



# Weekly Technical Office Hours for Partners

## *Remote Work in challenging times*

Friday, May 29, 2020

The meeting will start at  
WEST 12:00 - CET 13:00 – EEST 14:00

# Technical Office Hours for WE Microsoft Partners: Remote Work in challenging times



## Agenda

- 1. Introduction**
- 2. The Journey to Password-less**
- 3. Q & A**
- 4. Poll – Proposed topics for next session**
- 5. How to get further help**
  - Support channels and options

# Our Virtual Team



Jing Liu  
Cloud Solution Architect (Azure)



Aline Harmand  
Partner Tech. Strategist (Security)



Bojan Magusic  
Cloud Solution Architect (Security)



Hans Hofkens  
Partner Tech. Architect (Security)



Jos Verlinde  
Partner Tech. Architect (Teams)



Toni Willberg  
Cloud Solution Architect (Azure)



Nuria Baeza Garcia  
Cloud Solution Architect (Security)



Sara Canteiro  
Partner Tech. Architect (Teams)



Giorgio Cifani  
Partner Tech. Architect (Teams)



Juha Saarinen  
Partner Tech. Architect (Teams)

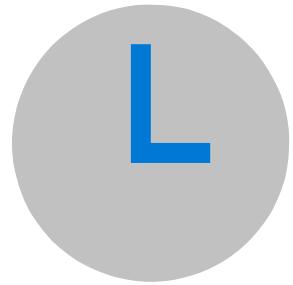


Olivier van der Kruijf  
Cloud Solution Architect (Azure)

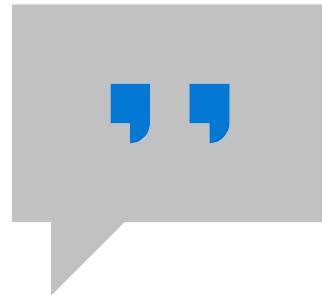


Philippe Goldstein  
Partner Tech. Manager

# WE Weekly Technical Office Hours – How it works



60 minutes  
40 min, presentation  
20 min, Q&A



Questions via  
chat through

Q&A

The screenshot shows a 'Live event Q&A' window. At the top, there are three icons: a person, a gear, and an information sign. Below that is a header bar with the title 'Live event Q&A' and a help icon. The main area has tabs for 'Featured' and 'My questions', with 'My questions' currently selected and highlighted in blue. Below the tabs, there are three user profiles with their names and a 'Reply' button next to each. At the bottom right of the main area, there are two emoji buttons: one with sunglasses and another with a smiley face. Below the main area, there's a section titled 'Ask a moderator' with the sub-instruction: 'Questions won't be visible to everyone until a moderator approves them'. There are input fields for 'Your name (optional)' and 'Ask a question', and a checkbox for 'Post as anonymous'.

# (WEEKLY) Technical Office Hours for WE Microsoft Partners:

## Remote Work in challenging times

JOIN  
UPCOMING  
SESSION



Currently we are receiving a lot of questions from our partners and customers with regards to recommendations and help on working remotely.

To address the main technical topics around working remotely, Microsoft's Western Europe OCP Technical Team is setting up a series of Weekly Office Hours for Partners,

every Friday at

13:00 – 14:00 CET (12:00 – 13:00 WEST)

All sessions will be held in English.

Add to Calendar 

**<https://aka.ms/WE-TechOfficeHours>**

Don't miss a session;  
Update your calendar by  
using the invite above.

Next  
Session  
Details

Upcoming  
Sessions

Materials &  
Recordings

Other  
Resources

Feedback  
Form

Hey, This landing page is actually a PowerPoint. Click through to see the next slides.



# Influence the Agenda

Please fill the following survey to influence the agenda and help us delivering session relevant for you.



or <http://aka.ms/WE-TechOfficeHours/Poll>

# The Journey to Passwordless



Aline Harmand  
Partner Tech. Strategist (Security)



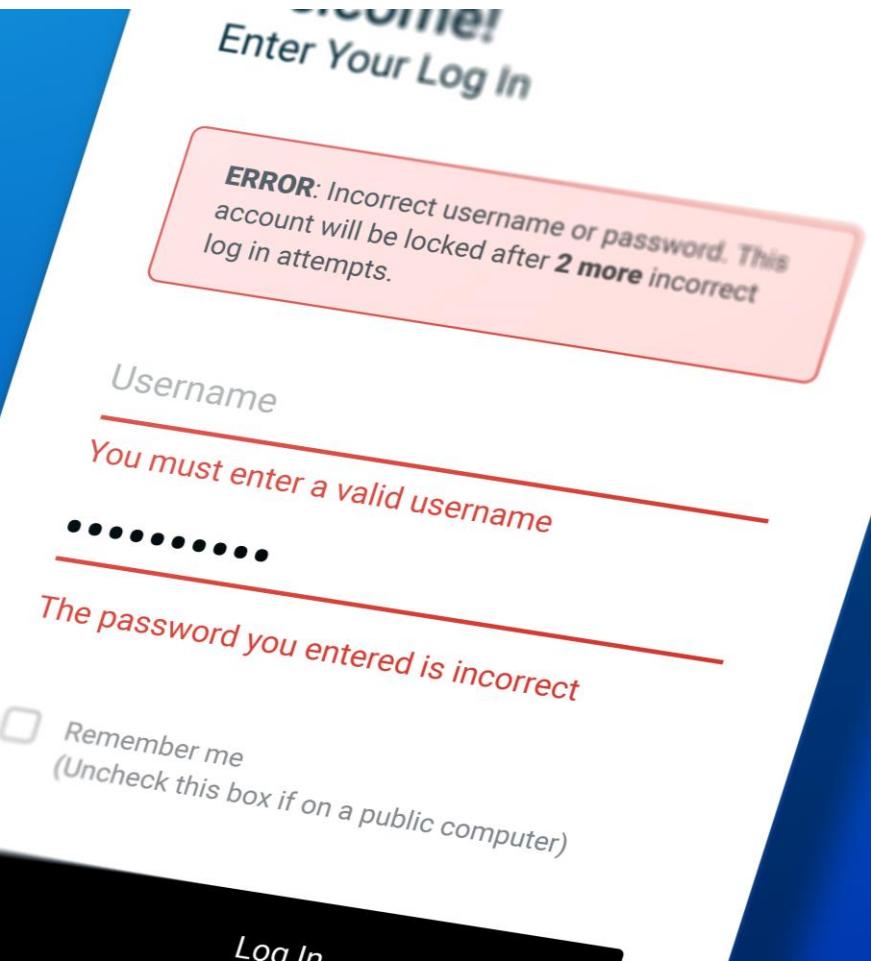
Bojan Magusic  
Cloud Solution Architect (Security)



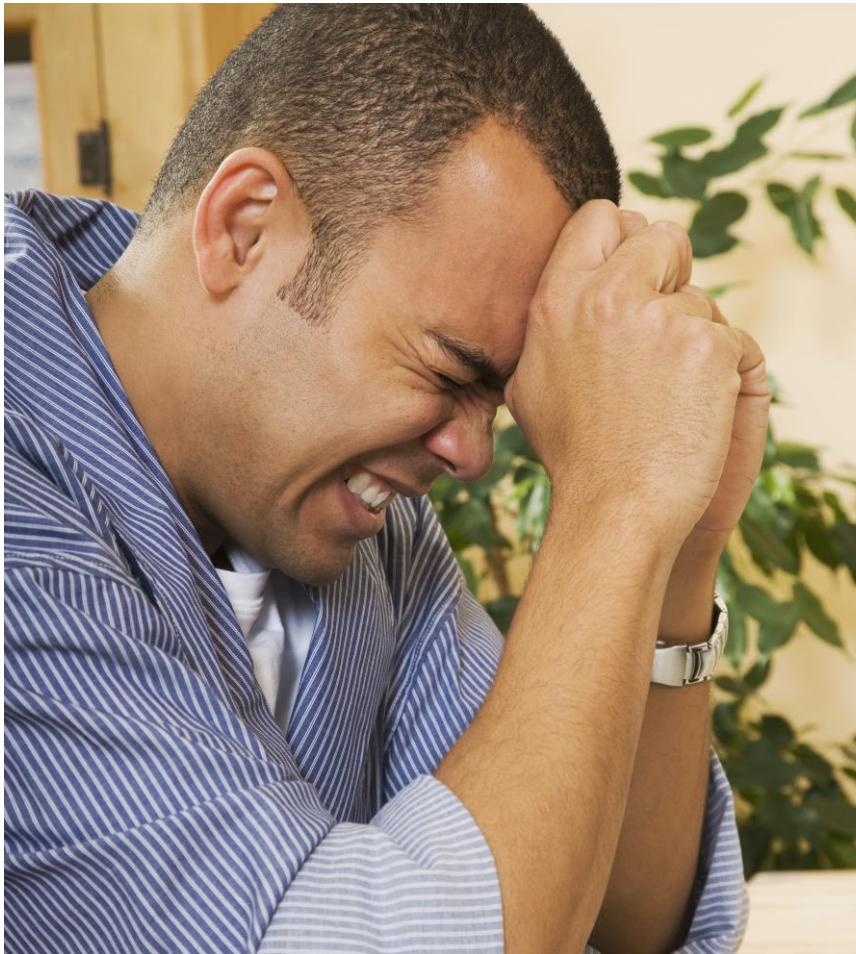
Hans Hofkens  
Partner Tech. Architect (Security)

# Almost everyone hates passwords

Users



IT Admins



Hackers



# Hackers ❤️ passwords

Most frequently rejected passwords  
from October 2018

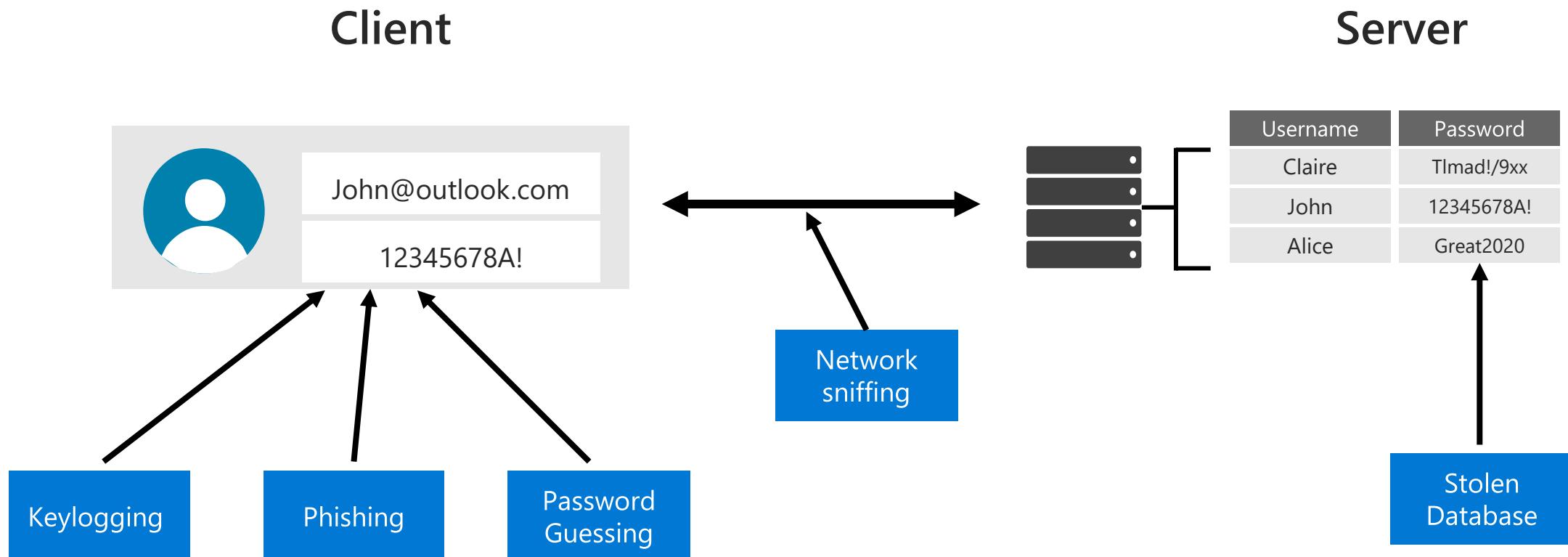
1	welc0me
2	2018
3	pa\$\$w0rd
4	1234
5	summer

6	fall
7	september
8	apple
9	soccer
10	london

<https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984>



# Attacks on passwords



# Why eliminate passwords?



Alpha-numeric passwords are hard to remember

On mobile devices passwords are difficult to enter

Even the strongest passwords are easily phishable.

# Passwords are expensive and insecure

Password reuse  
across multiple  
accounts

Passwords are  
the weak link

Data breaches  
are expensive

Passwords  
generate tons of  
support calls

73%  
of passwords are  
duplicates

81%  
of breaches  
leveraged  
passwords

\$3.86  
million, the  
average total  
cost of a data  
breach

20%  
of help desk calls  
are related to  
password resets

# Going passwordless is a journey. Start with a plan.

- Enable Azure MFA and Self-Service Password Reset in the event users need to fall back to using a password during the Pilot.

MFA all admins

Register all users for MFA

- Start with a Pilot

Deploy Windows Hello for Business for Windows 10 devices.

Try Microsoft Authenticator phone sign-in for added mobility.

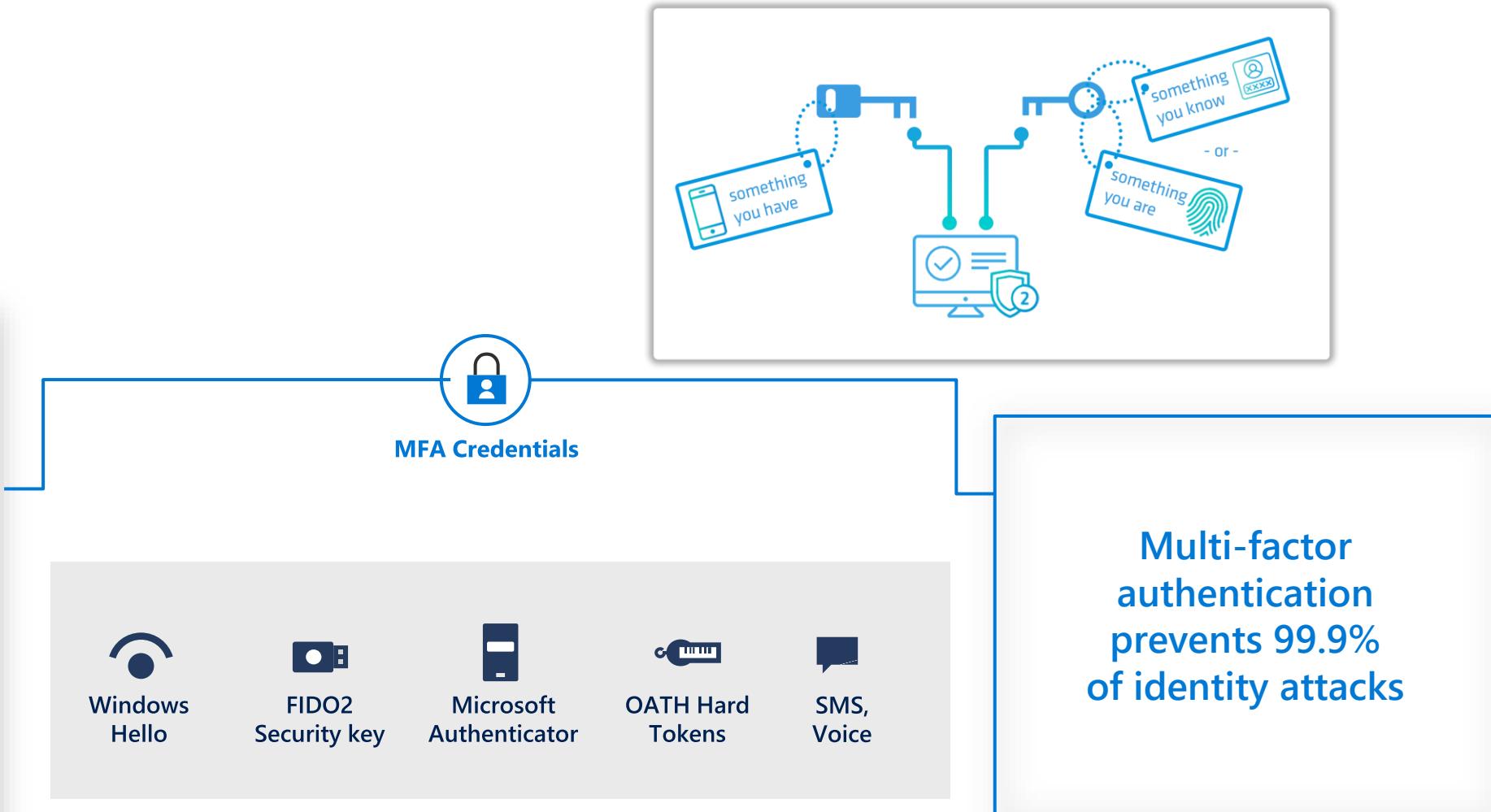
Pilot FIDO2 security keys

Identify and update apps to allow Azure AD authentication

- (Once possible) disable password-based auth

# Your password doesn't matter, but MFA does

**81%**  
of breaches  
leverage stolen or  
weak passwords



Free MFA options in all Azure AD subscriptions

# Enable MFA

## With Security Defaults

The screenshot shows the 'Contoso | Properties' page in the Azure Active Directory admin center. A modal window titled 'Enable Security defaults' is open. It contains a warning message: 'It looks like you have custom Conditional Access and Classic policies enabled. Enabling these policies prevents you from enabling Security defaults.' Below the message, a paragraph explains what security defaults are and how they protect against attacks. At the bottom of the modal, there are two buttons: 'Yes' (highlighted with a red arrow) and 'No'. In the background, the main page shows a summary of access management for Azure resources and a note about MOD Administrator permissions.

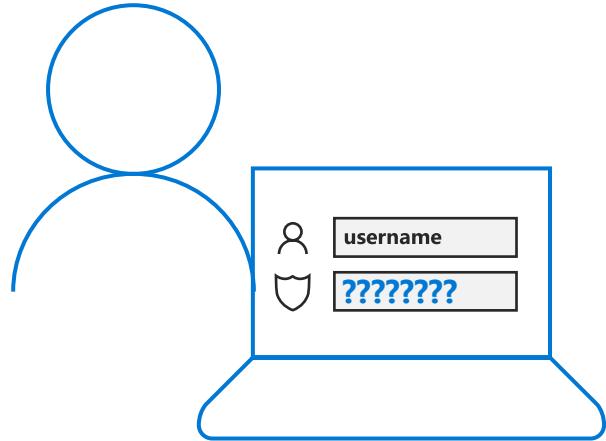
To learn more, see [What are security defaults?](#)

## With Conditional Access Policies

The screenshot shows the 'Conditional Access | Policies' page in the Azure Active Directory admin center. On the right side, a sidebar titled 'MFA for my test...' is open. It includes sections for 'Info' and 'Delete', a note about trying the new configuration, and a form to enter a 'Name' (set to 'MFA for my test users'). Under 'Assignments', it lists 'Users and groups' and 'Cloud apps or actions'. In the 'Conditions' section, it says '0 conditions selected'. The 'Policy Name' section shows 'Baseline Protection' (status: 'We recommend') and 'MFA for my test user'. The 'Access controls' section shows 'Grant' (status: '1 control selected') and 'Session' (status: '0 controls selected'). At the bottom, there's an 'Enable policy' section with a 'Report-only' toggle set to 'On' (highlighted with a red arrow). The main area displays sections for 'Policies', 'Insights and reporting', 'Diagnose and solve problems', 'Manage', and 'Custom controls (Preview)'.

To learn more, see [Quickstart: Require MFA for specific apps with Azure Active Directory Conditional Access](#)

# Empower user self-service to save time and money



- Resolving password issues for users is one of the largest IT costs
- Maximize user flexibility by enabling resets from an intuitive web interface or directly from the Windows login screen

The screenshot shows a 'change password' form on a 'contoso' website. At the top right, there's a navigation bar with three horizontal lines, a bell icon with a '5' notification, and a profile picture for 'Josilyn' with the text 'CONTOSO CLOUD'. The main title is 'change password'. Below it, a note says: 'Strong password required. Enter 8-16 characters. Do not include common words or names. Combine uppercase letters, lowercase letters, numbers, and symbols.' The form fields include 'User ID' (josilync@contoso.com), 'Old password' (empty input field), 'Create new password' (empty input field), 'Password strength' (progress bar indicating strength), and 'Confirm new password' (empty input field). At the bottom are 'submit' and 'cancel' buttons.

# How to enable Self-Service Password Reset?

<https://aad.portal.azure.com/>

The screenshot shows the Azure Active Directory admin center interface. The left sidebar includes links for Dashboard, All services, Favorites (Azure Active Directory, Users, Enterprise applications), Manage (Users, Groups, External Identities, Roles and administrators, Administrative units (Preview), Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings), and a Search bar. The main content area displays the 'Contoso | Overview' page for the Azure Active Directory tenant. It features sections for Overview, Contoso (Tenant ID: M365x038043.onmicrosoft.com, Tenant ID: 657617c0-7d72-4d64-8130-abd7c), Azure AD Connect (Status: Not enabled, Last sync: Sync has never run), and Sign-ins (a line chart showing sign-in activity over time). A callout box highlights the 'Password reset' link in the sidebar.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

&lt;&lt;

Dashboard &gt; Contoso &gt;

## Password reset | Properties

Contoso - Azure Active Directory

&lt;&lt;

Save Discard

Diagnose and solve problems

### Manage

Properties

Authentication methods

Registration

Notifications

Customization

On-premises integration

### Activity

Audit logs

Usage &amp; insights

### Troubleshooting + Support

New support request

Self service password reset enabled

None Selected All

### Select group

SSPRSecurityGroupUsers

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.

[Dashboard](#)[All services](#)**FAVORITES**[Azure Active Directory](#)[Users](#)[Enterprise applications](#)

Dashboard &gt; Contoso &gt;

## Password reset | Authentication methods

Contoso - Azure Active Directory

Save Discard

Diagnose and solve problems

### Manage

Properties

Authentication methods

Registration

Notifications

Customization

On-premises integration

### Activity

Audit logs

Usage &amp; insights

### Troubleshooting + Support

New support request

Number of methods required to reset

1

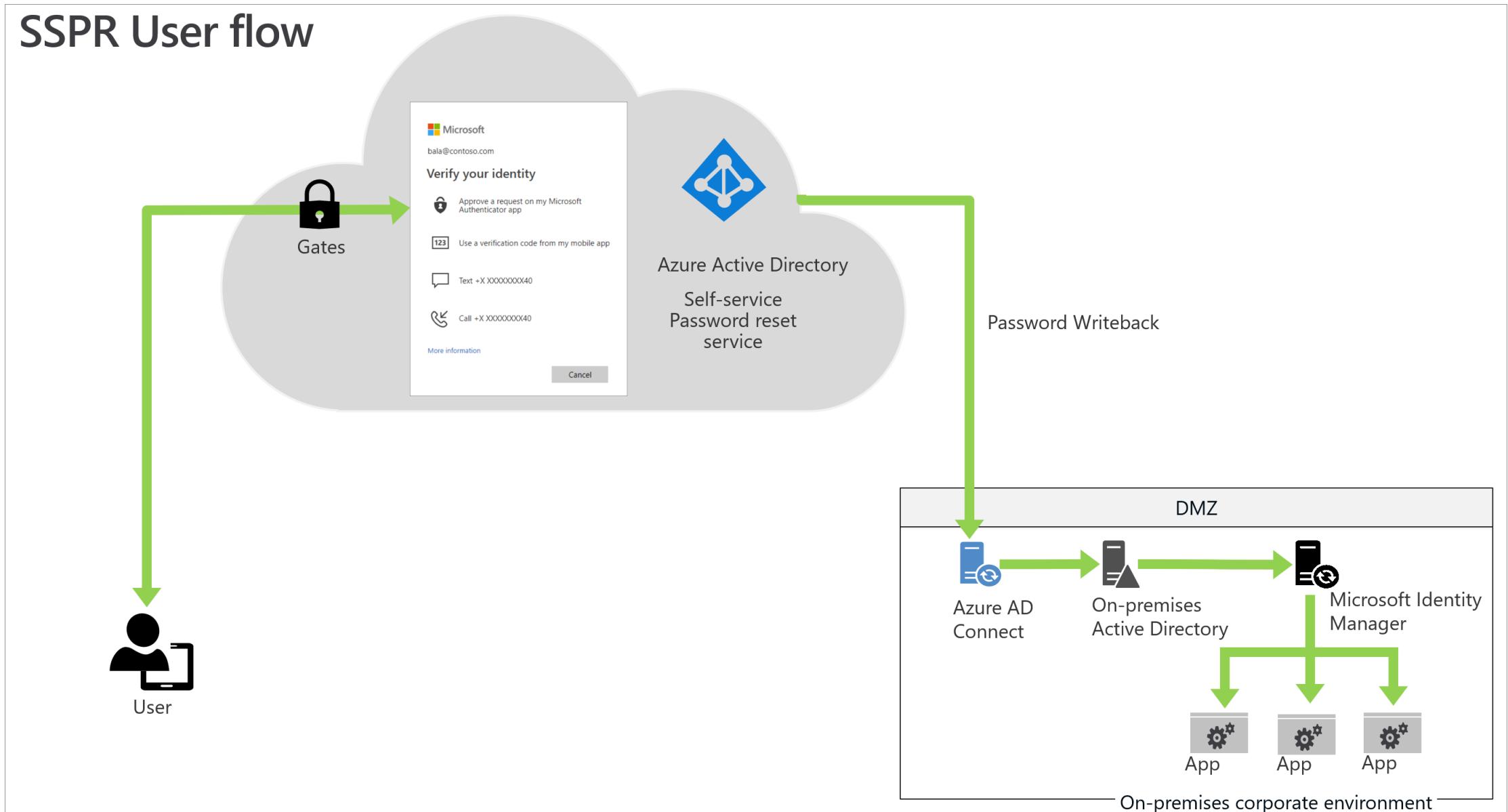
2

Methods available to users

 Mobile app notification Mobile app code Email Mobile phone (SMS only) 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.

# SSPR User flow in a hybrid environment



# Enable combined security information registration

The screenshot shows the Azure Active Directory admin center interface. On the left, the navigation pane includes sections for Dashboard, All services, Favorites (with Azure Active Directory selected), Azure Active Directory, Users, and Enterprise applications. Under User settings, there are links for Properties, Security, Monitoring (Sign-ins, Audit logs, Provisioning logs (Preview), Logs, Diagnostic settings, Workbooks), and Audit logs.

The main content area displays the "Contoso | User settings" page. The breadcrumb navigation shows Dashboard > Contoso | User settings. The title "Azure Active Directory admin center" is at the top of the main content area.

The main content area features a section titled "User feature previews". It contains three items:

- "Users can use preview features for My Apps" with a status of "None" (highlighted by a red arrow).
- "Users can use the combined security information registration experience" with a status of "All" (highlighted by a red arrow).
- "Administrators can access My Staff" with a status of "None".

At the bottom of the "User feature previews" section is a yellow button labeled "Manage user feature preview settings".

To learn more, see [Combined security information registration overview](#)

# Azure AD Password Protection

## Cloud intelligence to ensure strong passwords

- Dynamic banning of passwords based on known bad patterns and those you define.
- Built for hybrid environments.
- Built for secure no-internet zone domain controllers
- Unified admin experience for on-premises and cloud.
- Support for multi-forest environment
- High availability architecture

The screenshot shows the 'Authentication methods - Password Protection' section in the Azure portal. It includes fields for 'Custom smart lockout' (Lockout threshold: 10, Lockout duration in seconds: 60), a 'Custom banned passwords' section (Enforce customlist: Yes, list containing 'identity', 'fabric', and 'contoso'), and a 'Password protection for Windows Server Active Directory' section (Enable password protection on Windows Server Active Directory: Yes, Mode: Enforced).

Home > fab identity > Security > Authentication methods - Password Protection

Authentication methods - Password Protection

fab identity > Azure AD Security

Save Discard

Custom smart lockout

Lockout threshold 10

Lockout duration in seconds 60

Custom banned passwords

Enforce customlist Yes No

Custom banned password list identity fabric contoso

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory Yes No

Mode Enforced Audit

[Microsoft Password Guidance](#)

# Going passwordless is a journey. Start with a plan.

✓ Enable Azure MFA and Self-Service Password Reset in the event users need to fall back to using a password during the Pilot.

✓ MFA all admins

✓ Register all users for MFA

□ Start with a Pilot

Deploy Windows Hello for Business for Windows 10 devices.

Try Microsoft Authenticator phone sign-in for added mobility.

Pilot FIDO2 security keys

Identify and update apps to allow Azure AD authentication

□ (Once possible) disable password-based auth

# Microsoft's password replacement offerings

Standards-based private key authentication that is convenient and more secure than a password



Windows Hello for Business  
(FIDO2)

Microsoft Authenticator

FIDO2 security keys

# Windows Hello

Microsoft's premier  
passwordless experience



# Windows Hello for Business

## User friendly

- Passwordless: Biometrics or a PIN
- SSO with Windows apps using Web Account Manager (SSO) APIs

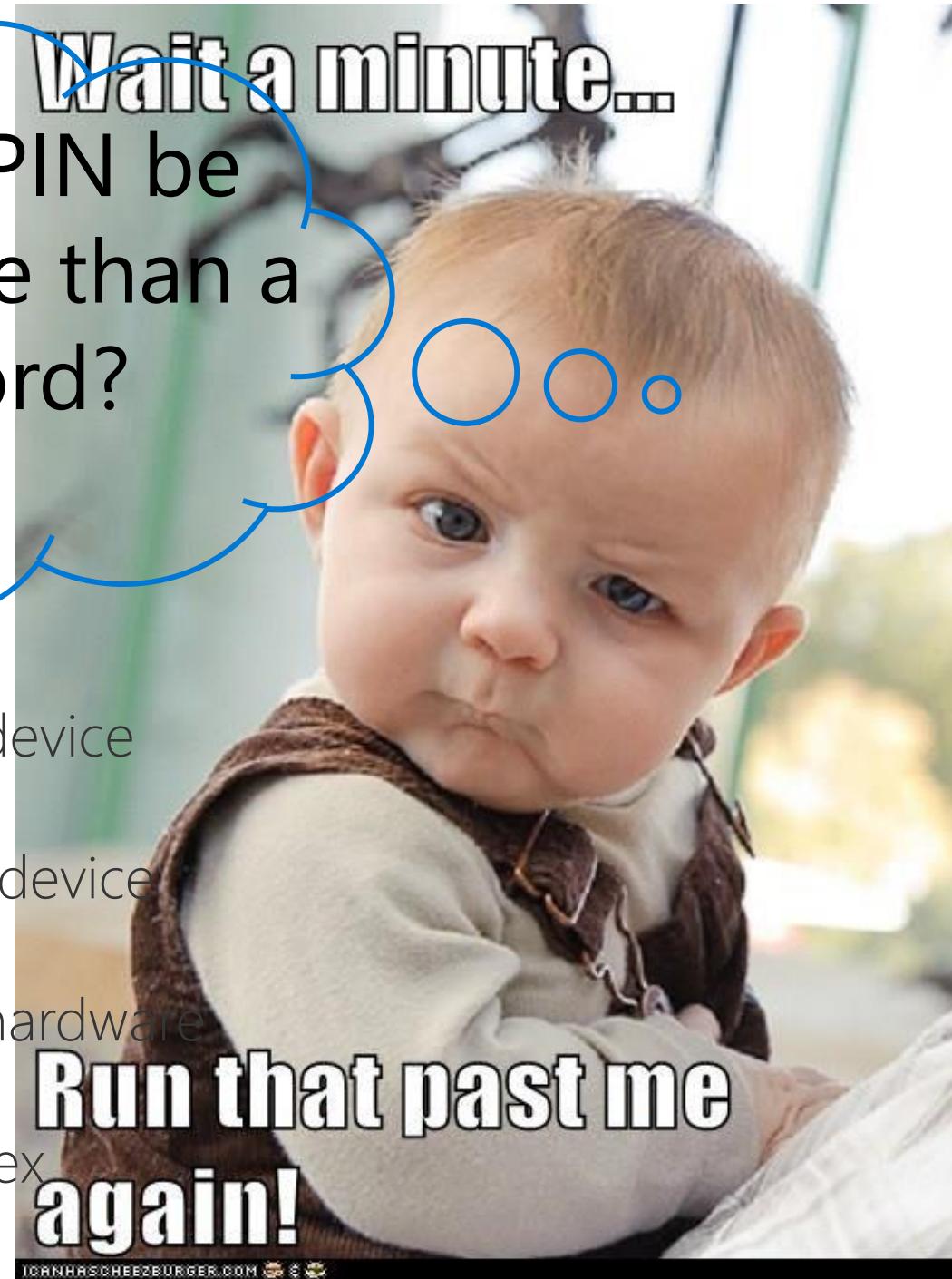
## Enterprise-grade

- Strong two-factor authentication
- Asymmetric key pair auth model
- Can be deployed in cloud, hybrid, or on-prem environments
- Multi account



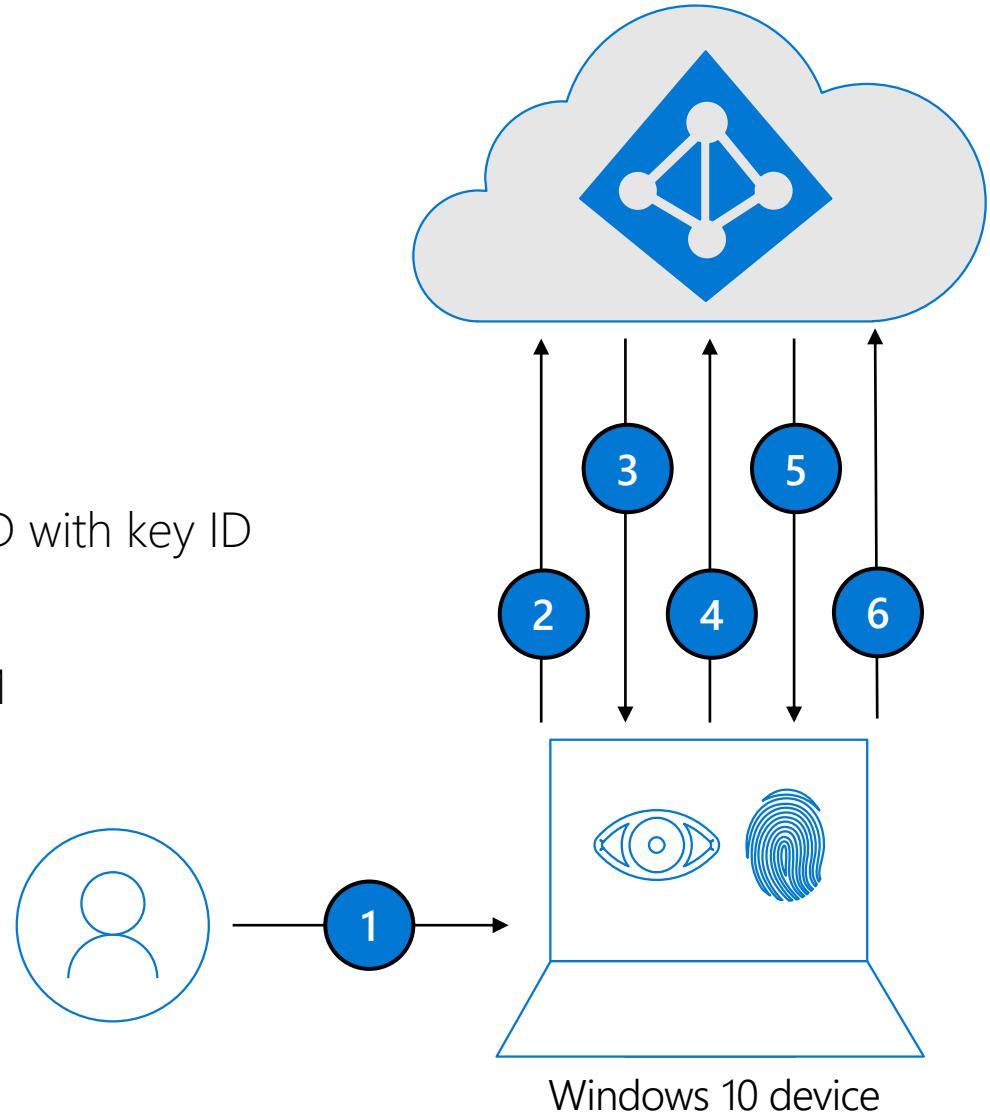
How can PIN be  
more secure than a  
Password?

- PIN is tied to the device
- PIN is local to the device
- PIN is backed by hardware
- PIN can be complex



# Windows 10 Hello for Business sign in

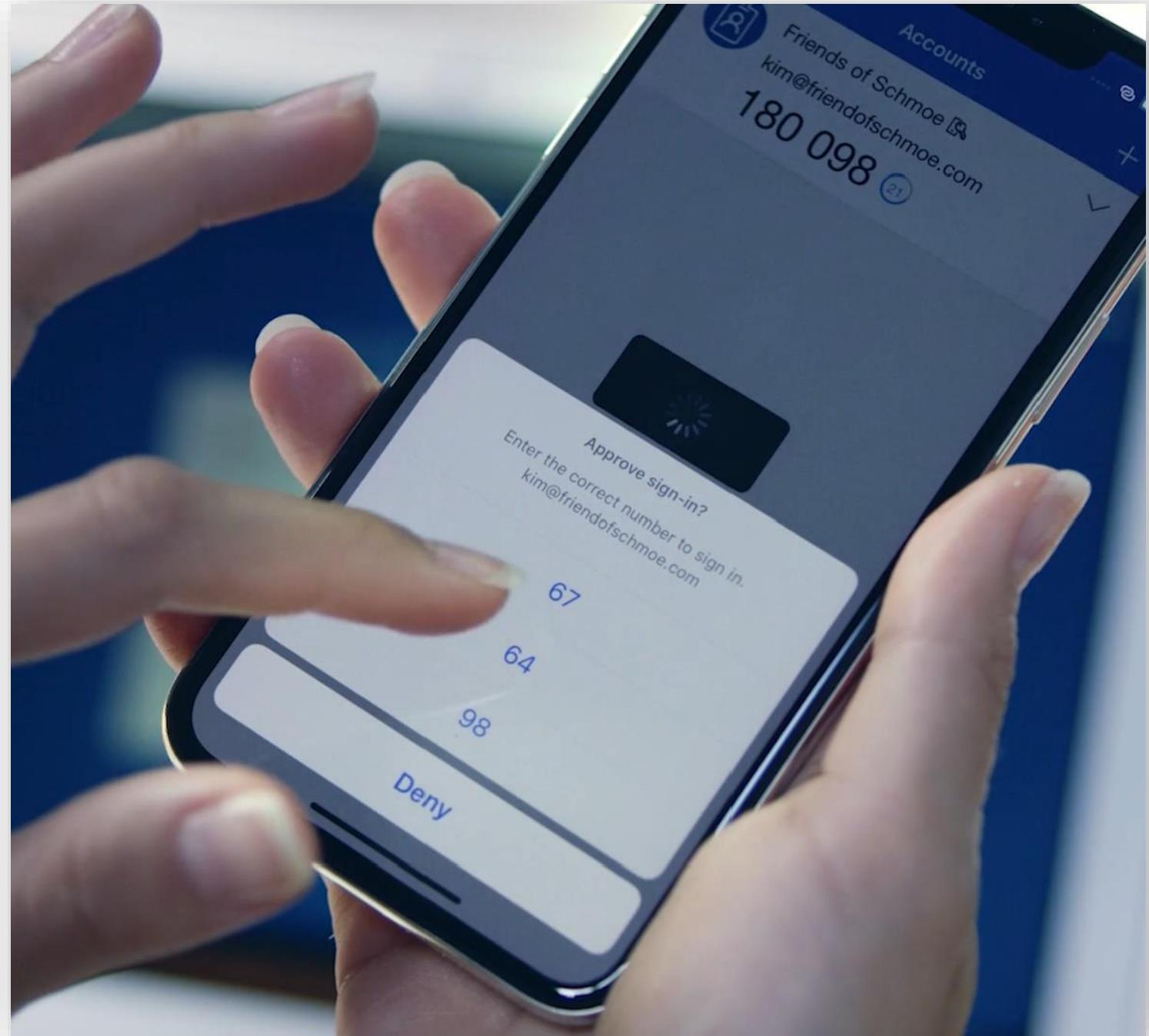
- 1 User sign-in with bio-gesture unlocks TPM holding private key
- 2 Windows sends "hello"
- 3 Azure AD sends back nonce
- 4 Windows uses private key to sign nonce and returns to Azure AD with key ID
- 5 Azure AD returns PRT + encrypted session key protected in TPM
- 6 Windows returns the signed PRT and derived session key to Azure AD to verify





# Microsoft Authenticator

Microsoft's passwordless  
anywhere solution



# Microsoft Authenticator

## Overview

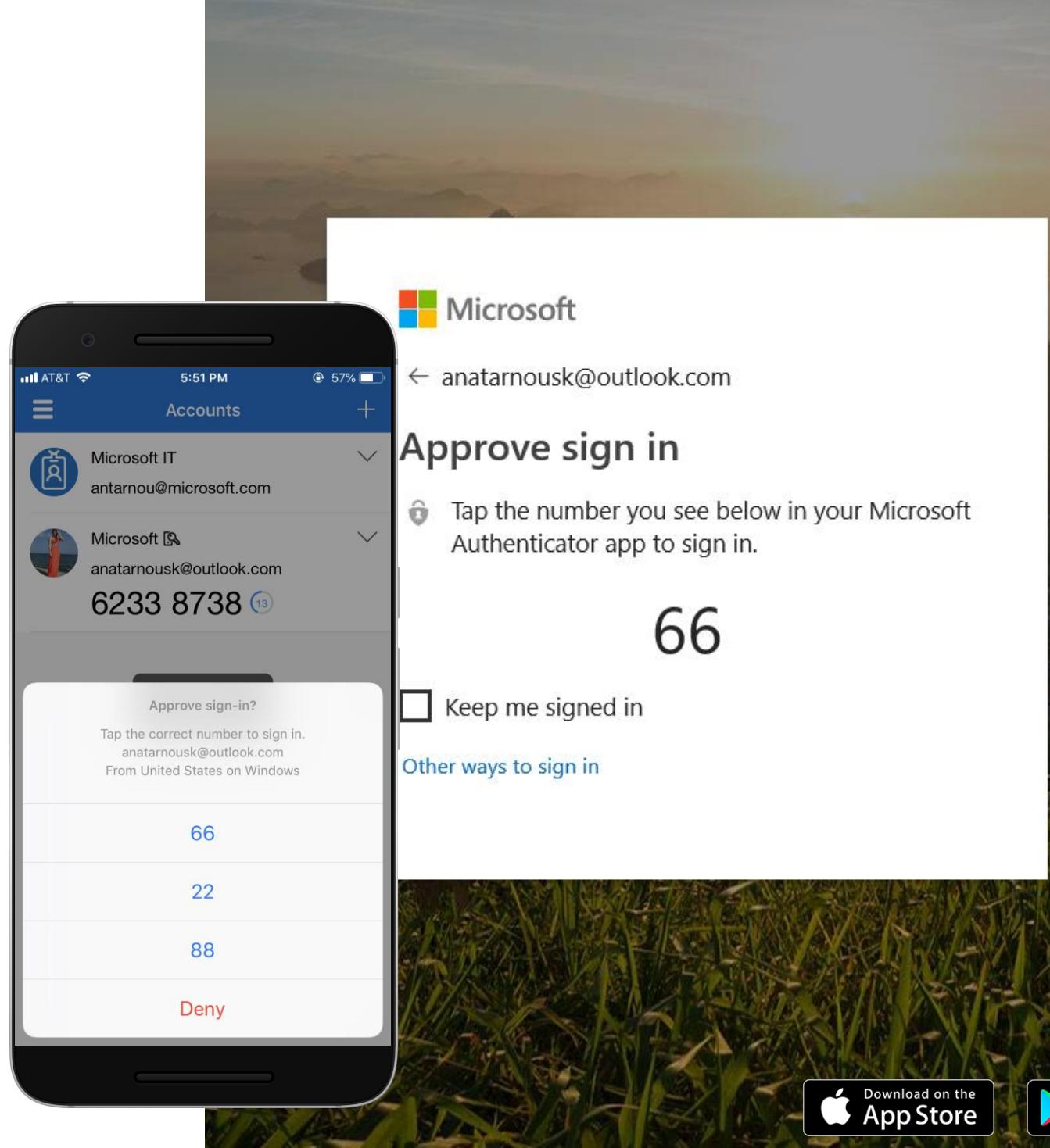
- Standard based MFA
- Multi-account

## Windows 10

- Passwordless authentication – i.e. device registration in OOBE, Windows Hello provisioning

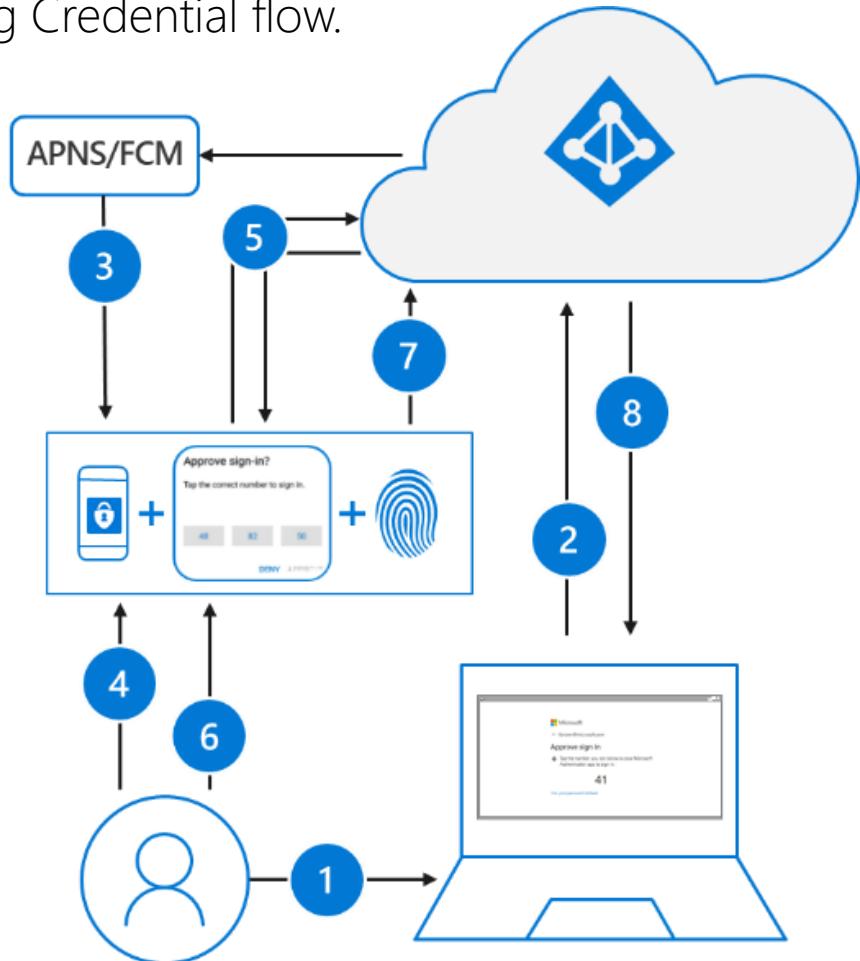
## Mobile

- SSO to native mobile apps



# How does Authenticator Passwordless Sign In work?

- 1 The user enters their username.
- 2 Azure AD detects that the user has a strong credential and starts the Strong Credential flow.
- 3 Notification is sent to the app via Apple Push Notification Service (APNS) on iOS devices, or via Firebase Cloud Messaging (FCM) on Android devices.
- 4 The user receives the push notification and opens the app.
- 5 The app calls Azure AD and receives a proof-of-presence challenge and nonce.
- 6 The user completes the challenge by entering their biometric or PIN to unlock private key.
- 7 The nonce is signed with the private key and sent back to Azure AD.
- 8 Azure AD performs public/private key validation and returns a token.



# How to enable authentication with Microsoft Authenticator?

The screenshot shows the Azure Active Directory admin center interface across three main sections: the left navigation bar, the central dashboard, and a detailed configuration page.

**Left Navigation Bar:** Shows the "Azure Active Directory admin center" header, a "Contoso | Overview" section, and a "Security" section highlighted with a yellow box. Other menu items include Dashboard, All services, Favorites, Azure Active Directory, Users, Enterprise applications, and Monitoring.

**Central Dashboard:** Shows the "Azure Active Directory admin center" header, a "Contoso | Overview" section, and a "Security" section. The "Authentication methods" link is highlighted with a yellow box.

**Detailed Configuration Page:** The "Authentication methods | Authentication method policy (Preview)" page. It includes a note to "Click here to enable users for the combined security info registration experience." Below is a table for managing authentication methods:

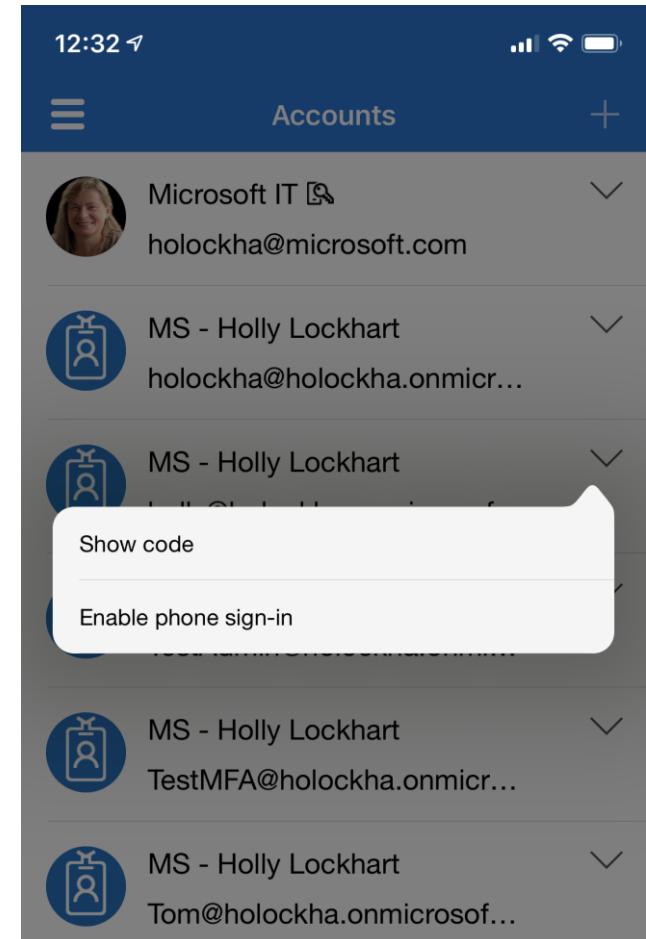
Method	Target	Enabled
FIDO2 Security Key	1 user	No
Microsoft Authenticator passwordless sign-in	1 user	Yes
Text message	1 user	Yes

Below the table is a "Microsoft Authenticator passwordless sign-in settings" section with "Save" and "Discard" buttons. A note states: "Your tenant must be enabled for MFA with push notifications through the Microsoft Authenticator app in order to use this method." At the bottom, there are "ENABLE" and "TARGET" buttons set to "Yes" and "All users". The "USE FOR" dropdown is set to "Sign in" and "Strong".

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>

# How does the end-user enable? 3 steps:

1. Latest version of Microsoft Authenticator installed on devices running iOS 8.0 or greater, or Android 6.0 or greater.
2. Enroll in Azure Multi-Factor Authentication
3. Choose the drop-down arrow next to the account name, and then select Enable phone sign-in.



# FIDO2 Security Keys

Password-less security devices  
based on the FIDO2 standard

Azure Active Directory account  
*Public Preview*



# What will be included?



**Passwordless sign-in using FIDO2 security keys**



- Azure Active Directory Joined (AADJ)
- Hybrid AADJ Windows 10 devices



**Seamless SSO to Cloud and on-premises resources**

# What is FIDO2?

## FIDO Alliance

- Launched in February 2013
- Develop and promote authentication standards that help reduce the world's over-reliance on passwords

## WebAuthn

- Extensible web authentication API

## CTAP2

- Extensible client-to-authenticator protocol



# Passwordless with FIDO2 security keys

Microsoft uses open standards that work with innovative offerings from partners

USB/NFC Key



USB Biometric Key



NFC Badges & Wearables



# Passwordless with FIDO2 security keys

Provider	Contact
Yubico	<a href="https://www.yubico.com/support/contact/">https://www.yubico.com/support/contact/</a>
Feitian	<a href="https://www.ftsafe.com/about/Contact_Us">https://www.ftsafe.com/about/Contact_Us</a>
HID	<a href="https://www.hidglobal.com/contact-us">https://www.hidglobal.com/contact-us</a>
Ensurity	<a href="https://www.ensurity.com/contact">https://www.ensurity.com/contact</a>
eWBM	<a href="https://www.ewbm.com/support">https://www.ewbm.com/support</a>
AuthenTrend	<a href="https://authentrend.com/about-us/#pg-35-3">https://authentrend.com/about-us/#pg-35-3</a>
Gemalto (Thales Group)	<a href="https://safenet.gemalto.com/multi-factor-authentication/authenticators/passwordless-authentication/">https://safenet.gemalto.com/multi-factor-authentication/authenticators/passwordless-authentication/</a>
OneSpan Inc.	<a href="https://www.onespan.com/products/fido">https://www.onespan.com/products/fido</a>
IDmelon Technologies Inc.	<a href="https://www.idmelon.com/#idmelon">https://www.idmelon.com/#idmelon</a>

# Secure Authentication Flow

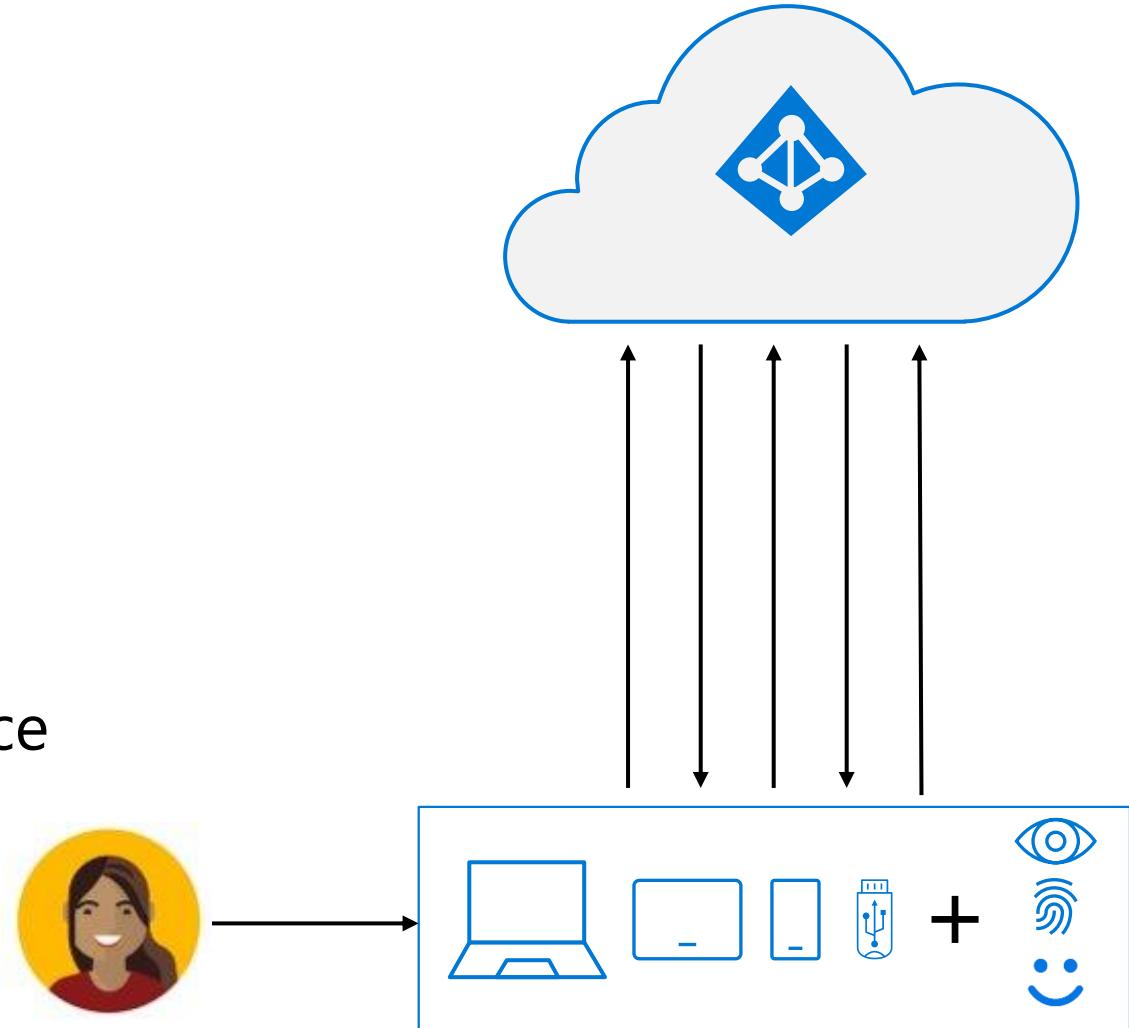
A simple, common architecture

Based on public-key technology

Private-keys are securely stored  
on the device

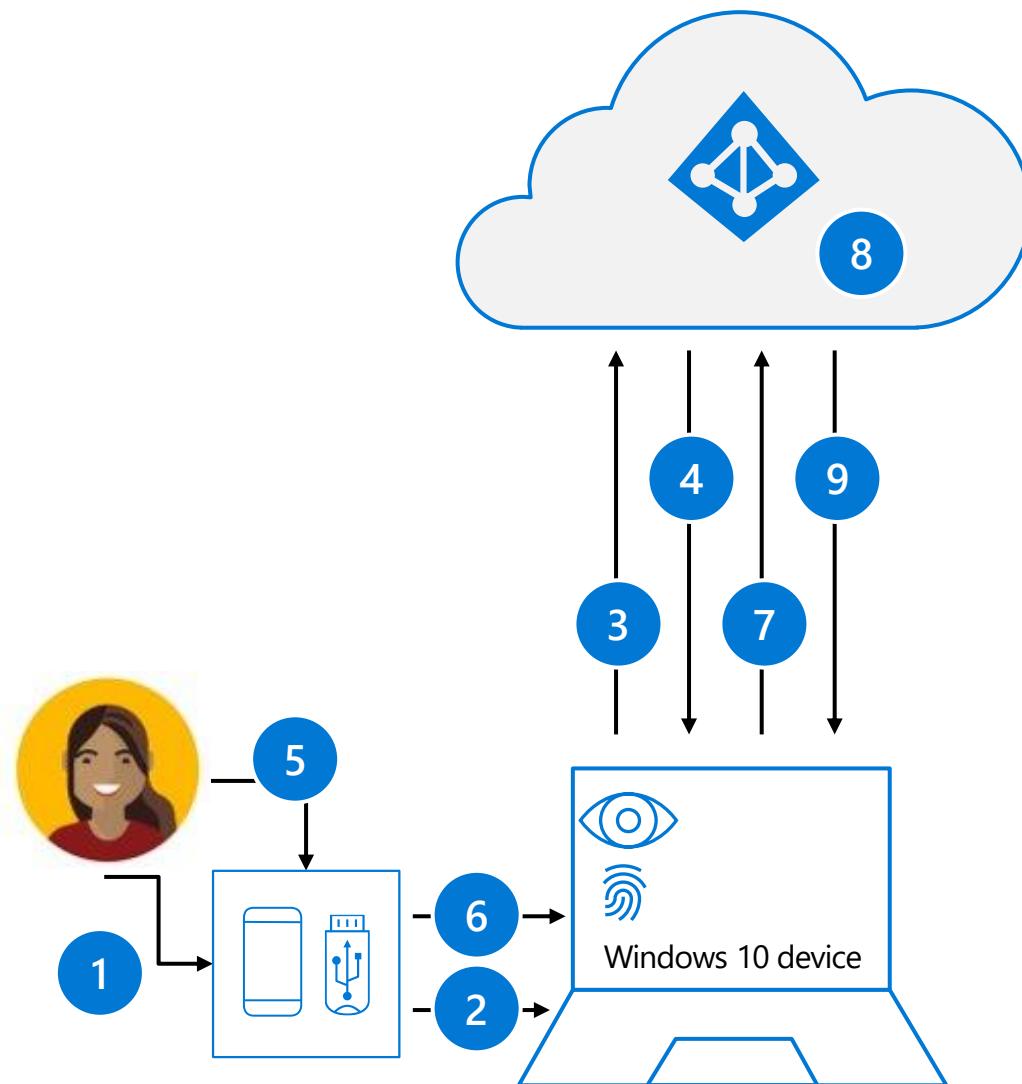
Requires a local gesture  
(e.g., biometric, PIN)

Private-keys are bound to a single device  
and never shared

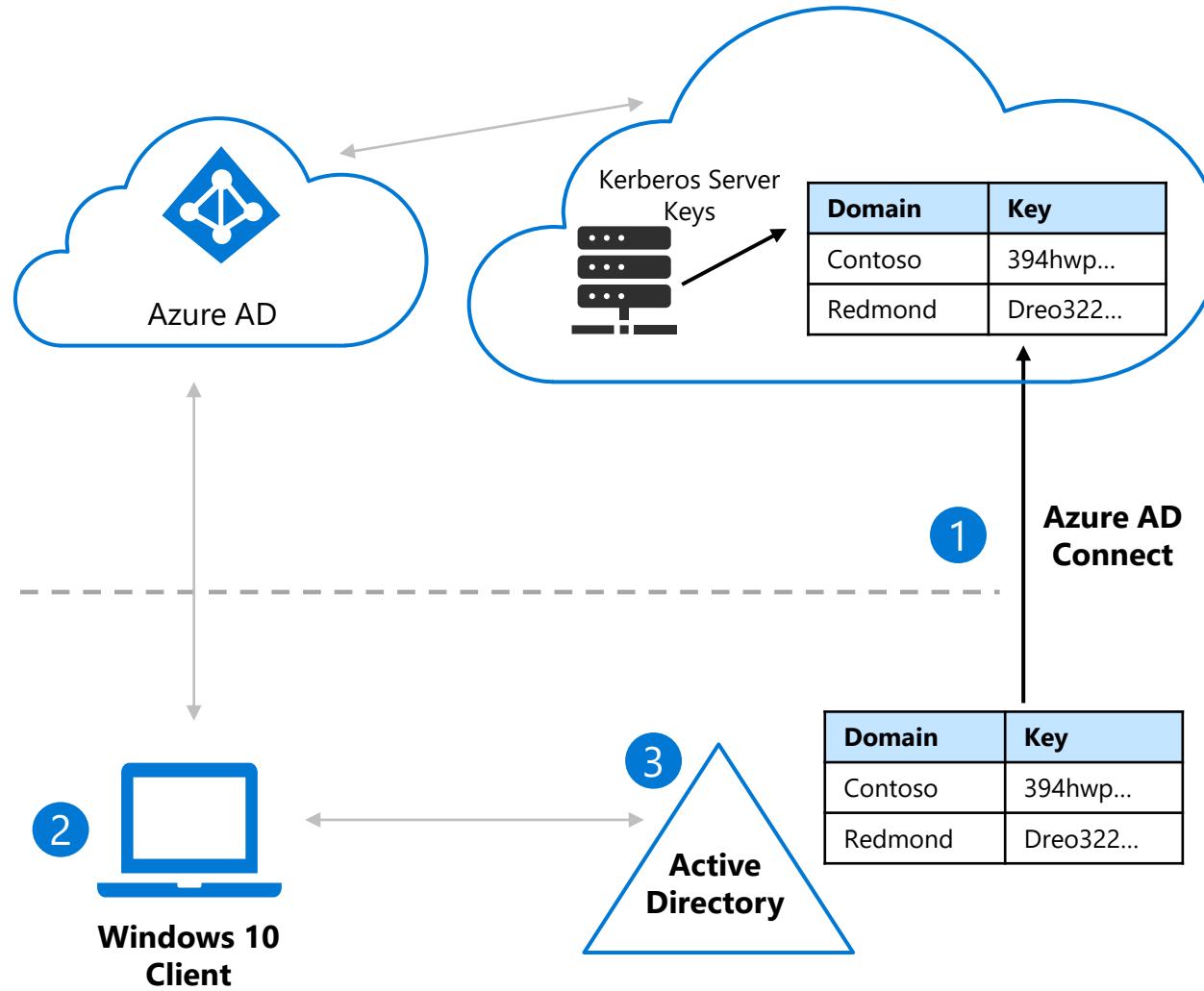


# Strong Authentication with FIDO2 security key

- 1 User plugs FIDO2 security key into computer
- 2 Windows detects FIDO2 security key
- 3 Windows device sends auth request
- 4 Azure AD sends back nonce
- 5 User completes gesture to unlock private key stored in security key's secure enclave
- 6 FIDO2 security key signs nonce with private key
- 7 PRT token request with signed nonce is sent to Azure AD
- 8 Azure AD verifies FIDO key signature
- 9 Azure AD returns PRT to enable access to cloud resources

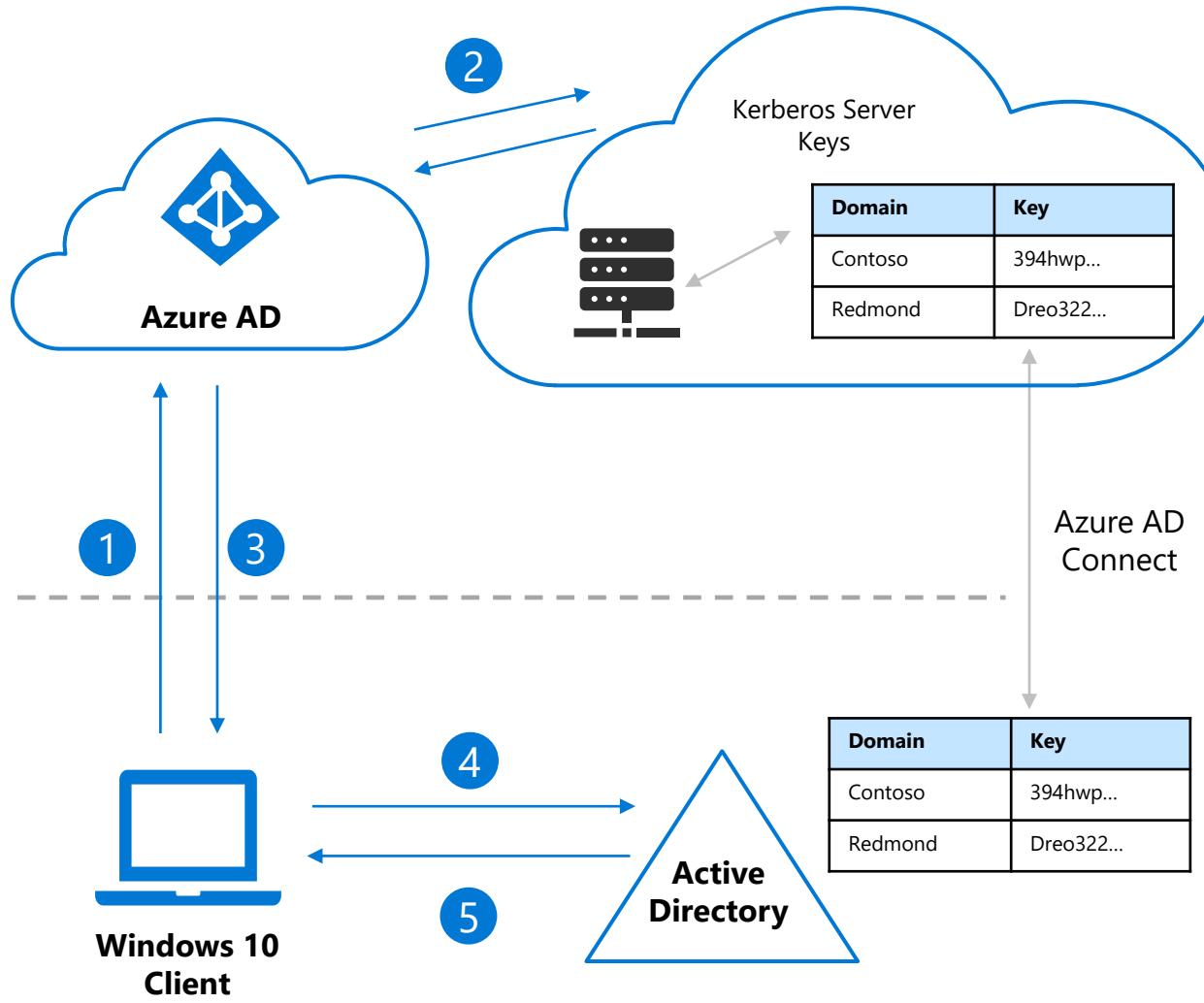


# Deployment Components



- 1 Latest version of AAD Connect
- 2 Latest Windows Insider Build
- 3 Patch for Domain Controller (Server 2016/2019)

# Authentication



- 1 User authenticates to Azure AD with a FIDO2 security key.
- 2 Azure AD checks the tenant for a Kerberos server key matching the user's on-premises AD Domain.
  - Azure AD Generates a partial Kerberos Ticket Granting Ticket (TGT) for the users on-premises AD Domain. The TGT contains only the user SID. No authorization data (groups) are included in the TGT.
- 3 The partial TGT is returned to the Windows along with Azure AD Primary Refresh Token (PRT).
- 4 Windows contacts on-premises AD Domain Controller and trades the partial TGT for a full TGT.
- 5 Windows now has Azure AD PRT and a full Active Directory TGT.

# **DEMO**

# Azure AD Changes to Enable FIDO2 (1 of 2)

- Enable combined security information registration
- Sign into the Azure portal as a user administrator or global administrator.
- Go to **Azure Active Directory > User settings > Manage user feature preview settings**
- Under **Users can use preview features for registering and managing security info - enhanced**, choose to enable for a **Selected** group of users or for **All** users.
- Click **Save** to save changes.

# Azure AD Changes to Enable FIDO2 (2 of 2)

- Enable FIDO2 authentication method
  - Sign into the Azure portal as a global administrator

Browse to **Azure Active Directory > Security > Authentication methods > Authentication method policy (Preview)**

- Select **FIDO2 Security Key**
- In the bottom pane, set **ENABLE** to **Yes**
- In the bottom pane, set the **TARGET** to **Select users** (based on test user group)
- **Do not change any other settings while this feature is in preview!**
- **Save** the FIDO2 Security Key method

## Authentication methods

Wingtiptoys – Azure AD Security



- Usage and insights
- Getting started

## MANAGE

- Authentication methods

- Password protection (Preview)

## ACTIVITY

- Audit logs

## TROUBLESHOOTING + SUPPORT

- Troubleshoot

- New support request

 Documentation

## Allowed methods

= Recommended

METHOD	TARGET	ENABLED	
Password	All users	Yes	
Phone call	All users	Yes	
Microsoft Authenticator app	1 group	Yes	
Verification code – authenticator app		No	
Verification code – hardware token		No	
Text message		No	
FIDO		No	
PIN		No	
Email address		No	
Security questions	5 groups	Yes	



Bob, the IT admin wants to enable FIDO in their tenant. So Bob goes to the new cred management experience and clicks FIDO

## Authentication methods

Wingtiptoys – Azure AD Security



- Usage and insights
- Getting started

## MANAGE

- Authentication methods

- Password protection (Preview)

## ACTIVITY

- Audit logs

## TROUBLESHOOTING + SUPPORT

- Troubleshoot

- New support request

 Documentation

## Allowed methods

= Recommended

METHOD	TARGET	ENABLED
Password	All users	Yes
Phone call	All users	Yes
Microsoft Authenticator app	1 group	Yes

## FIDO2 Security Keys

Save

Discard

## ENABLE

Yes No

## TARGET USERS

- All users
- Select users

[+ add users and group](#)

## NAME

Fido Pilot group

## REGISTRATION

Required

## GENERAL

Allow self-service set-up for groups

Yes No

## Enforce Attestation

Yes No

## KEY RESTRICTION POLICY

Enforce key restrictions

Yes No

Restrict specific keys

Allow Block

[+ add AAGUID](#)

# Enable security keys for Windows sign in

Windows Hello for Business settings lets users access their devices using a gesture, such as biometric authentication, or a PIN. [Learn more](#)

Configure settings for enrolled Windows 10, Windows 10 Mobile and later.

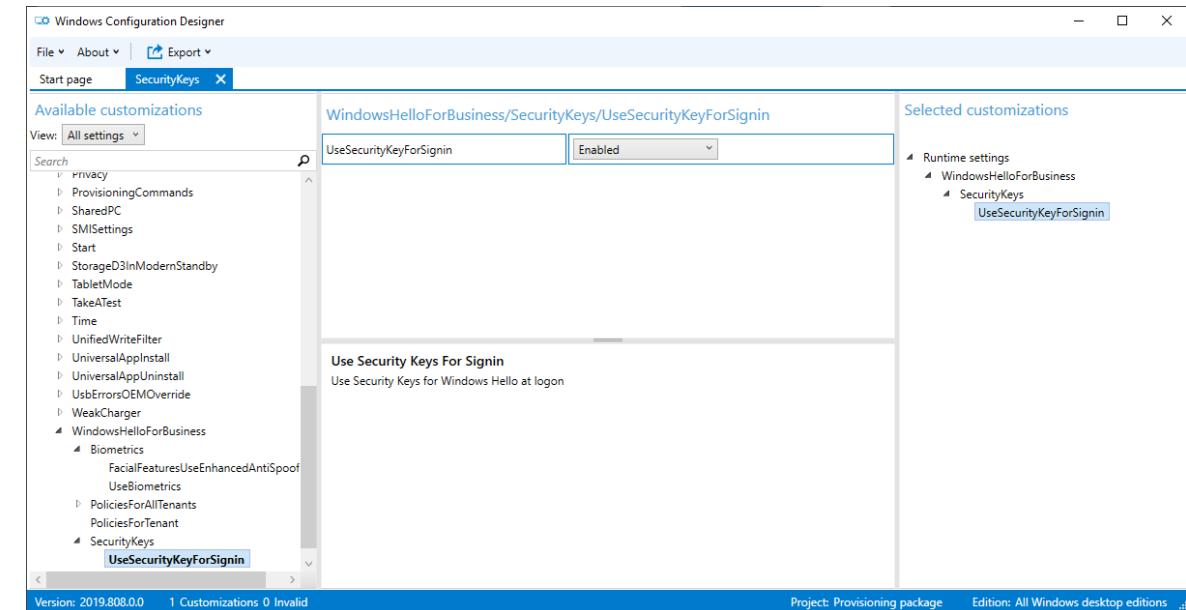
Name  
All users and all devices

Description  
This is the default Windows Hello for Business configuration applied with the lowest priority to all users regardless of group membership.

Configure Windows Hello for Business: ⓘ Not configured

Use security keys for sign-in: ⓘ Enabled

**Enable FIDO2 Credential Provider via Intune**



**Or Enable FIDO2 Credential Provider via Windows Configuration Designer**

My Sign-ins

https://mysignins.microsoft.com/security-info

My Sign-ins

Overview Security info Organizations Devices Privacy

You can now enable your phone number (+32 4...) to be used as a username for sign in. Enable

## Security info

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

**Default sign-in method:** Microsoft Authenticator - notification [Change](#)

Add method			
	Alternate phone	+32	<a href="#">Change</a> <a href="#">Delete</a>
	Phone	+32	<a href="#">Change</a> <a href="#">Delete</a>
	Microsoft Authenticator	H's iPhone 11 Pro	<a href="#">Delete</a>
	Microsoft Authenticator	Hans's iPad Pro	<a href="#">Delete</a>
	Microsoft Authenticator	Hans's iPhone 8	<a href="#">Delete</a>
	Microsoft Authenticator	SM-T810	<a href="#">Delete</a>
	Security key	Feitian K26 (USB-C)	<a href="#">Delete</a>
	Security key	Security Key by Yubico	<a href="#">Delete</a>
	Security key	Feitian K27 (USB-A)	<a href="#">Delete</a>
	Email	hans.hofkens@microsoft.com	<a href="#">Change</a> <a href="#">Delete</a>

New tab x + aad.portal.azure.com InPrivate

CHECK OUT SETUP - OneNote... SETUP - My machin... Other favorites

# InPrivate Browsing

InPrivate search with Microsoft Bing

What InPrivate Browsing does

- Deletes your browsing info when you close all InPrivate windows
- Saves favorites and downloads (but not download history)
- Prevents Microsoft Bing searches from being associated with you

What InPrivate Browsing doesn't do

- Hide your browsing from your school, employer, or internet service provider
- Give you additional protection from [tracking](#) by default
- Add additional protection to what's available in normal browsing

More details

This site uses cookies for analytics, personalized content and ads. By continuing to browse this site, you agree to this use.

[Learn more](#)

## Microsoft Azure

 Microsoft

### Sign in

to continue to Microsoft Azure

Email, phone, or Skype

---

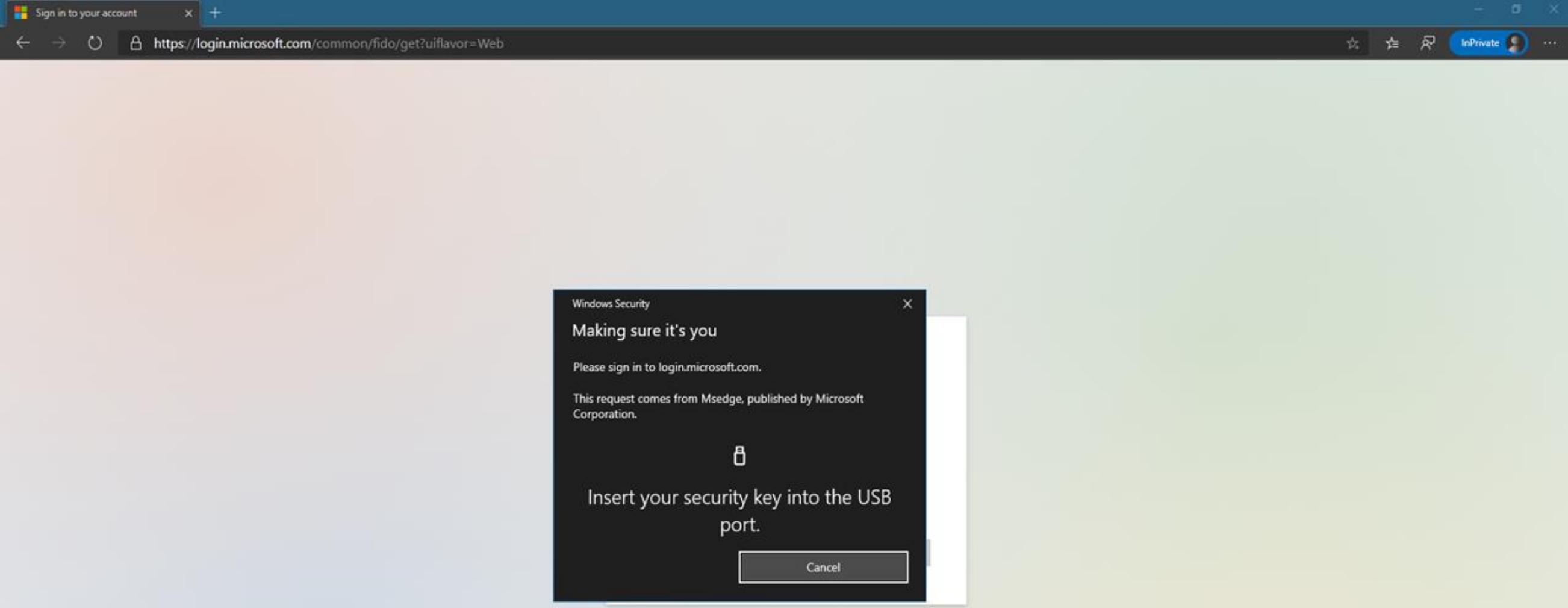
No account? [Create one!](#)

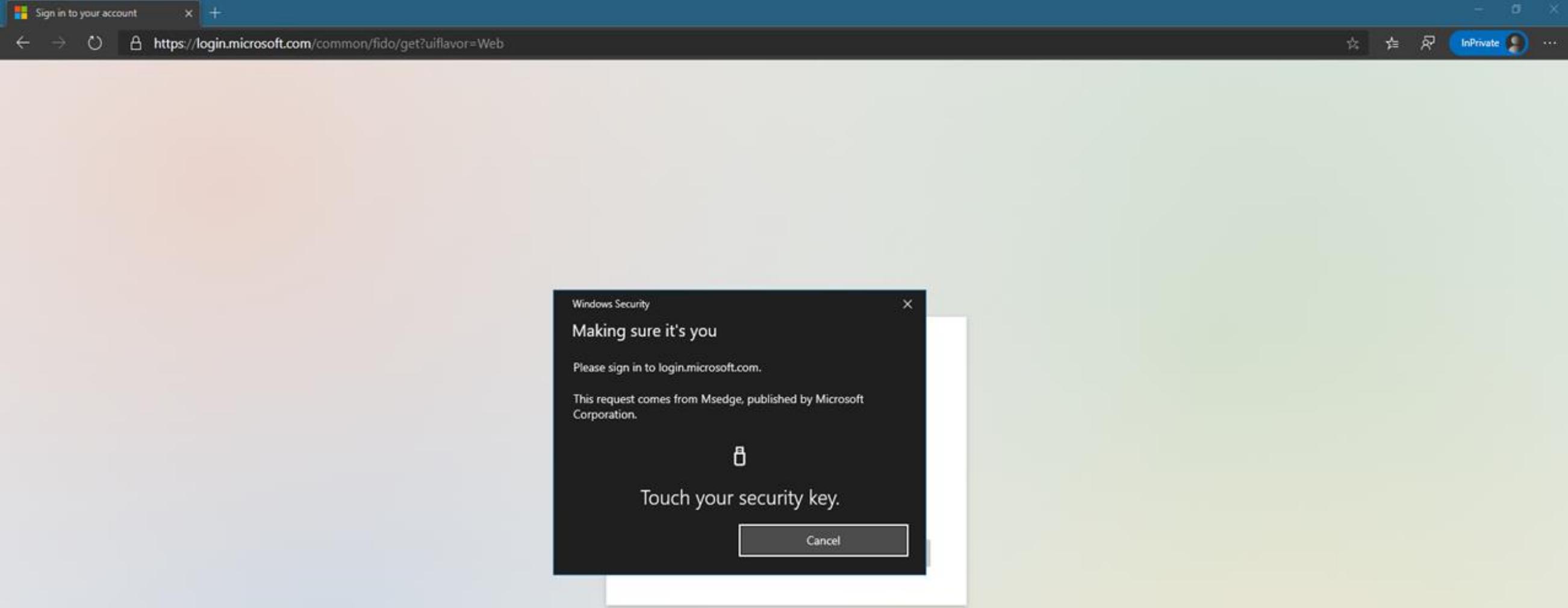
[Can't access your account?](#)

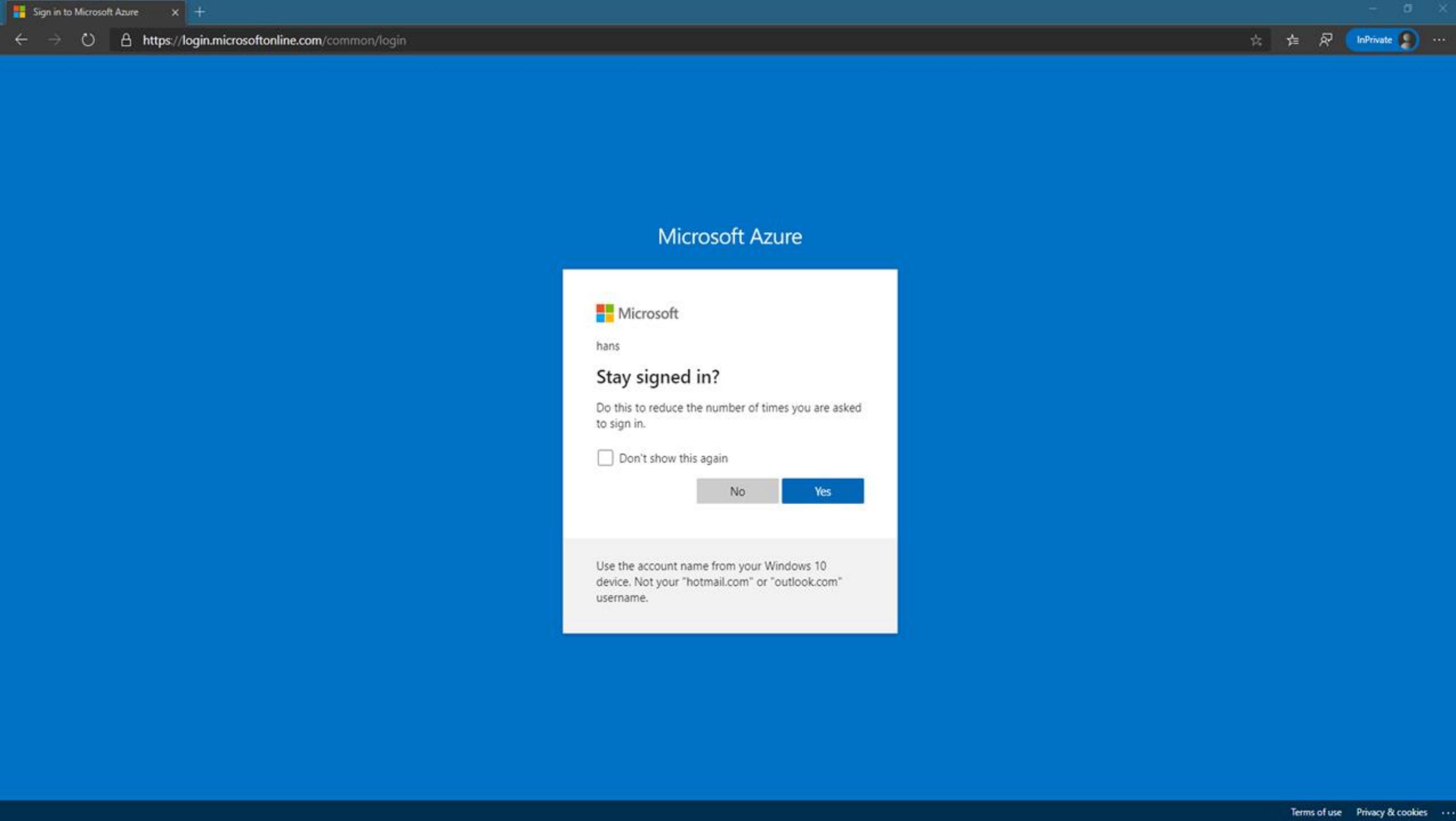
[Sign in with a security key](#) (?)

[Next](#)

 Sign in with GitHub







Dashboard - Azure Active Direct... + https://aad.portal.azure.com InPrivate

# Azure Active Directory admin center

Dashboard Hans Welcome to the Azure AD admin center

Azure AD helps you protect your business and empower your users.

Learn more about Azure AD

Risky users

Access reviews of

Access reviews status

Azure AD Premium P2

Guest members: 2  
Members: 0  
Guest app access: 0  
App access: 0

2

Quick tasks

Add a user  
Add a guest user  
Add a group  
Find a user  
Find a group  
Find an enterprise app

Proxy

Enterprise Mobility + Security

Azure Active Directory  
Azure Information Protection (formerly RMS)  
Intune  
Advanced Threat Analytics

Azure portal

portal.azure.com

What's new

Azure AD makes the leaders quadrant in Gartner's 2017 Magic Quadrant for Access Management

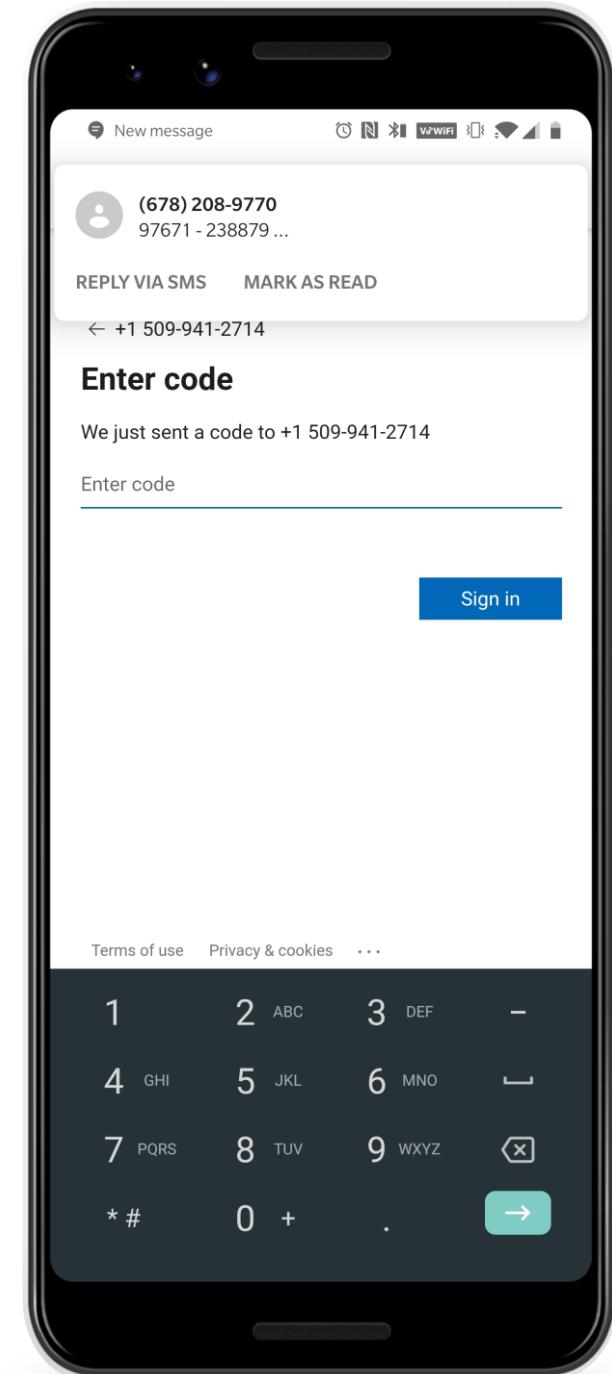
Audit Logs

View activity

The new Azure AD admin console is GA

# New! SMS Sign-In

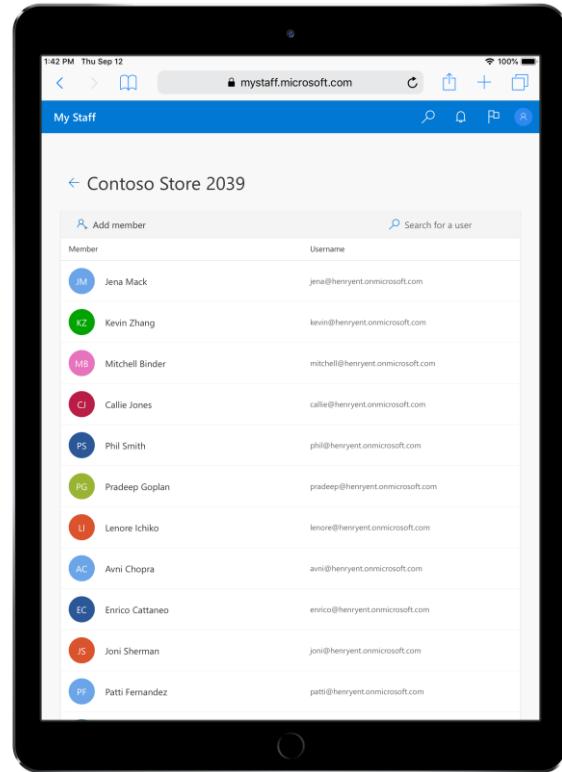
*Public Preview*



# Azure AD • Firstline Worker

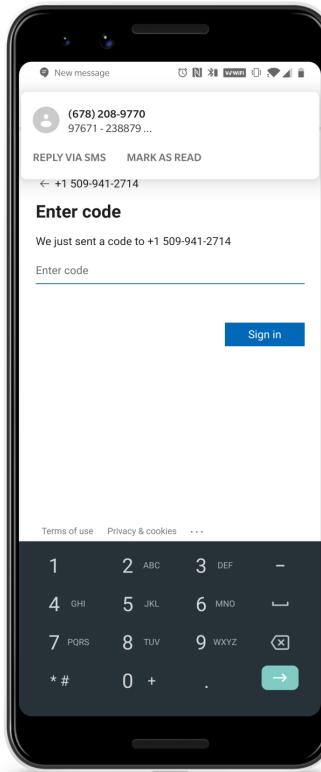


Public Preview



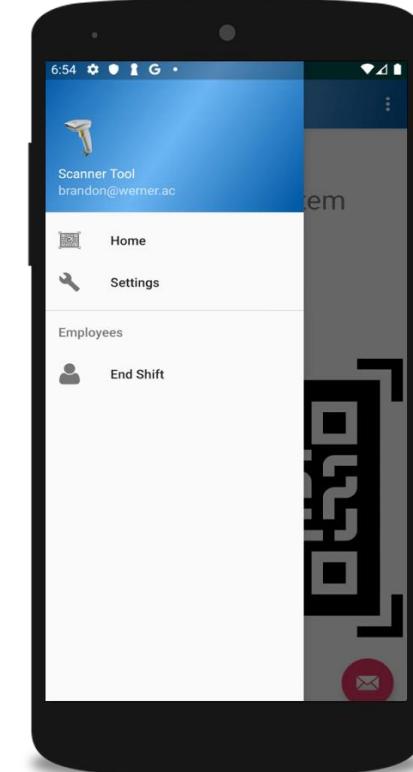
## My Staff

Managers of FLW's can provision users, reset passwords, and add phone numbers.



## SMS Sign-in

FLWs can use their phone number as their ID and a code to sign in.



## Global sign out

FLWs that use shared devices can sign out of all their applications

# How to enable SMS Sign-In?

The screenshot shows three main sections of the Azure Active Directory admin center:

- Left Panel (Navigation):** Shows the 'Security | Getting started' section with links for Conditional Access, Identity Protection, Security Center, Identity Secure Score, Named locations, Authentication methods (which is highlighted), and MFA.
- Middle Panel (Documentation):** Shows the 'Documentation' section with a list of Azure Active Directory offers, including Azure AD Conditional Access, Azure AD Identity Protection, Azure Security Center, Identity Secure Score, Named locations, Authentication methods, and Multi Factor Authentication.
- Right Panel (Authentication methods policy):** Shows the 'Authentication methods | Authentication method policy (Preview)' screen. It displays a table of authentication methods:

Method	Target	Enabled
FIDO2 Security Key		No
Microsoft Authenticator passwordless sign-in	1 user	Yes
<b>Text message</b>	1 user	Yes

A yellow box highlights the 'Text message' row. Below the table, there are 'Text message settings' with 'Save' and 'Discard' buttons, and options to 'ENABLE Yes' or 'No' and 'TARGET All users' or 'Select users'. A note says 'Click here to enable users for the combined security info registration experience.' A 'USE FOR:' dropdown is set to 'Sign in'. At the bottom, a table lists users: Alex Wilber (User, checked for sign-in).

## Limitations (during public preview):

- SMS-based authentication isn't currently compatible with Azure Multi-Factor Authentication.
- With the exception of Teams, SMS-based authentication isn't currently compatible with native Office applications.
- SMS-based authentication isn't recommended for B2B accounts.
- Federated users won't authenticate in the home tenant. They only authenticate in the cloud.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-sms-signin>

# SMS sign-in is risky – Monitoring is key

## Azure AD sign-in logs

The screenshot shows the Microsoft Azure Sign-ins log interface. It displays a table of sign-in events from the last 24 hours. The columns include Date, Request ID, User, Application, Status, and IP address. The data shows several successful sign-ins for a user named Alex Wilber, primarily using Office 365 services like SharePoint and Exchange.

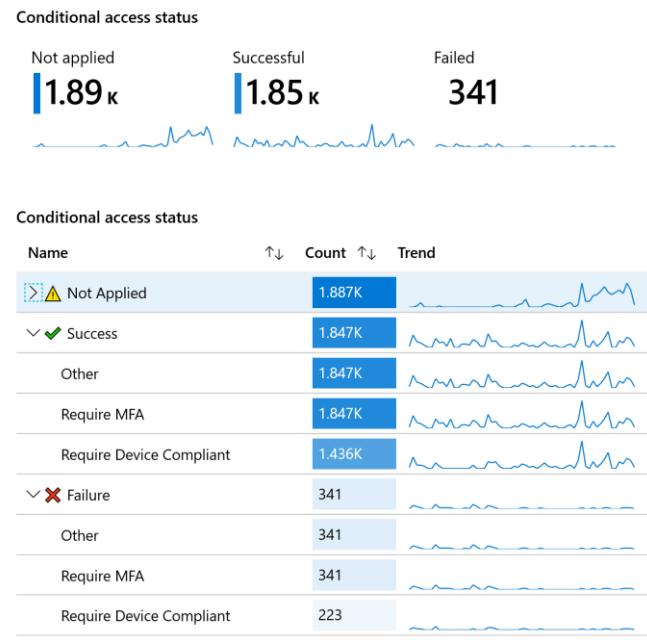
Date	Request ID	User	Application	Status	IP address
5/19/2020, 11:17:51 A...	fb4184eb-478e-448b...	Alex Wilber	Office 365 SharePoint ...	Success	2.110.116.163
5/19/2020, 11:17:50 A...	ee4252c0-3617-48e4...	Alex Wilber	Office 365 SharePoint ...	Success	2.110.116.163
5/19/2020, 11:17:48 A...	ee4252c0-3617-48e4...	Alex Wilber	Office365 Shell WCSS...	Success	2.110.116.163
5/19/2020, 11:17:48 A...	f1e2aafb-a598-4463...	Alex Wilber	Office365 Shell WCSS...	Success	2.110.116.163
5/19/2020, 11:17:47 A...	3834b8bc-9ed1-4eb2...	Alex Wilber	Office 365 Exchange ...	Success	2.110.116.163
5/19/2020, 11:17:46 A...	45425d96-4242-4488...	Alex Wilber	Office365 Shell WCSS...	Success	2.110.116.163
5/19/2020, 11:17:42 A...	c94016fd-2ae4-b71...	Alex Wilber	O365 Suite UX	Success	2.110.116.163
5/19/2020, 11:17:35 A...	45425d96-4242-4488...	Alex Wilber	O365 Suite UX	Interrupted	2.110.116.163

Export Queries to use in Azure  
Sentinel

## Azure Monitor built-in dashboards

The screenshot shows the Azure Monitor Log query editor. It displays a query for 'SigninLogs' filtered by specific application display names and error codes. The query uses 'extend' and 'case' statements to map conditional access status codes to descriptive names like 'Success', 'Failure', 'Not Applied', and 'Disabled'. The results are presented in a table and a chart.

```
let data = SigninLogs
| where AppDisplayName in ('*') or '*' in ('*')
| where UserDisplayName in ('*') or '*' in ('*')
| extend errorCode = toint(Status.errorCode)
| extend Reason = tostring(Status.failureReason)
| extend CAStatus = case(
    ConditionalAccessStatus == "success", "Success",
    ConditionalAccessStatus == "failure", "Failure",
    ConditionalAccessStatus == "notApplied", "Not Applied",
    ConditionalAccessStatus == "", "Not Applied",
    "Disabled"
) | mvexpand ConditionalAccessPolicies
```



# Going passwordless is a journey. Start with a plan.

- ✓ Enable Azure MFA and Self-Service Password Reset in the event users need to fall back to using a password during the Pilot.
  - ✓ MFA all admins
  - ✓ Register all users for MFA
- ✓ Start with a Pilot
  - Deploy Windows Hello for Business for Windows 10 devices.
  - Try Microsoft Authenticator phone sign-in for added mobility.
  - Pilot FIDO2 security keys
  - Identify and update apps to allow Azure AD authentication
- (Once possible) disable password-based auth

# Passwordless use cases

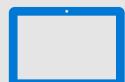
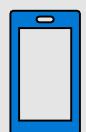
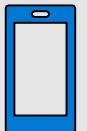
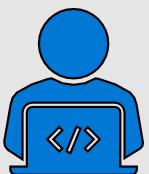
Information Worker



First line Worker



Shared Desk Worker



# Passwordless authentication scenarios

Scenario	Phone authentication	Security keys	Windows Hello for Business
<b>Computer sign in: From assigned Windows 10 device</b>	No	Yes With biometric, PIN	Yes With biometric recognition and/or PIN
<b>Computer sign in: From shared Windows 10 device</b>	No	Yes With biometric, PIN	No
<b>Web app sign-in: from a user-dedicated computer</b>	Yes	Yes Provided single sign-on to apps is enabled by computer sign-in	Yes Provided single sign-on to apps is enabled by computer sign-in
<b>Web app sign-in: from a mobile or non- windows device</b>	Yes	No	No
<b>Computer sign in: Non-Windows computer</b>	No	No	No

For information on selecting the best method for your organization, see [Deciding a passwordless method](#).

# Resources

Passwordless deployment guide

- <https://aka.ms/PasswordlessDocs>

Windows Hello for Business

- <https://aka.ms/whfb>
- <https://aka.ms/whfbplan>
- <https://aka.ms/whfbdeploy>

Microsoft FIDO2

- <https://aka.ms/gopasswordless>



# Open Q & A

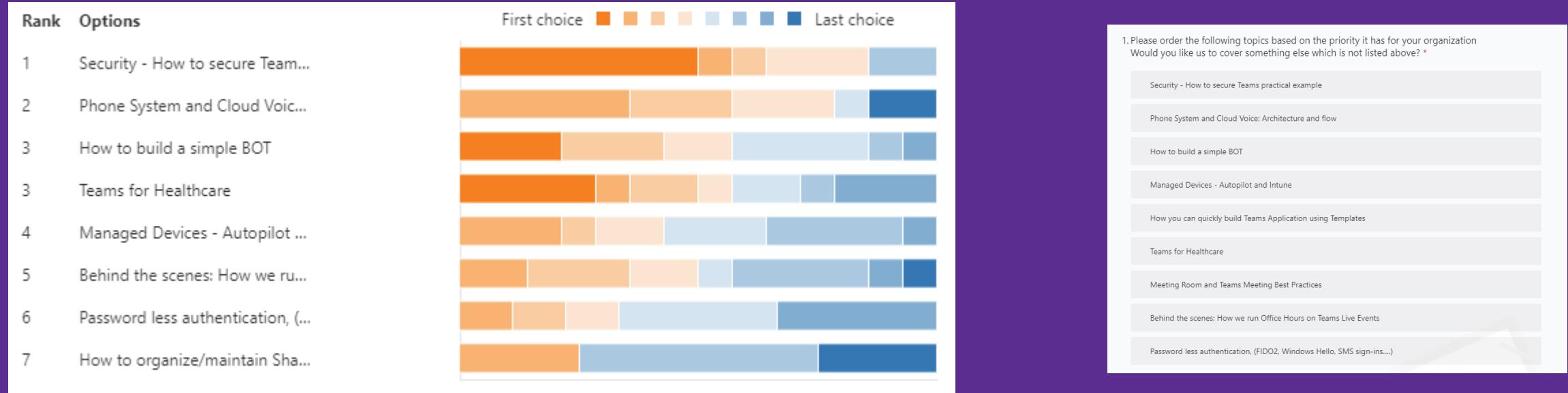
Please ask any question in the Q&A

We will read your questions and answer them in this meeting , or a next meeting.





# <https://aka.ms/WE-TechOfficeHours/Poll>



# Sessions

Planned Sessions	Main Topics
<b>Friday, May 29, 2020</b>	The journey to Passwordless
<b>Friday, June 5, 2020</b>	Phone System and Cloud Voice: Architecture and Flow

<https://aka.ms/WE-TechOfficeHours/Poll>

# Partner Support Resources

# WE Weekly Technical Office Hours

- **Goal:** address the main technical topics around working remotely and leveraging Microsoft technology (incl. Teams, Security, Power Platform, Windows Virtual Desktop...)
- Weekly Sessions – [aka.ms/WE-TechOfficeHours](https://aka.ms/WE-TechOfficeHours)
  - **Fridays at 13:00 – 14:00 CET** (12:00 – 13:00 WEST, 14:00 – 15:00 EEST)
- Hosted and moderated by **experts** on these topics, from **WE OCP Technical Team, EMEA Partner Tech Services and Corp Engineering Team**

# Get help now

- Check out the [Technical Support Options](#) for Microsoft Partners  
<https://support.microsoft.com/en-us/help/4020188/technical-support-for-microsoft-partners>
- If you have a **dedicated Partner Development Manager / Partner Technology Strategist** – reach out to them [directly](#) with your query
- If you do not have a dedicated Partner Development Manager / Partner Technology Strategist, and you need **guidance on a specific customer scenario** (pre-sales technical or deployment assistance) – make use of your [advisory hours](#) and reach out to [Partner Technical Services](#)

# Other Partner Resources

- **Best practices and discussion for remote work**
  - [Best practices](#), based on Microsoft internal learnings
  - (new) [Microsoft Tech Community](#) forum for discussing / sharing best practices
- **Enabling Microsoft Teams**
  - We recommend that partners lead with the [CSP Trial](#). See details in our [news article](#).
  - For customers who **don't align to the CSP Trial**, partners can get access to the **Office 365 E1 Trial** for them. Go to [Partner Center Support](#) and click on *CSP > Cannot find an offer in the catalog*.
- **Resources for Education Partners**
  - Check out the [EDU Partner Flash on Yammer](#)
  - **Office 365 A1 – Free** versions to **all educational institutions**: unlimited chat, built-in group and one-on-one audio or video calling, 10 GB of team file storage, and 2 GB of personal file storage per user. You also get real-time collaboration with the Office apps for web, including Word, Excel, PowerPoint, and OneNote. No restrictions for # of users.
  - **Microsoft Teams for Free** (**Individuals** and **IT roll-out** – in Office 365 A1 above): unlimited chat, built-in group and one-on-one audio or video calling, 10 GB of team file storage, and 2 GB of personal file storage per user.
  - **Minecraft: Education Edition**: We've extended access to Minecraft: Education Edition to all free and paid O365 Education accounts through the end of June 2020 and published a [M:EE remote learning toolkit](#) with links to >100 Minecraft lessons and STEM curriculum.

# Thank You!

