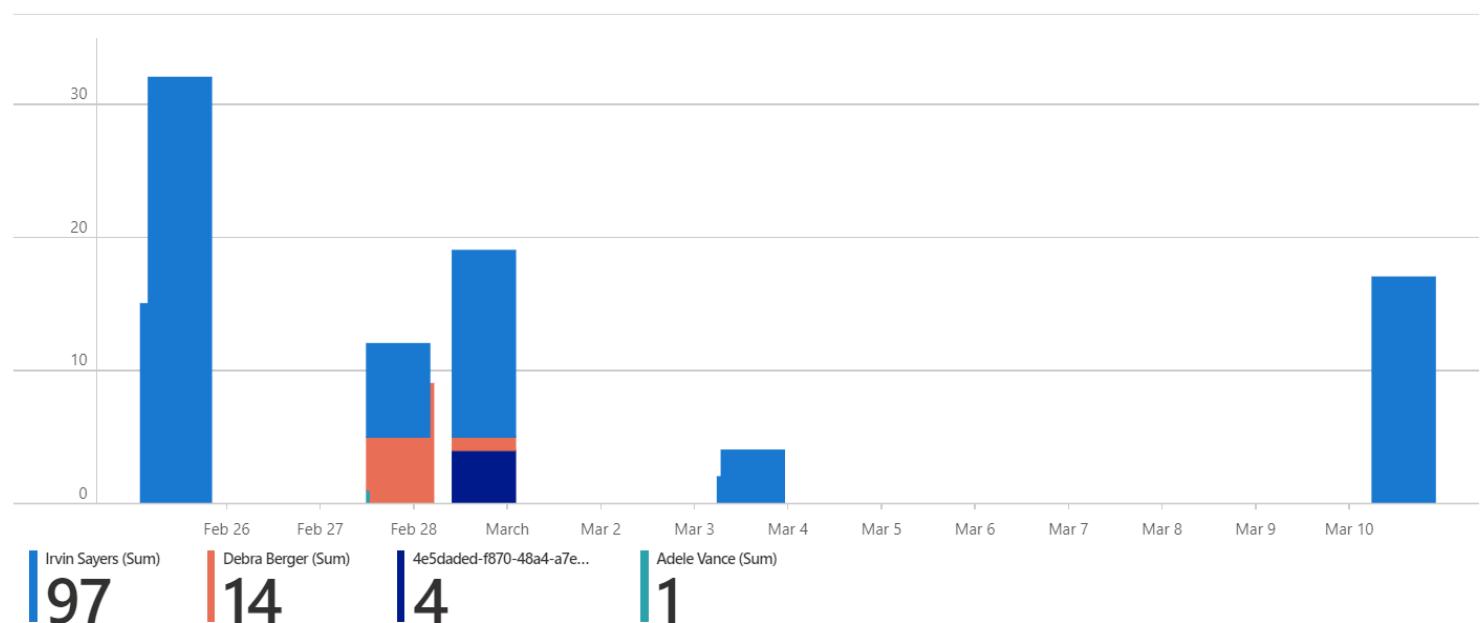
To investigate the top prompted users, filter this report by user.

% Prompts by user



...

Hourly prompts by user



...

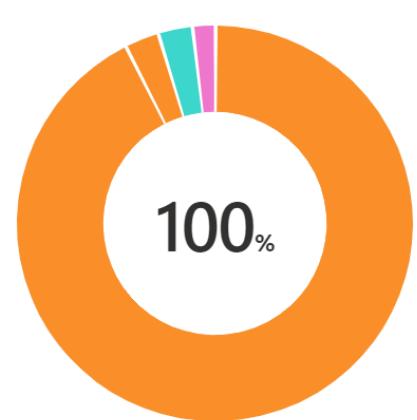
# Authentication Prompts Analysis

## Authentications prompts by policy

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

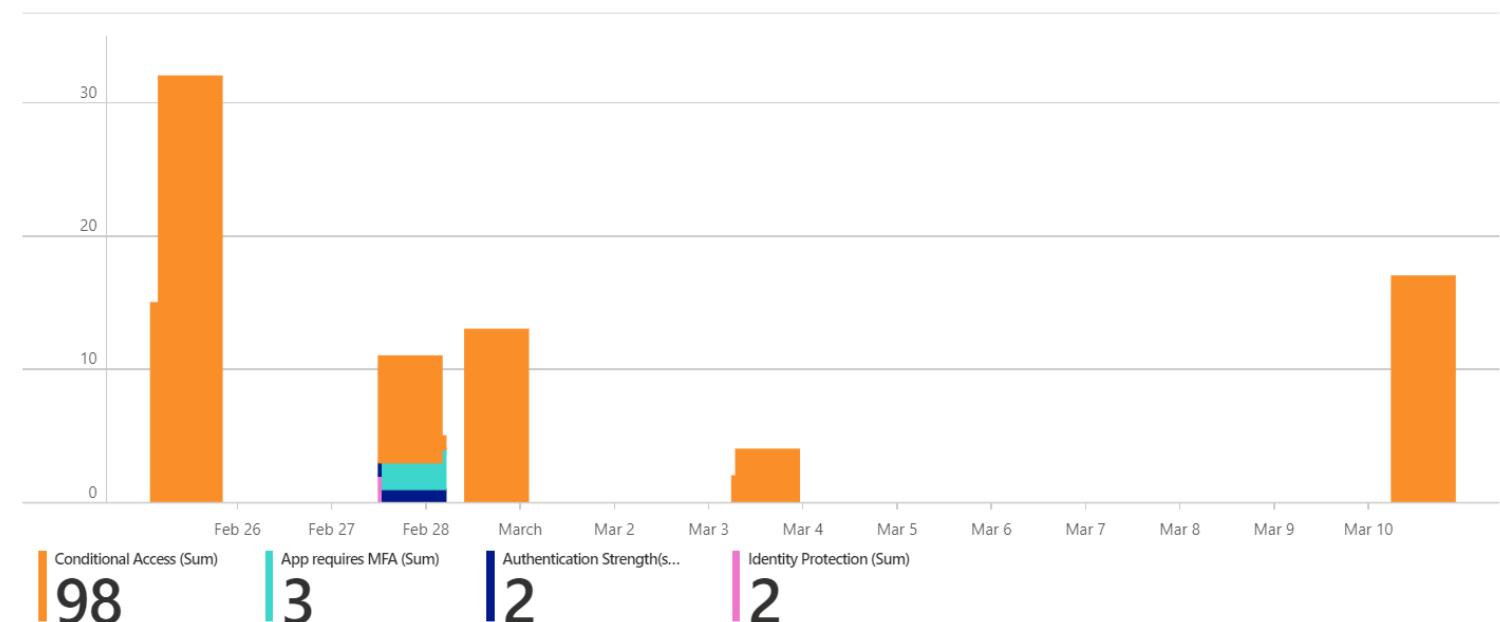
"App requires MFA" occurs when the application itself enforces the policy and requires a fresh MFA.

Prompts by authentication policy



⋮

Hourly prompts by authentication policy



⋮

# Authentication Prompts Analysis

A dark, atmospheric image of Neuschwanstein Castle in Germany. The castle, a prominent example of Romanesque Revival architecture, is perched on a hillside. Its light-colored stone walls, multiple towers with dark roofs, and intricate stonework are visible against a hazy sky. The surrounding landscape includes green fields and distant hills. Overlaid on the center of the image is the text "Trusted IPs" in a large, white, sans-serif font.

Trusted IPs

A photograph of Neuschwanstein Castle in Germany, a prominent example of Romanesque Revival architecture. The castle features light-colored stone walls, dark slate roofs with numerous gables and finials, and several tall, thin towers with conical roofs. It is situated on a rocky outcrop with a dense forest in the foreground. The surrounding landscape consists of rolling green hills and fields under a clear sky.

# Named Locations

A close-up photograph of a chain-link fence. A single red heart-shaped padlock hangs from one of the horizontal wires. The background is a soft-focus view of a cloudy sky and some buildings, suggesting an urban or suburban setting.

Keep Me Signed In

A close-up photograph of a red heart-shaped padlock hanging from a chain-link fence. The fence's diamond pattern is visible in the foreground. In the background, a blurred view of a residential area with houses and trees under a cloudy sky is visible.

# 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?

Thank  
you!

Stay safe!