Microsoft

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)

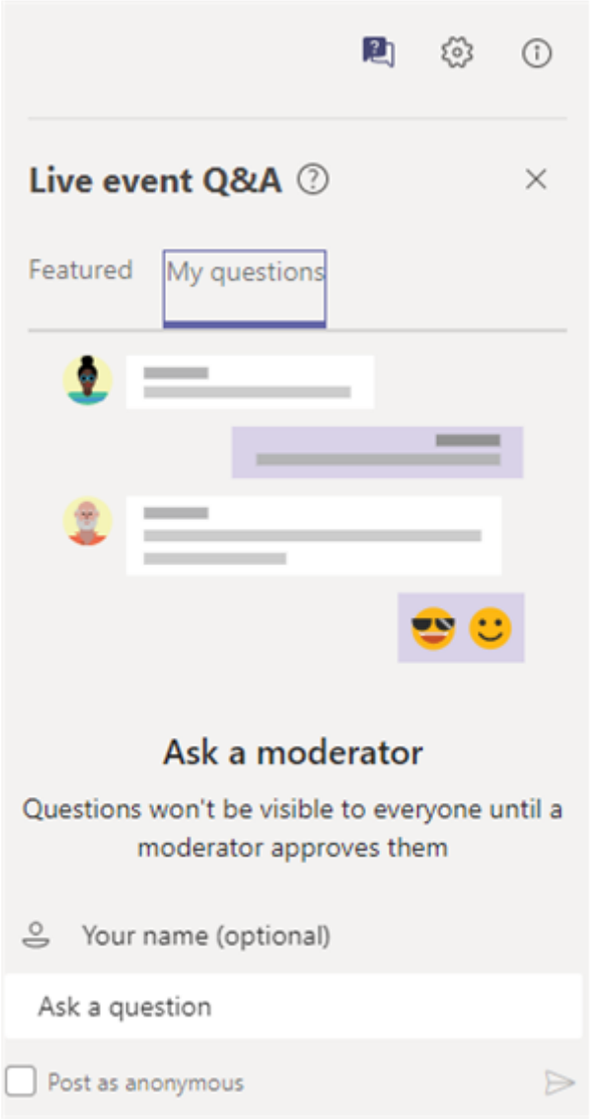
Philippe Goldstein
Partner Tech. Manager

WE Weekly Technical Office Hours – How it works

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

Questions via chat through

Q&A



(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

Don't miss a session;

Update your calendar by using the invite above.

https://aka.ms/WE-TechOfficeHours

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.

Microsoft

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

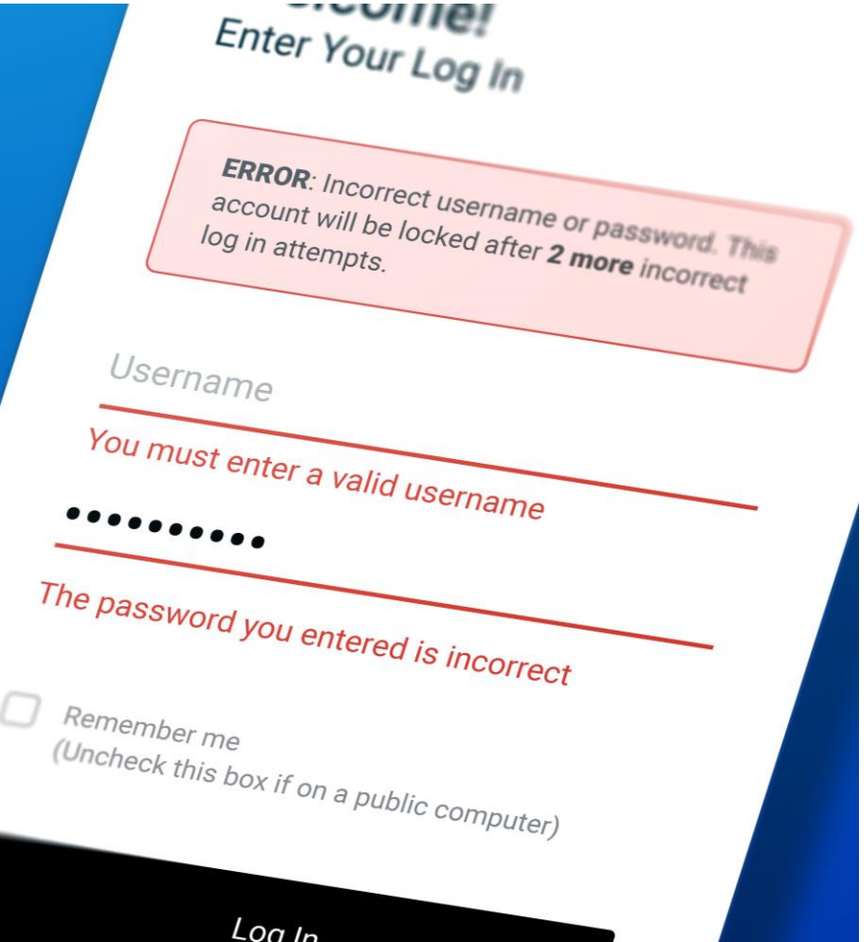
Aline Harmand
Partner Tech. Strategist (Security)

Bojan Magusic
Cloud Solution Architect (Security)

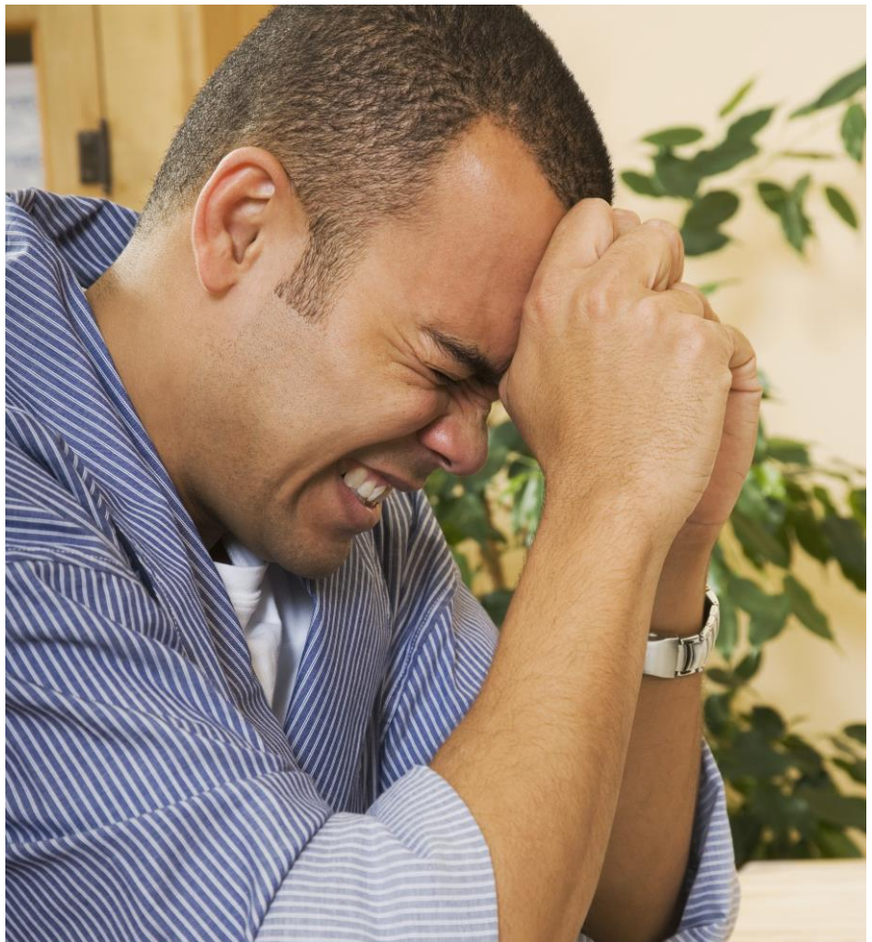
Hans Hofkens
Partner Tech. Architect (Security)

Almost everyone hates passwords

Users



IT Admins



Hackers

Hackers ♥passwords

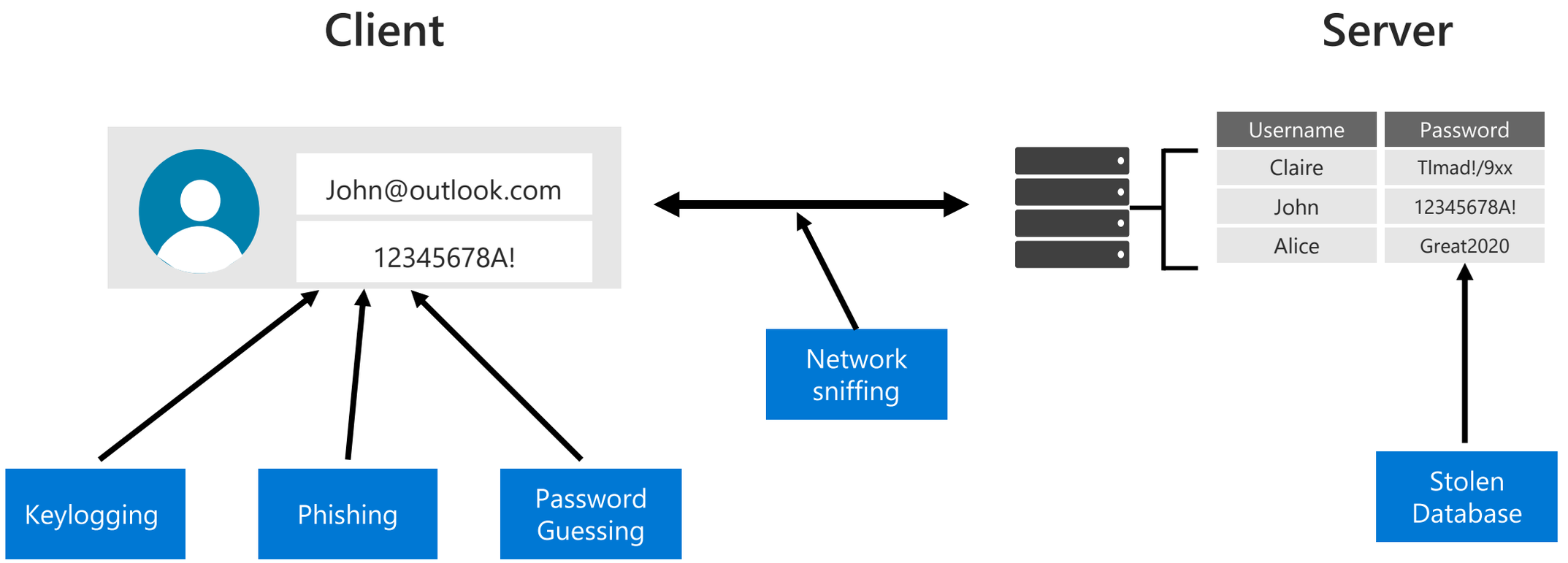
Most frequently rejected passwords from October 2018

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

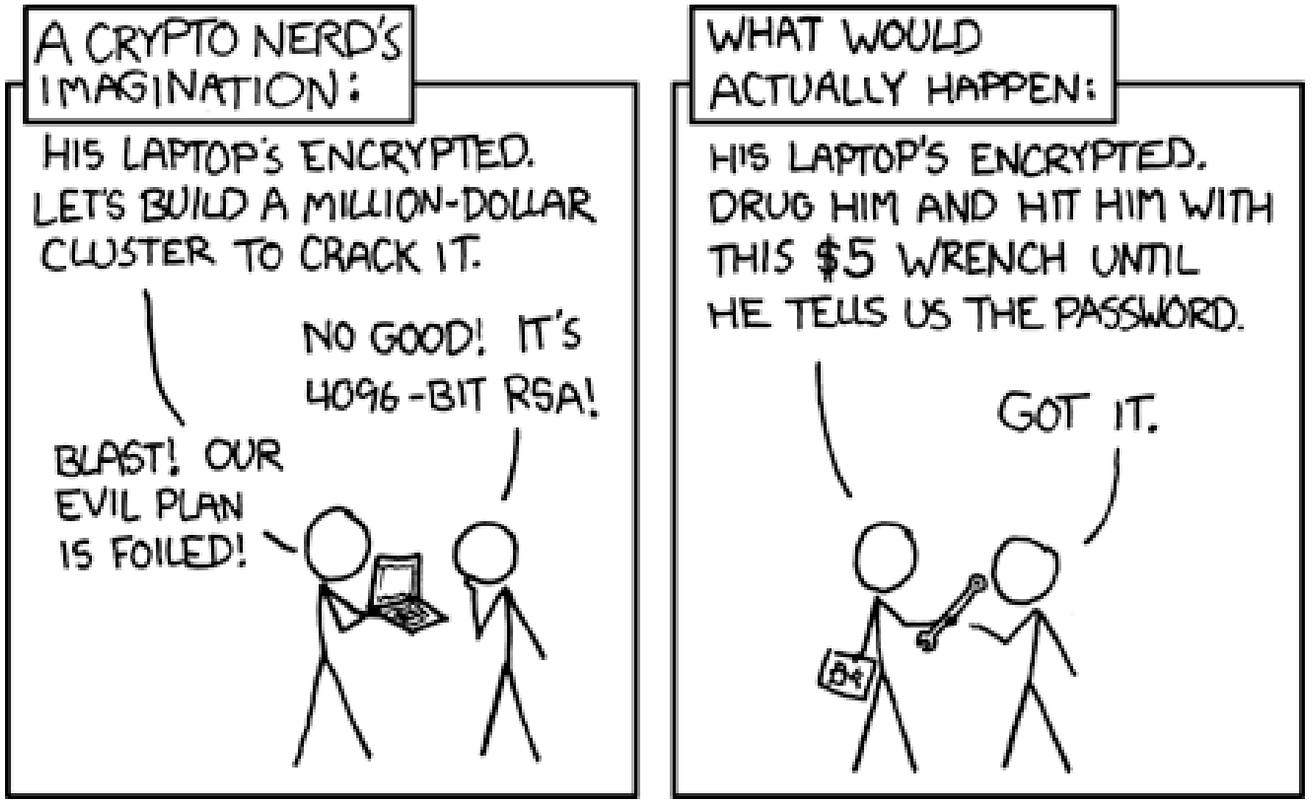
6	fall
7	september
8	apple
9	soccer
10	london

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

73%
of passwords are duplicates

Passwords are the weak link

81%
of breaches leveraged passwords

Data breaches are expensive

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

Passwords generate tons of support calls

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.

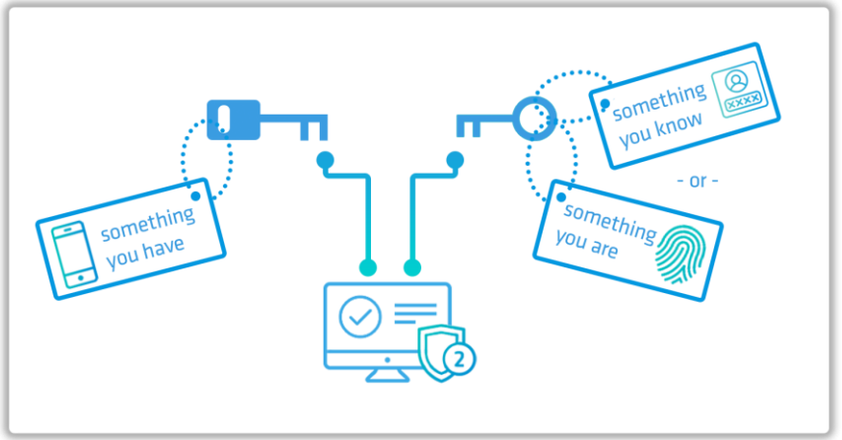
  Try Microsoft Authenticator phone sign-in for added mobility.

  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

MFA Credentials

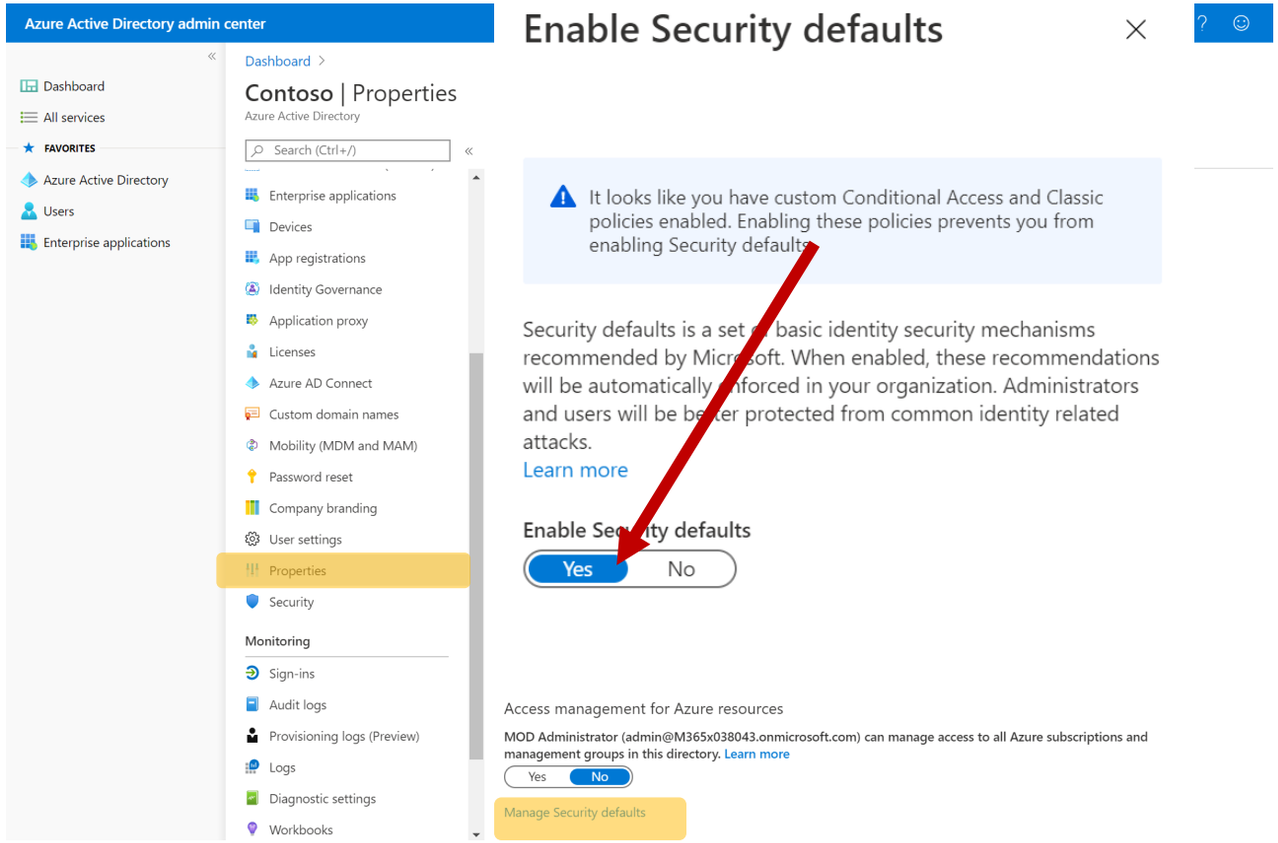
- Windows Hello
- FIDO2 Security key
- Microsoft Authenticator
- OATH Hard Tokens
- SMS, Voice

Multi-factor authentication prevents 99.9% of identity attacks

Free MFA options in all Azure AD subscriptions

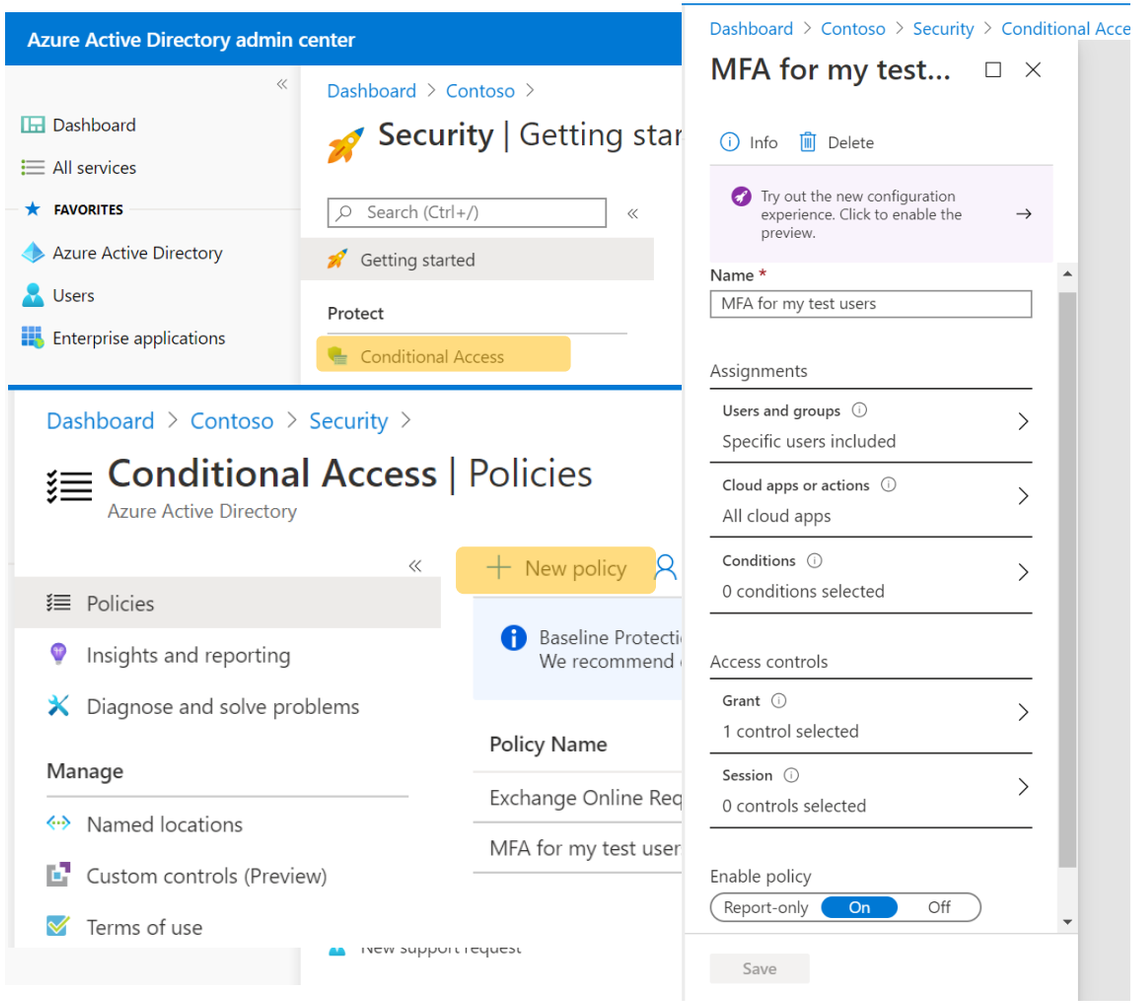
Enable MFA

With Security Defaults



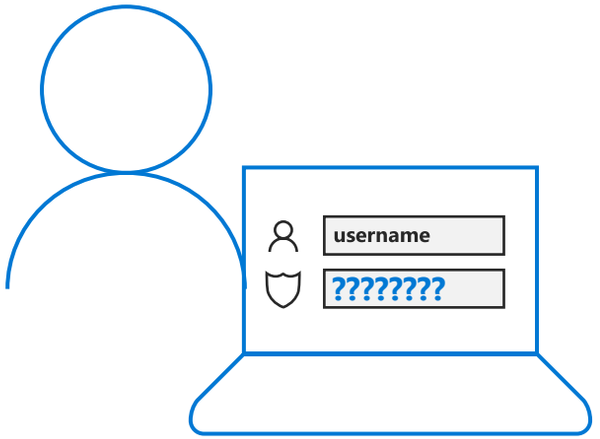
To learn more, see [What are security defaults?]

With Conditional Access Policies

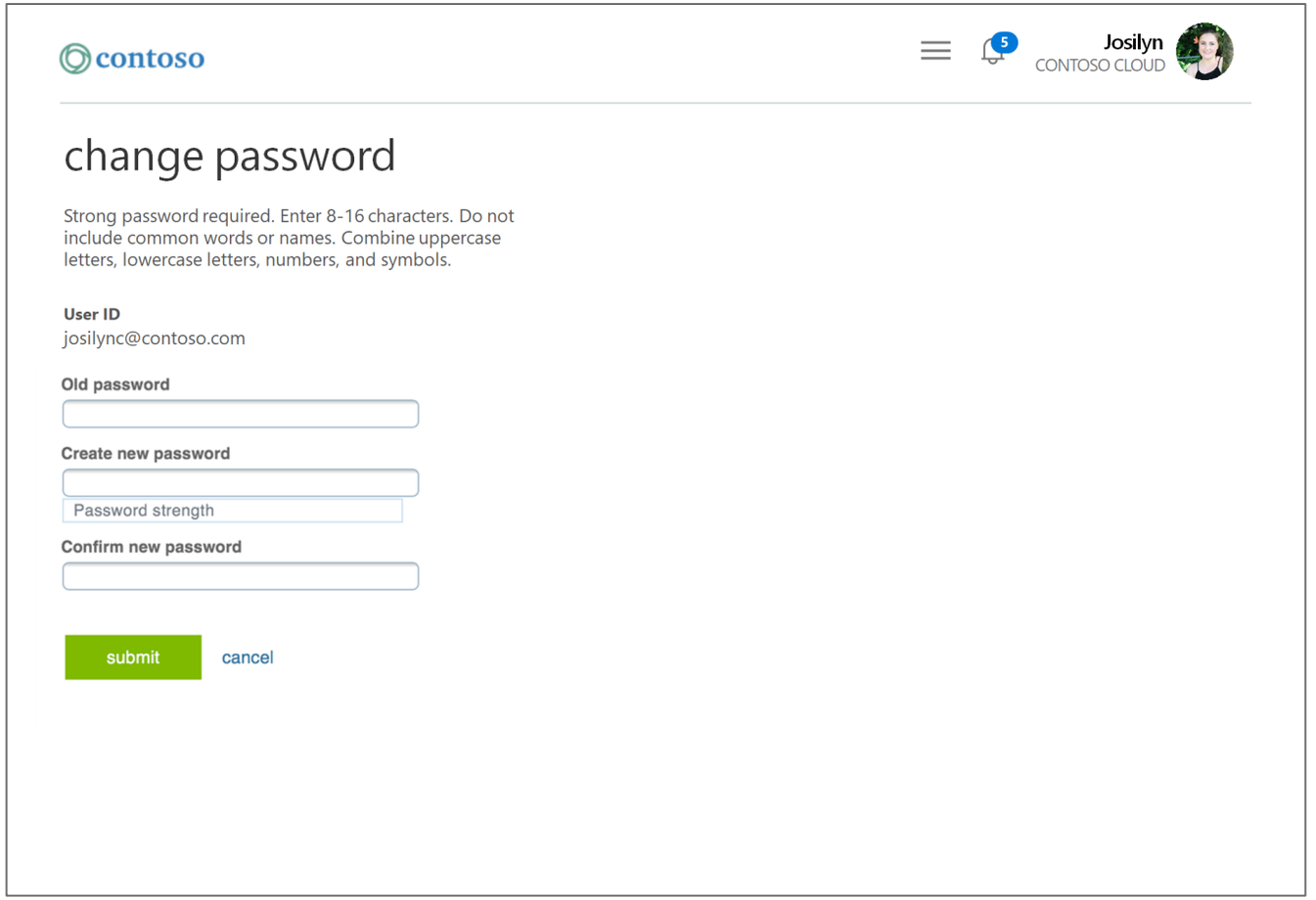


To learn more, see [Quickstart: Require MFA for specific apps with Azure Active Directory Conditional Access]

Empower user self-service to save time and money

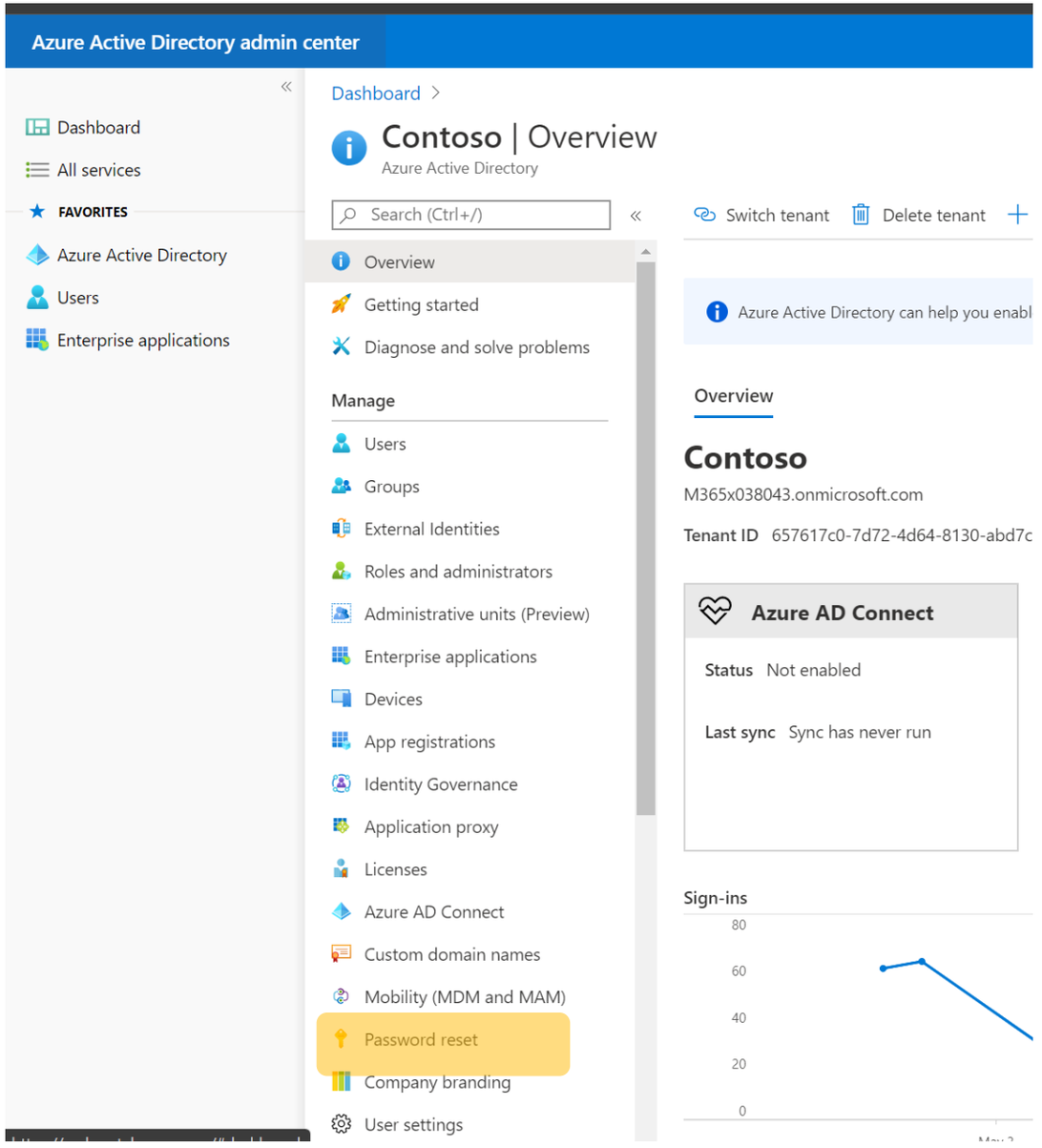


- Resolving password issues for users is one of the largest IT costs
- Maximize user flexibility by enabling resets from an intuitive web interface or directly from the Windows login screen

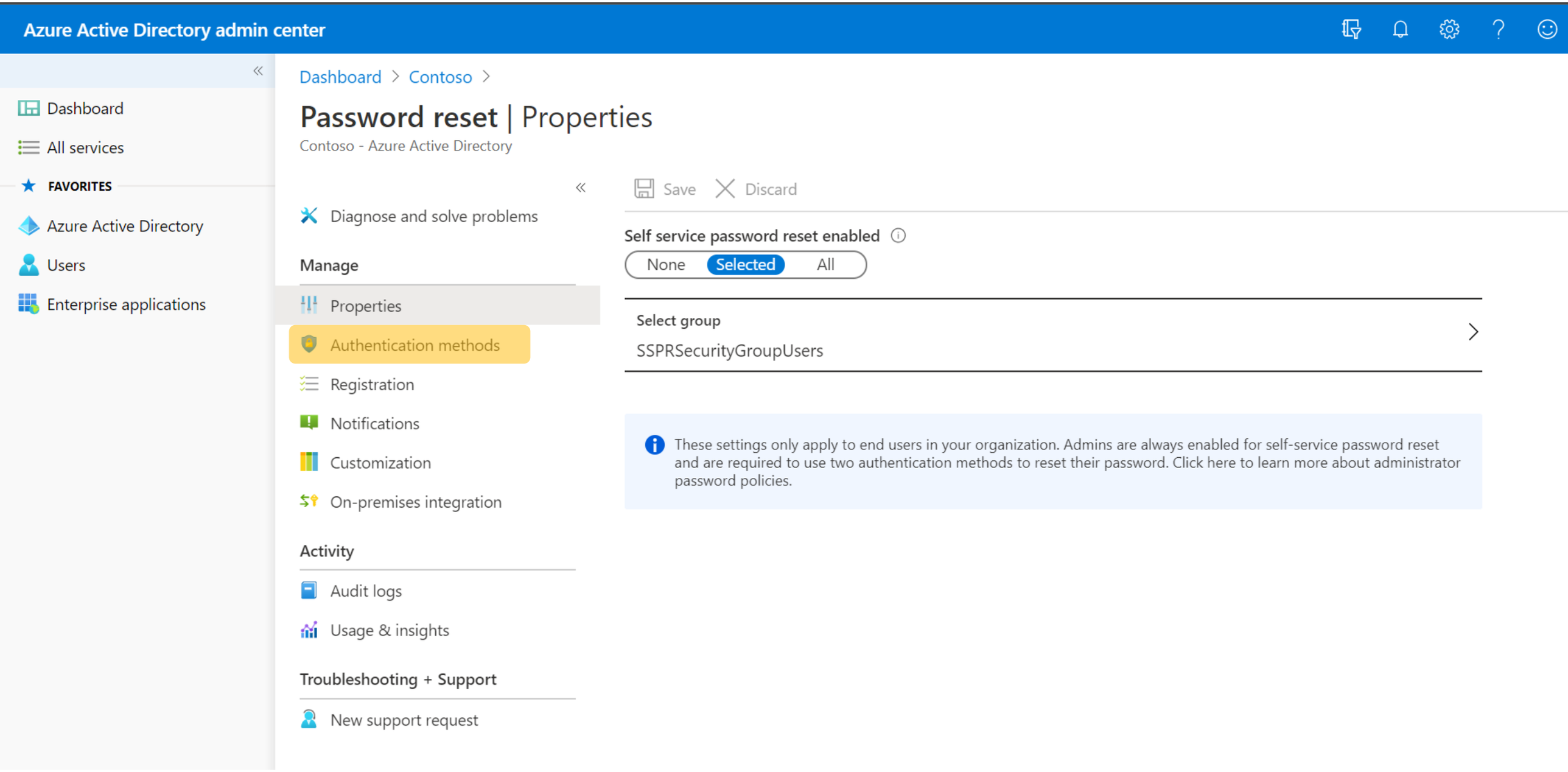


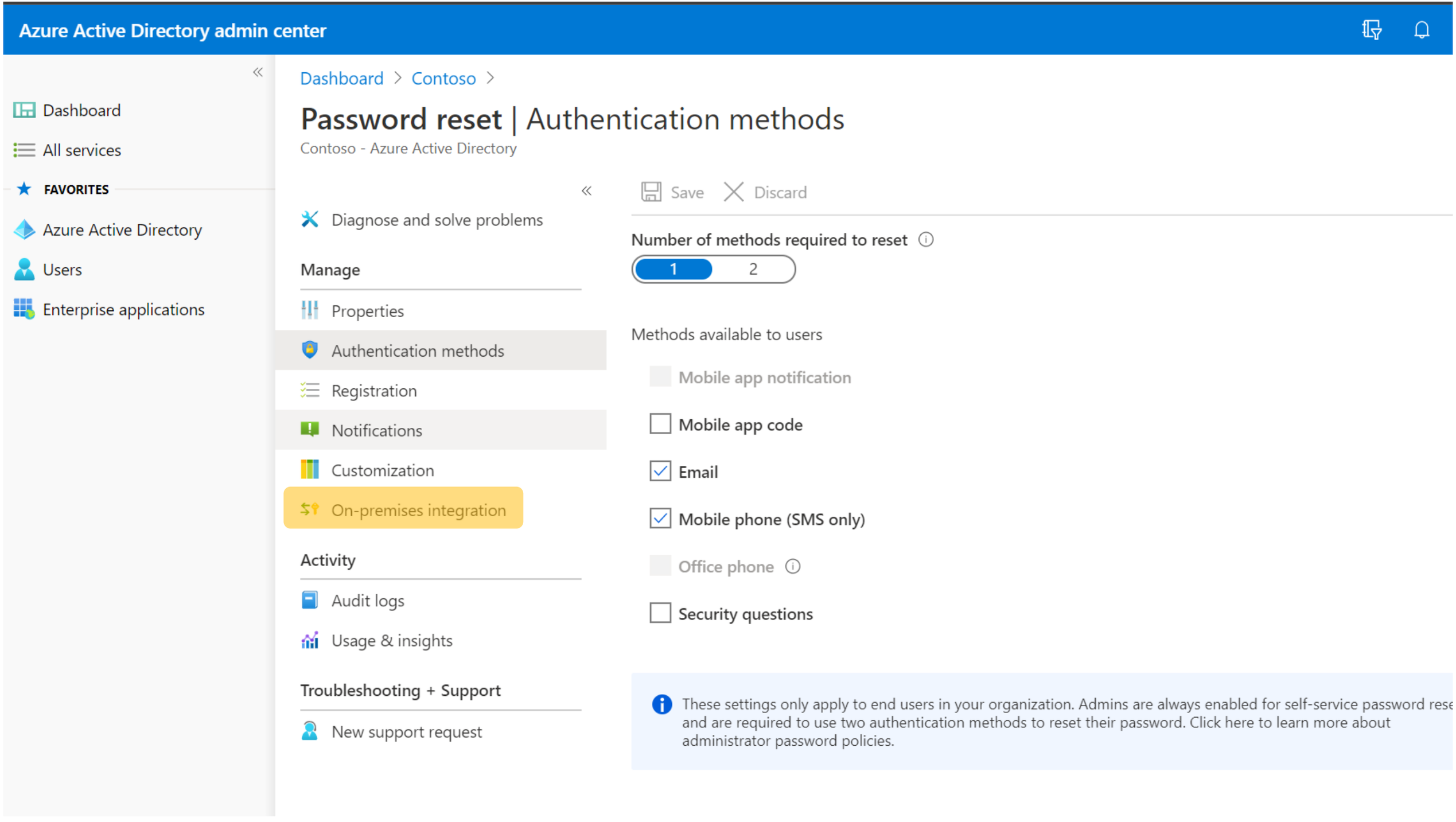
How to enable Self-Service Password Reset?

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

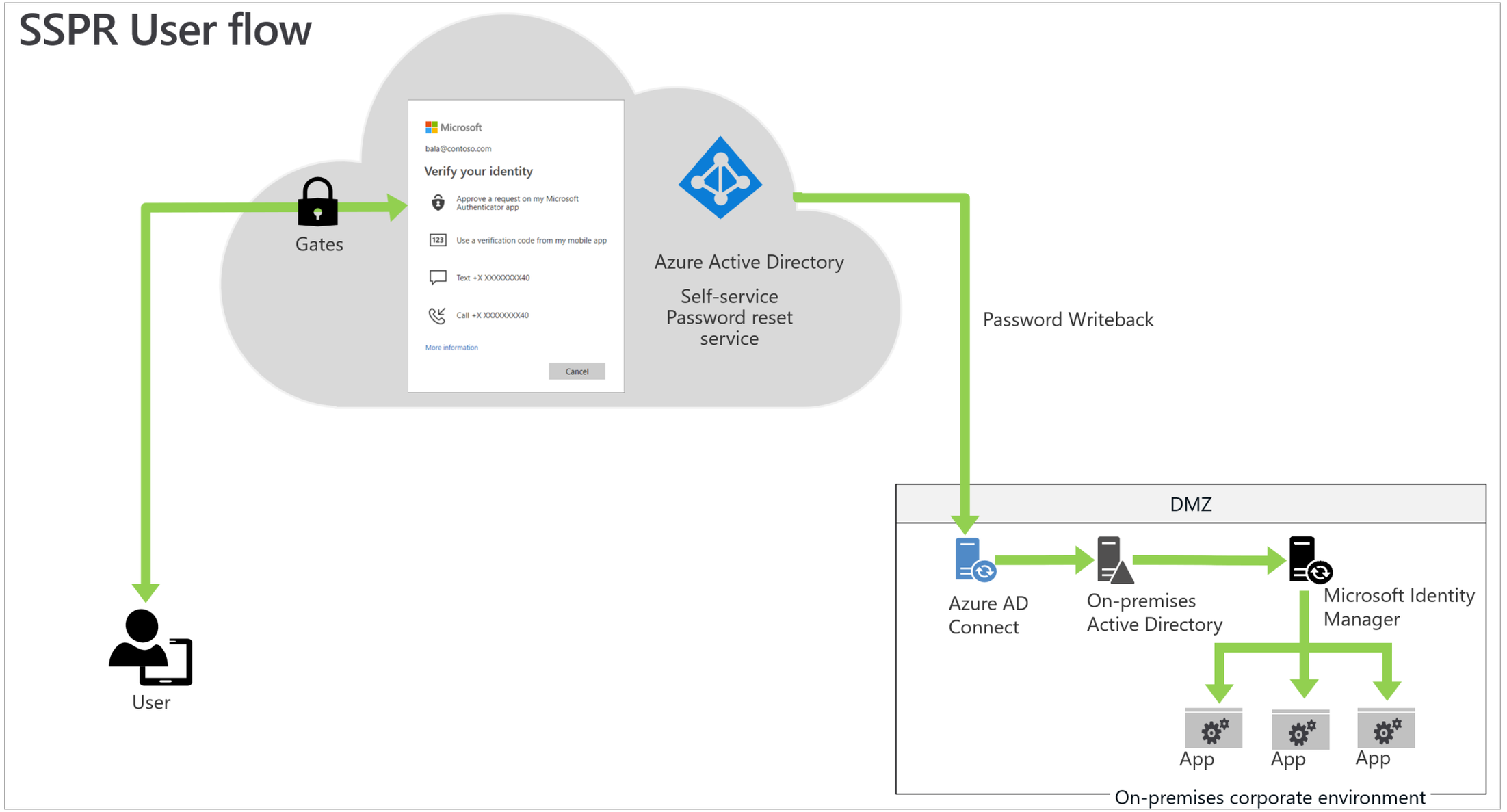


https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks

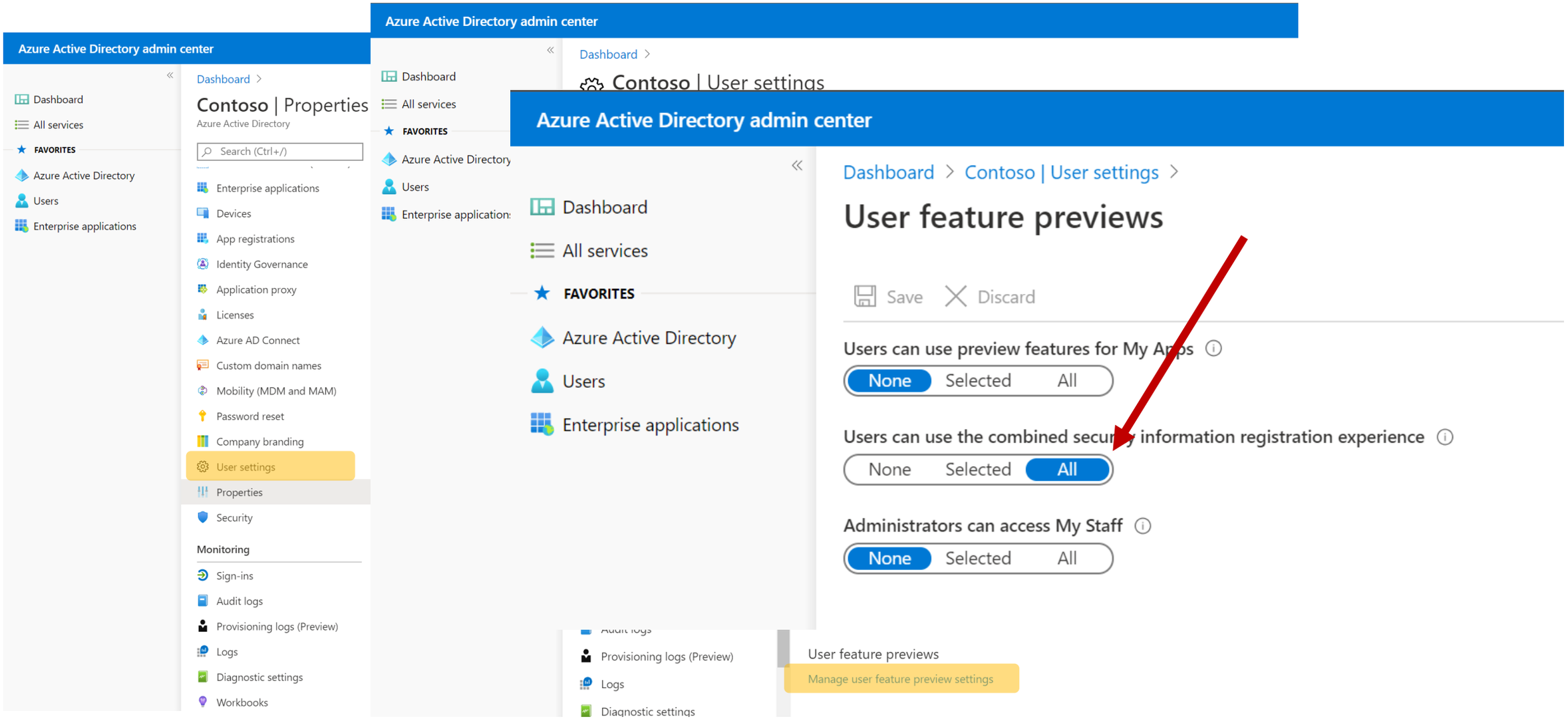

Azure Active Directory admin center
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Dashboard > Contoso >
Password reset | Properties
Contoso - Azure Active Directory
Diagnose and solve problems
Manage
Properties
Authentication methods
Registration
Notifications
Customization
On-premises integration
Activity
Audit logs
Usage & insights
Troubleshooting + Support
New support request
Save
Discard
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.


Azure Active Directory admin center
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Dashboard > Contoso >
Password reset | Authentication methods
Contoso - Azure Active Directory
Diagnose and solve problems
Manage
Properties
Authentication methods
Registration
Notifications
Customization
On-premises integration
Activity
Audit logs
Usage & insights
Troubleshooting + Support
New support request
Save
Discard
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 rese
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

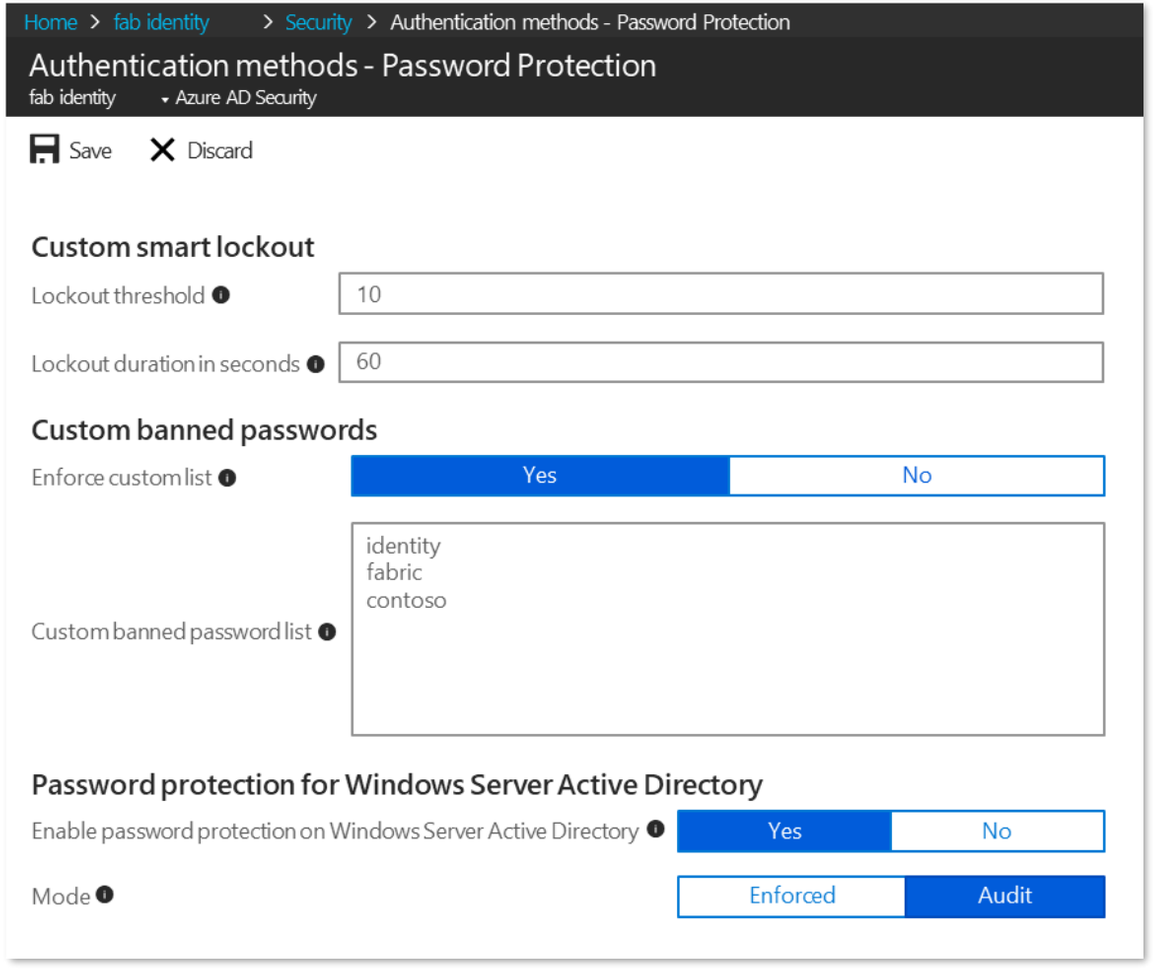


To learn more, see [Combined security information registration overview]

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



[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

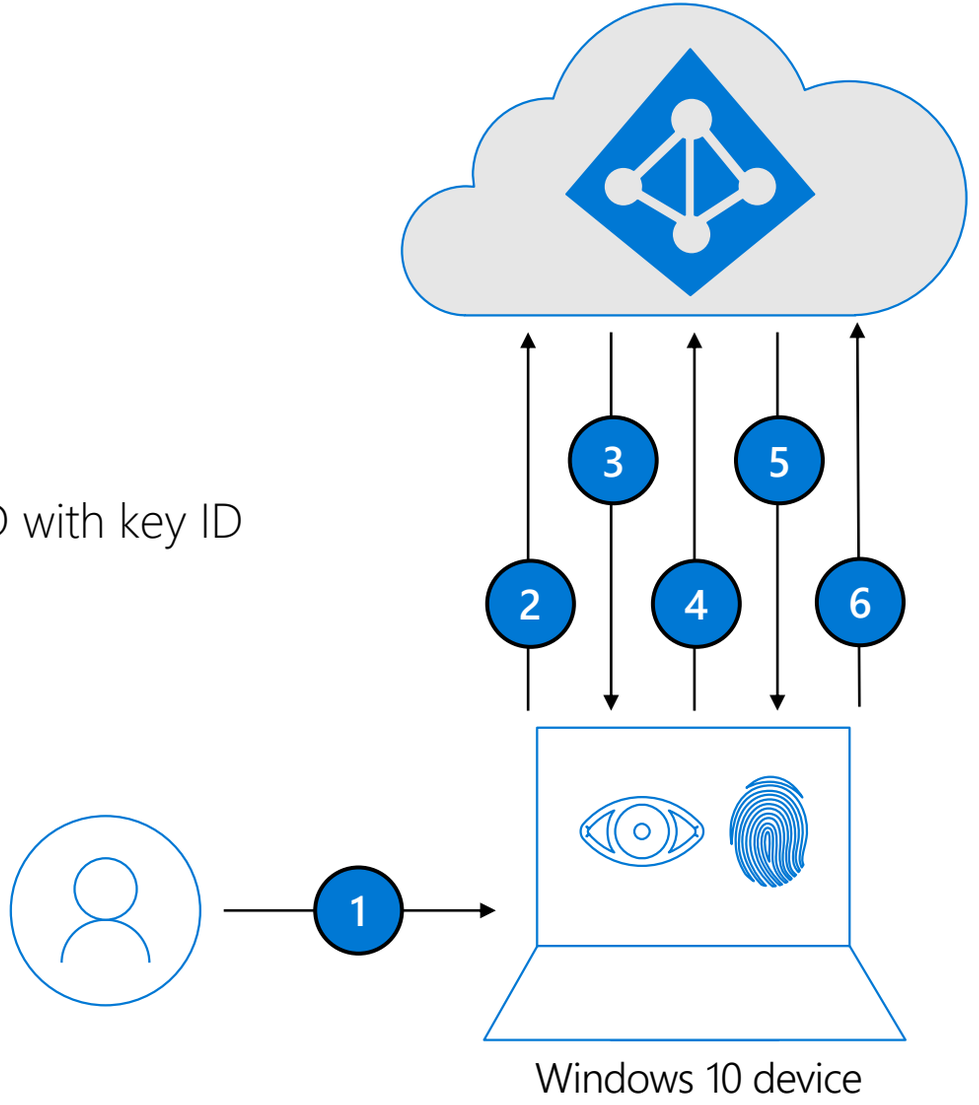
- Strong two-factor authentication
- Asymmetric key pair auth model
- Can be deployed in cloud, hybrid, or on-prem environments
- Multi account

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

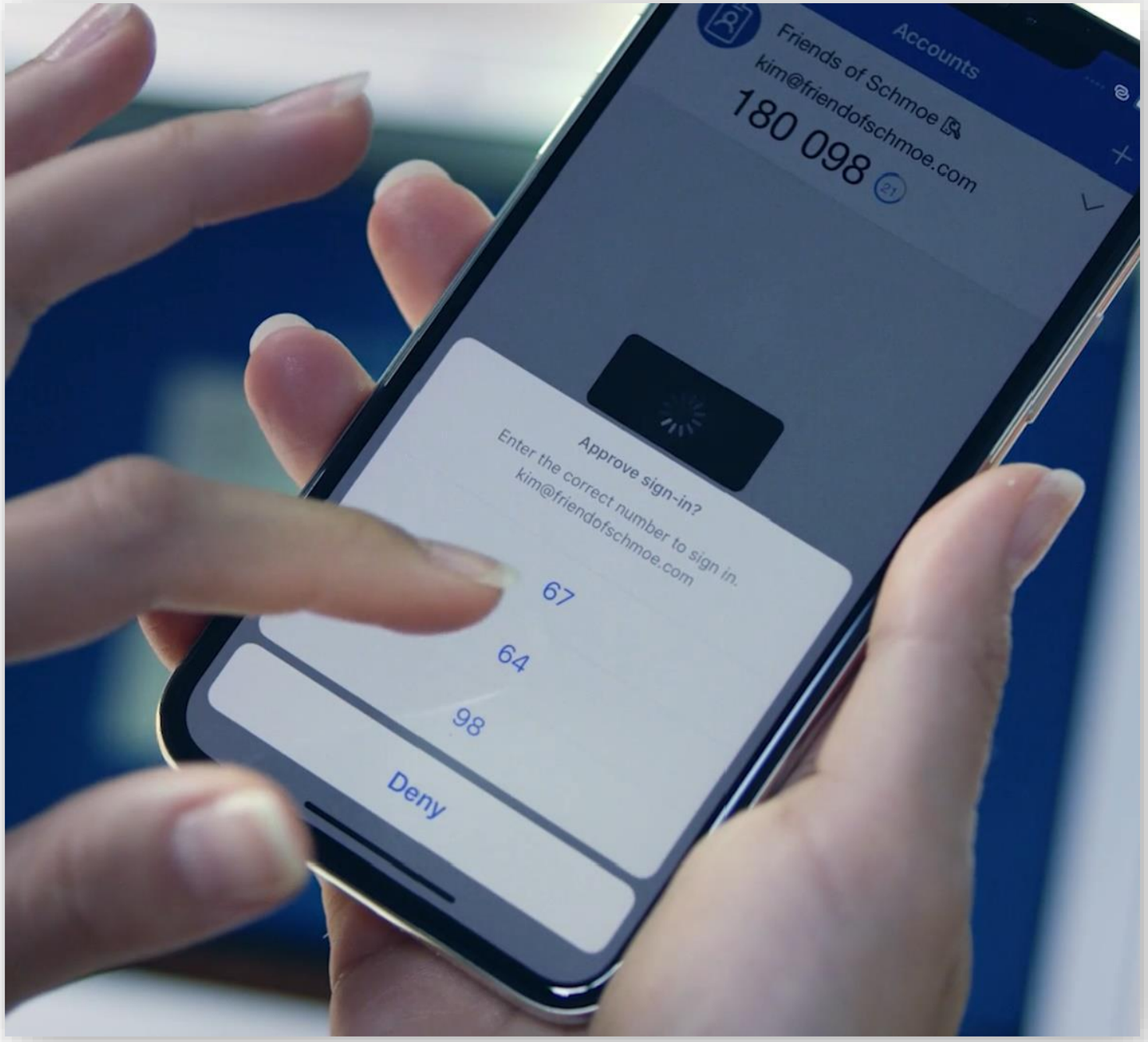
1. User sign-in with bio-gesture unlocks TPM holding private key
2. Windows sends “hello”
3. Azure AD sends back nonce
4. Windows uses private key to sign nonce and returns to Azure AD with key ID
5. Azure AD returns PRT + encrypted session key protected in TPM
6. Windows returns the signed PRT and derived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




Looking for you...
12:00
Friday, March 29

Microsoft Authenticator

Microsoft’s passwordless anywhere solution



Microsoft Authenticator

Overview

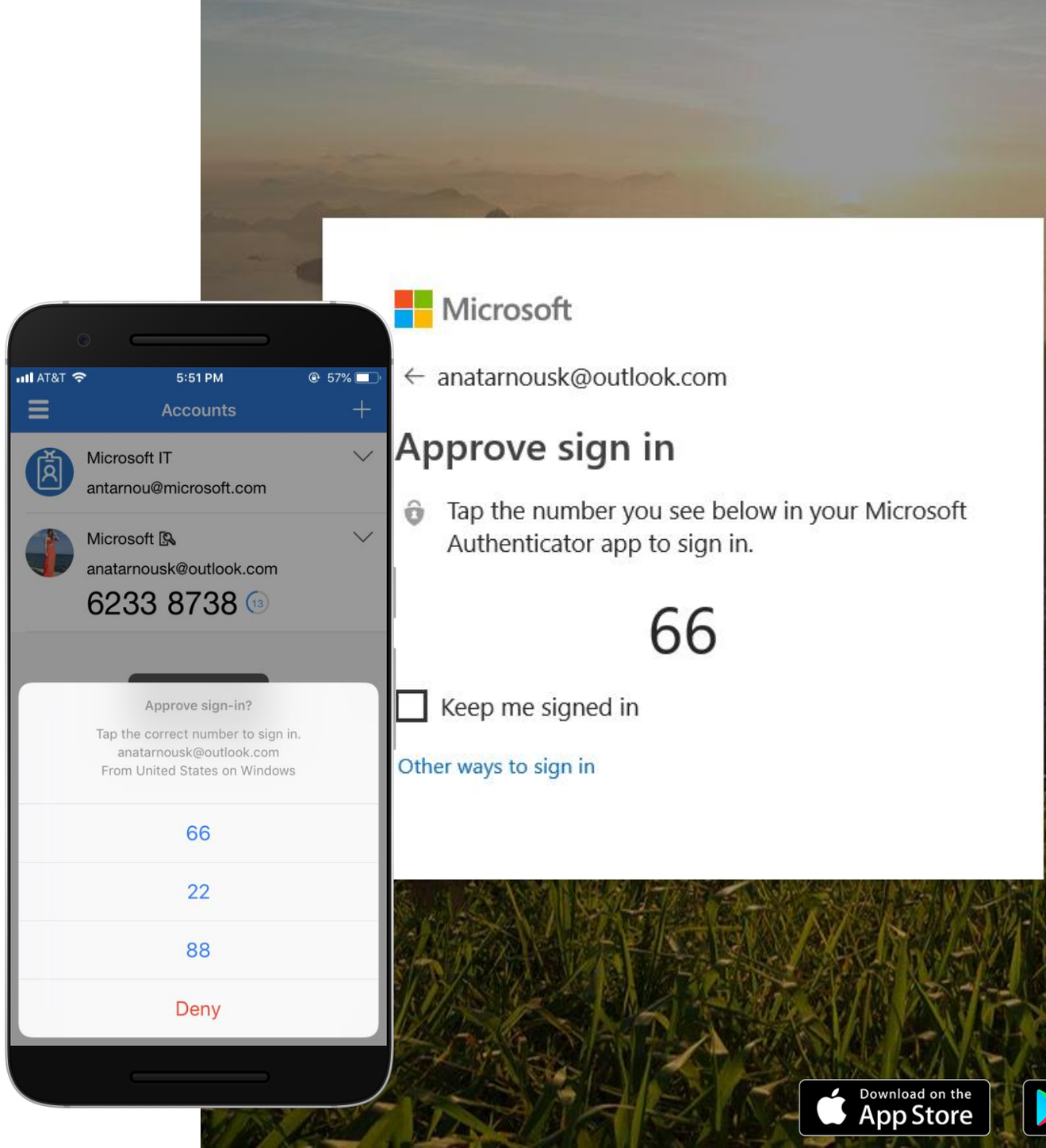
- Standard based MFA
- Multi-account

Windows 10

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

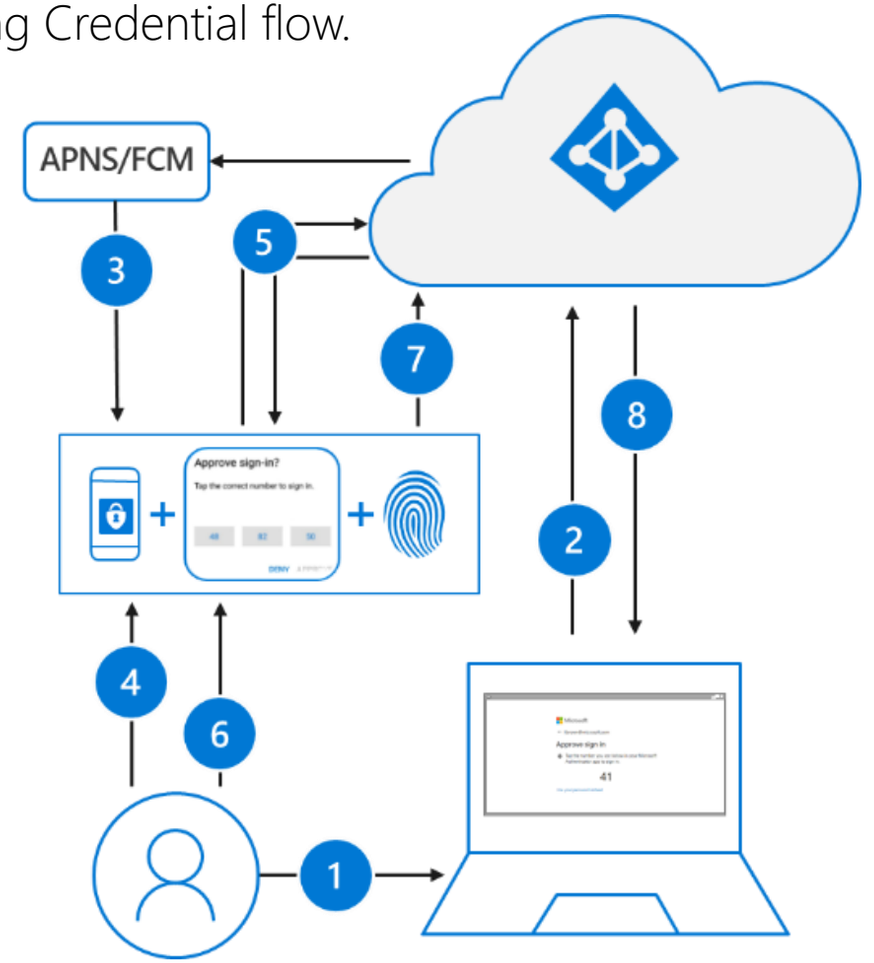
Mobile

- SSO to native mobile apps

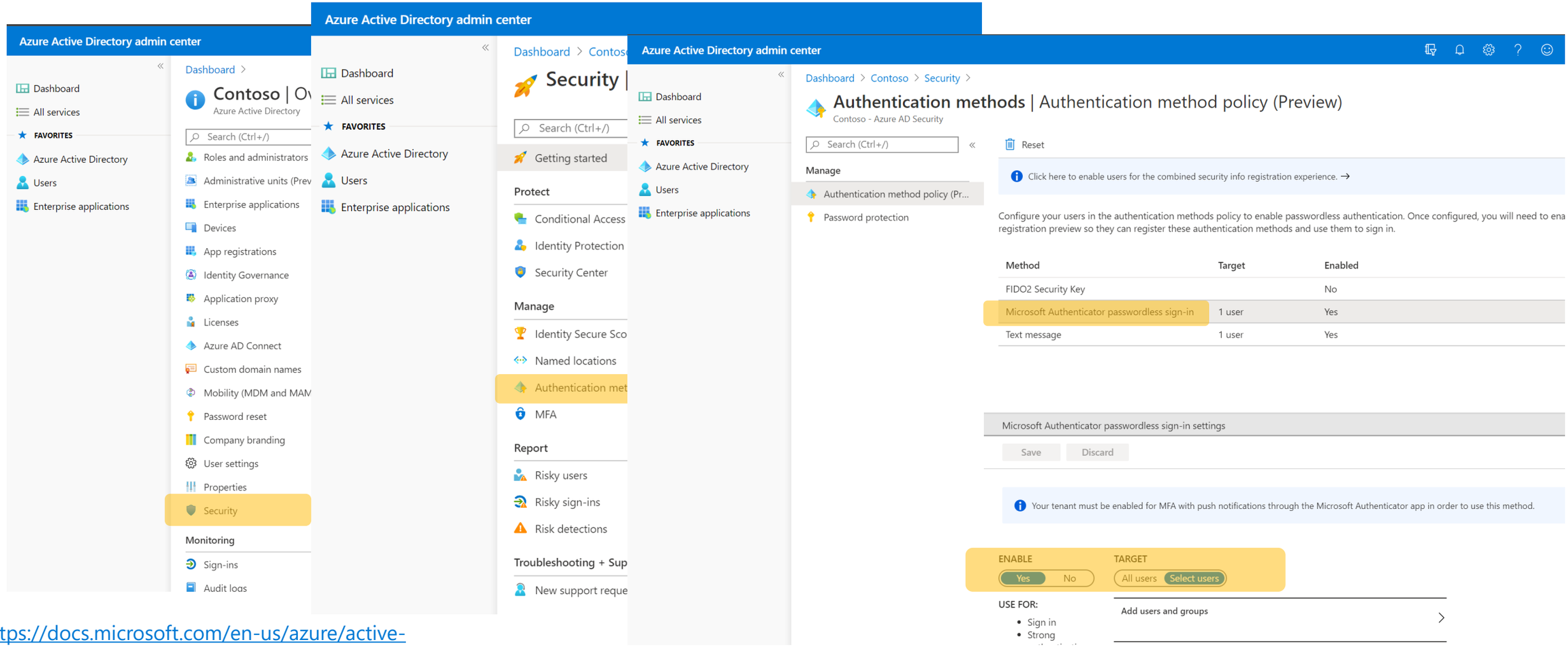


How does Authenticator Passwordless Sign In work?

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?



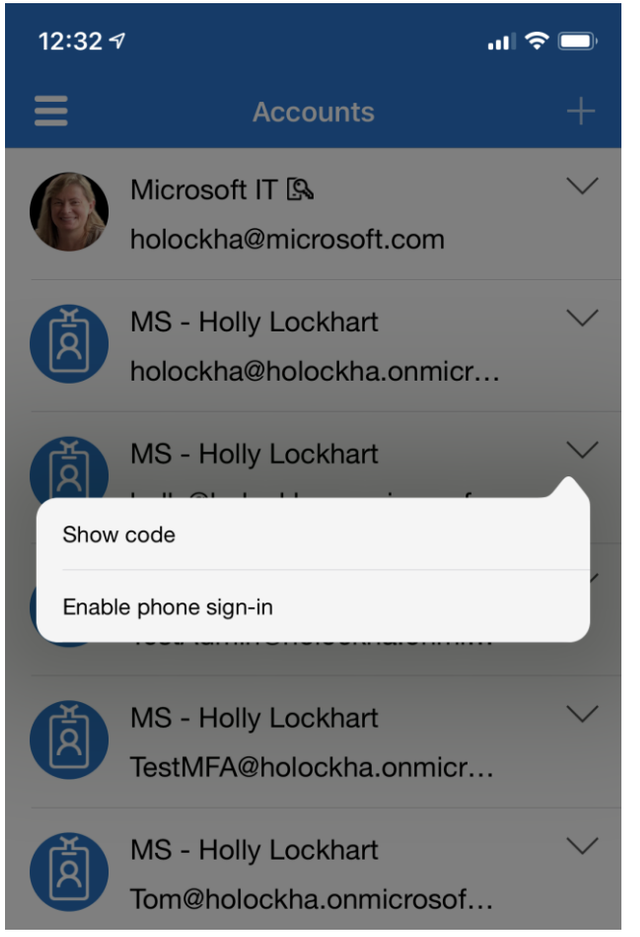
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

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

fido™ ALLIANCE

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

yubico Trust the Net.

FEITIAN WE BUILD SECURITY

ENSURITY TECHNOLOGIES

eWBM

HID

Passwordless with FIDO2 security keys

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

Secure Authentication Flow

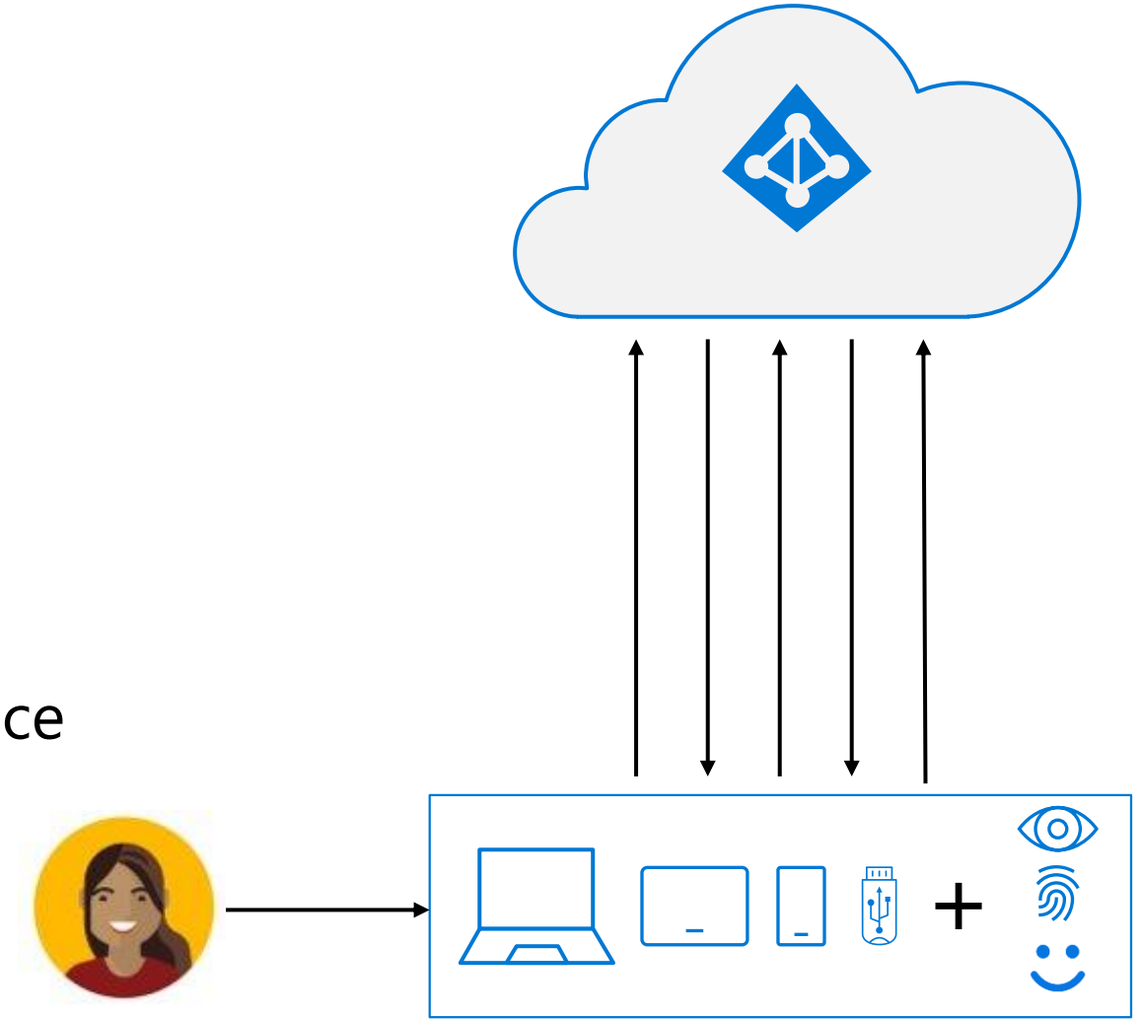
A simple, common architecture

Based on public-key technology

Private-keys are securely stored
on the device

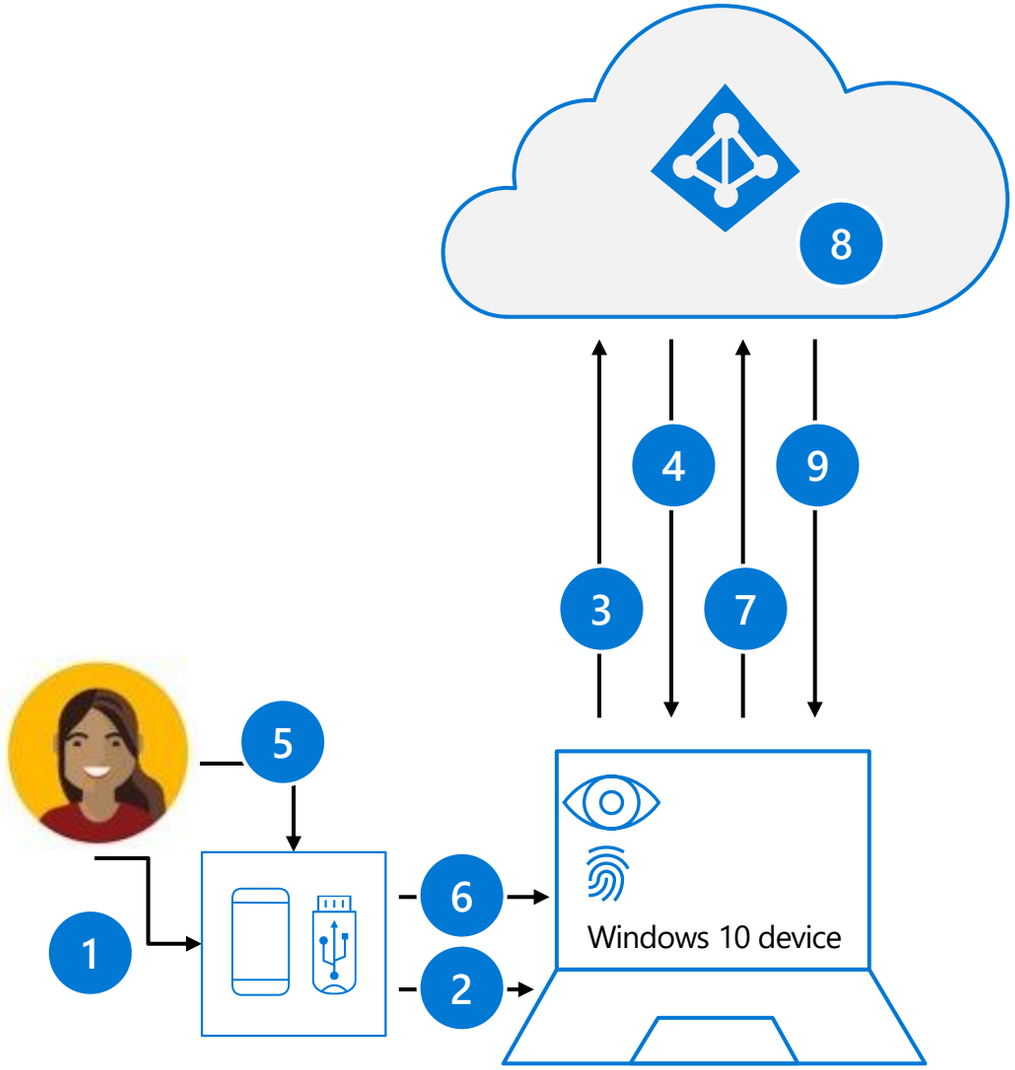
Requires a local gesture
(e.g., biometric, PIN)

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

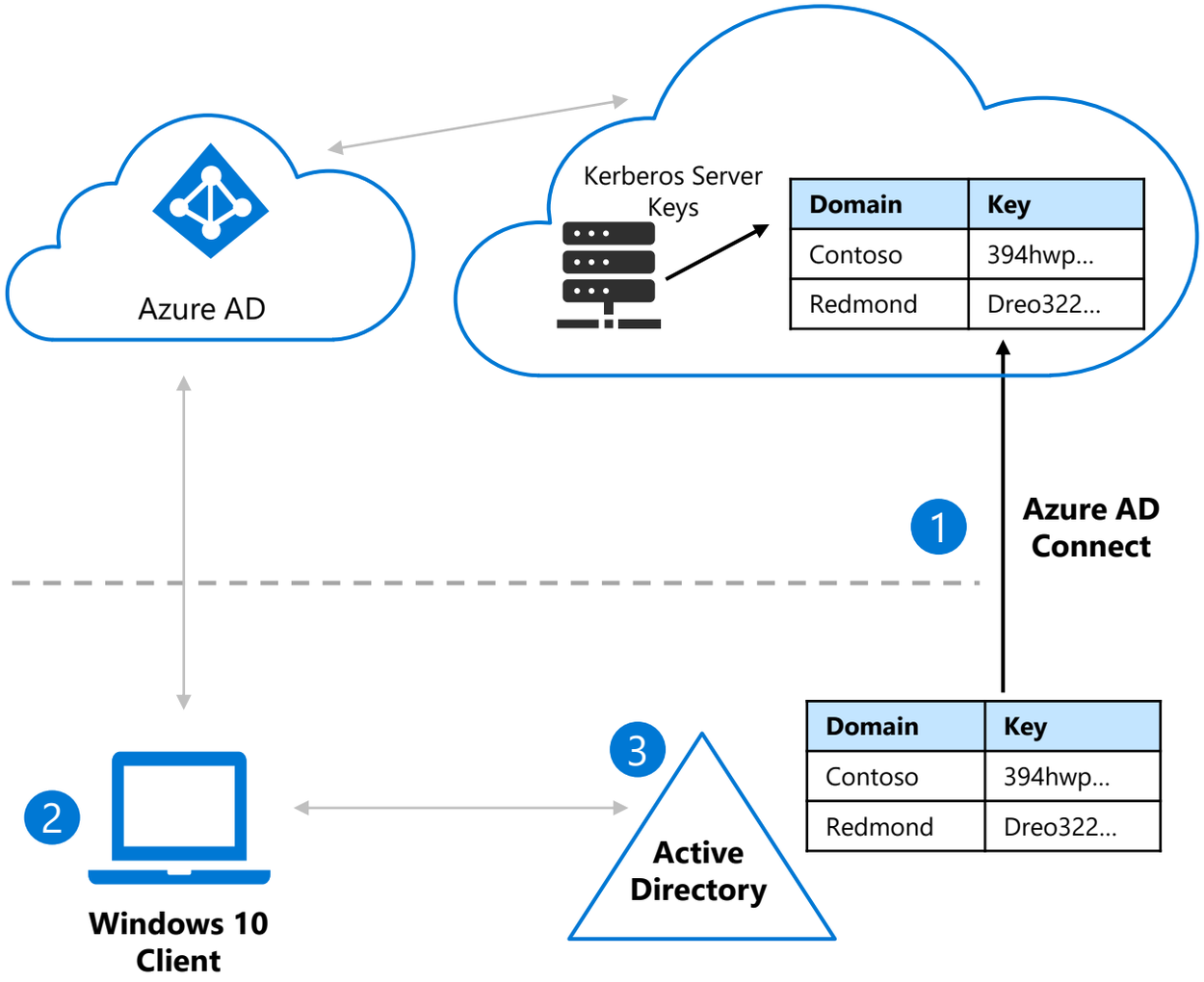


Strong Authentication with FIDO2 security key

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

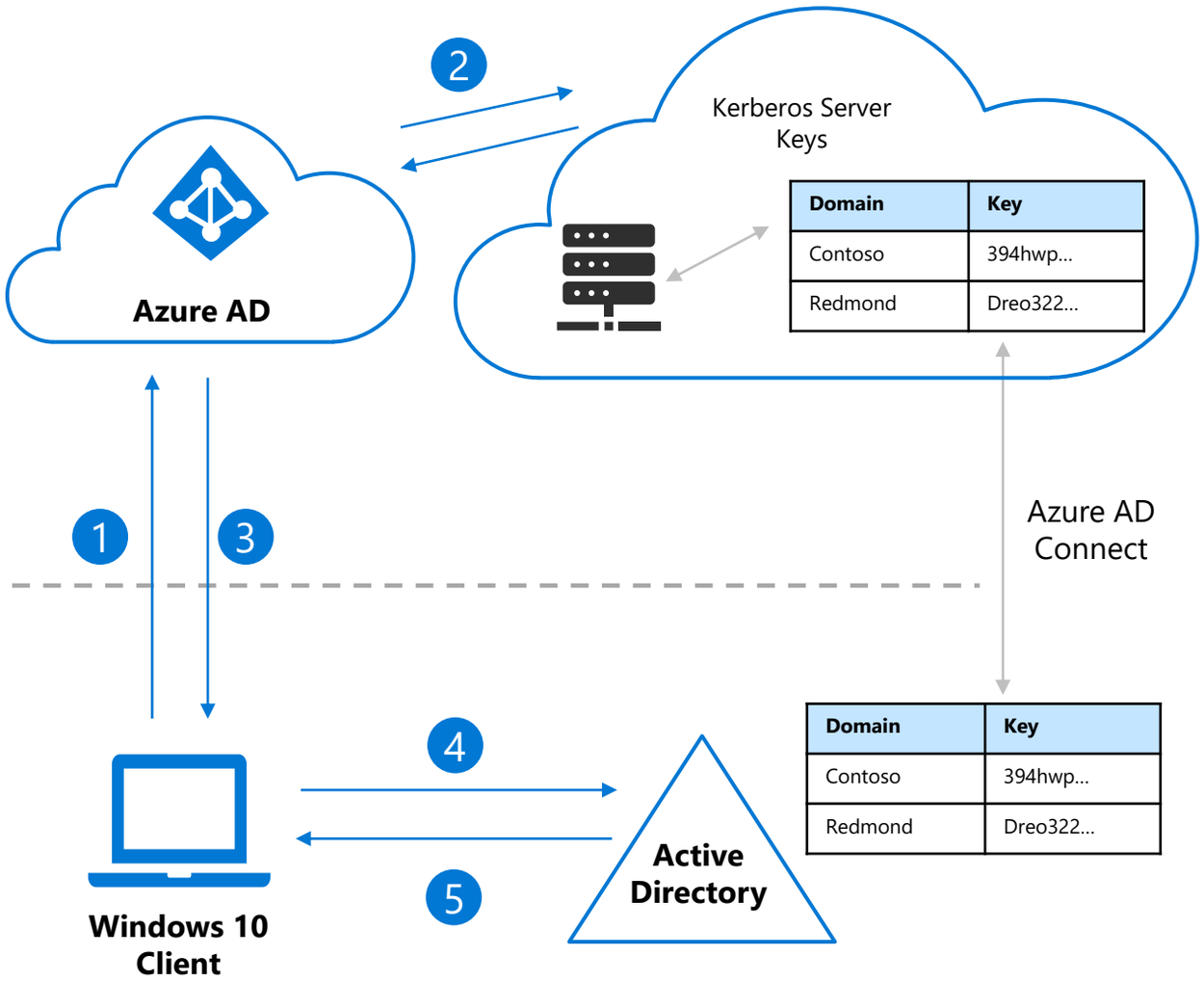


Deployment Components



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	REGISTRATION
Fido Pilot group	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

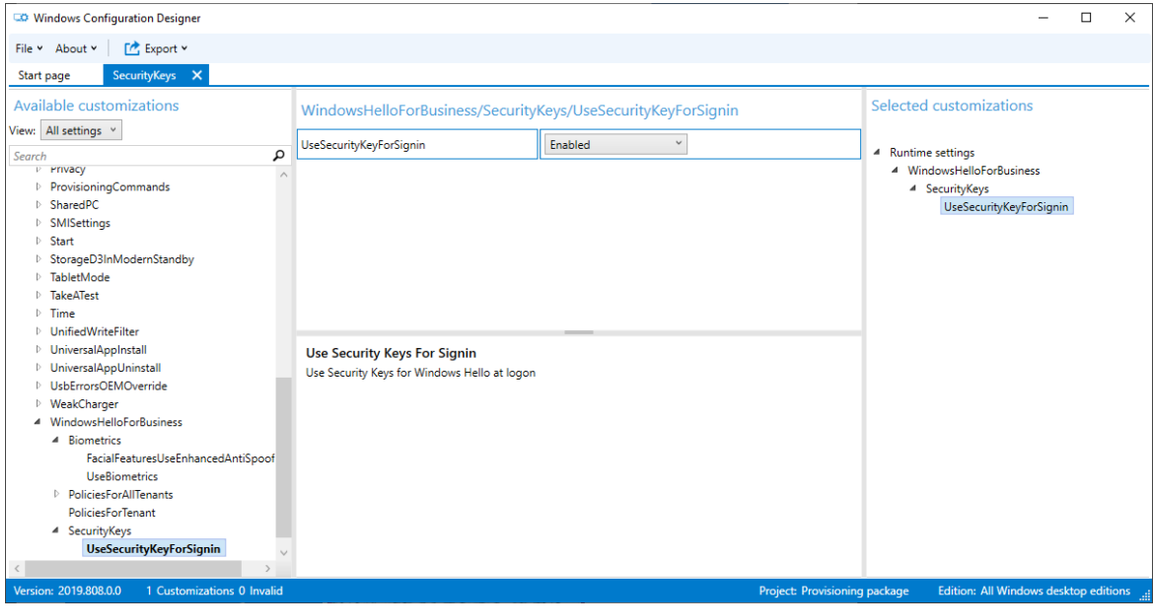
Description

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

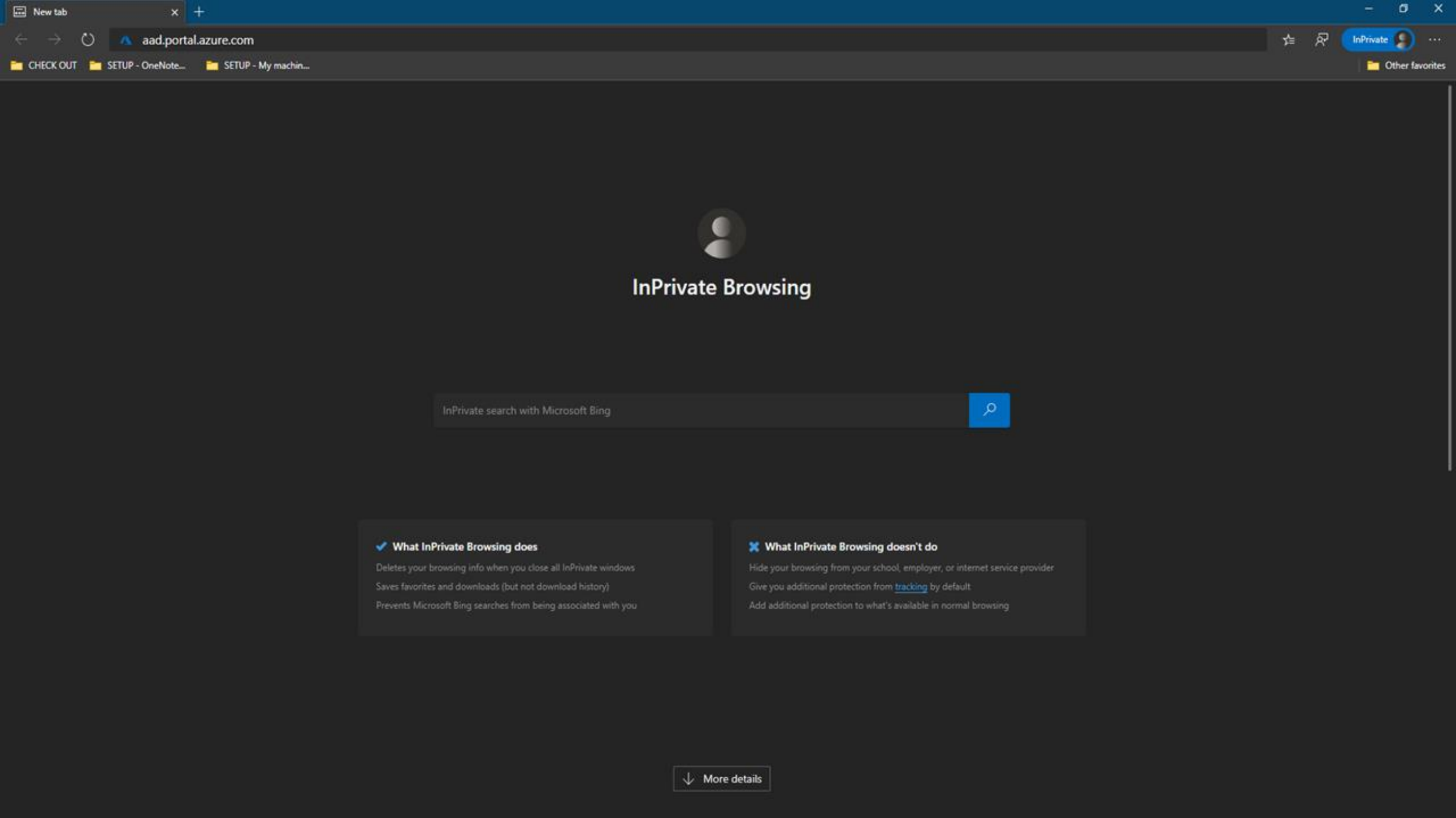
Security info

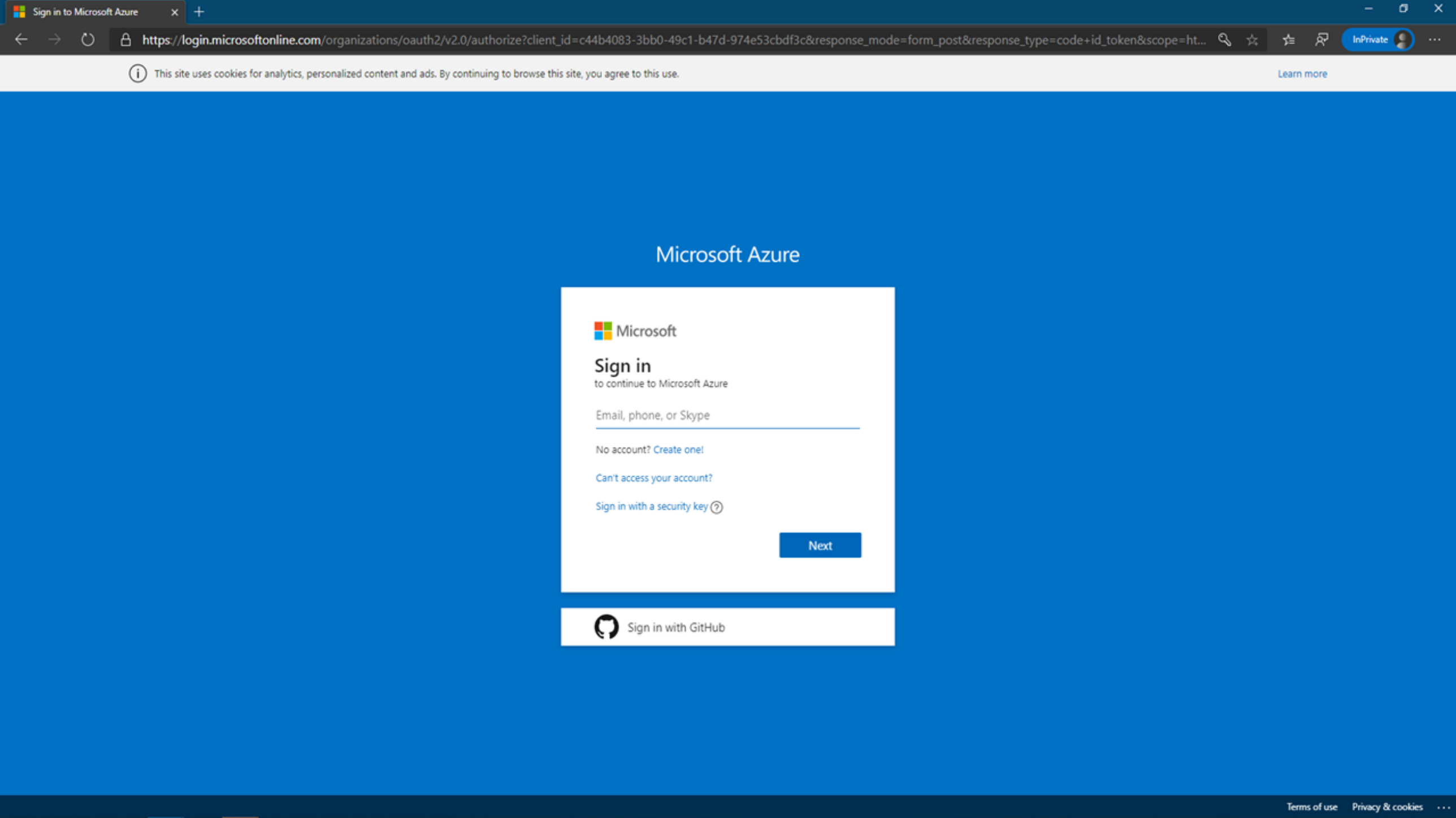
These are the methods you use to sign into your account or reset your password.

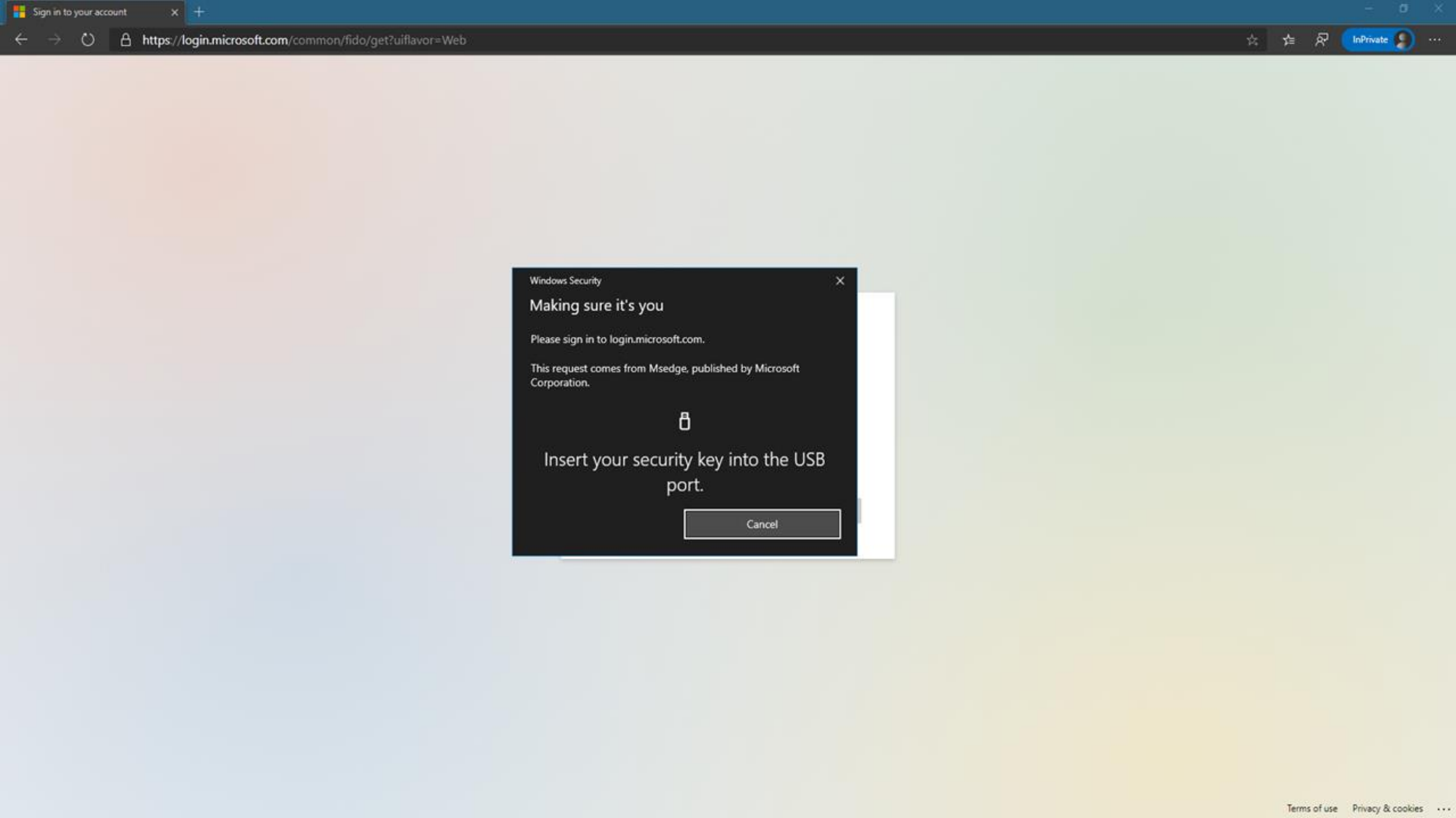
Default sign-in method: Microsoft Authenticator - notification Change

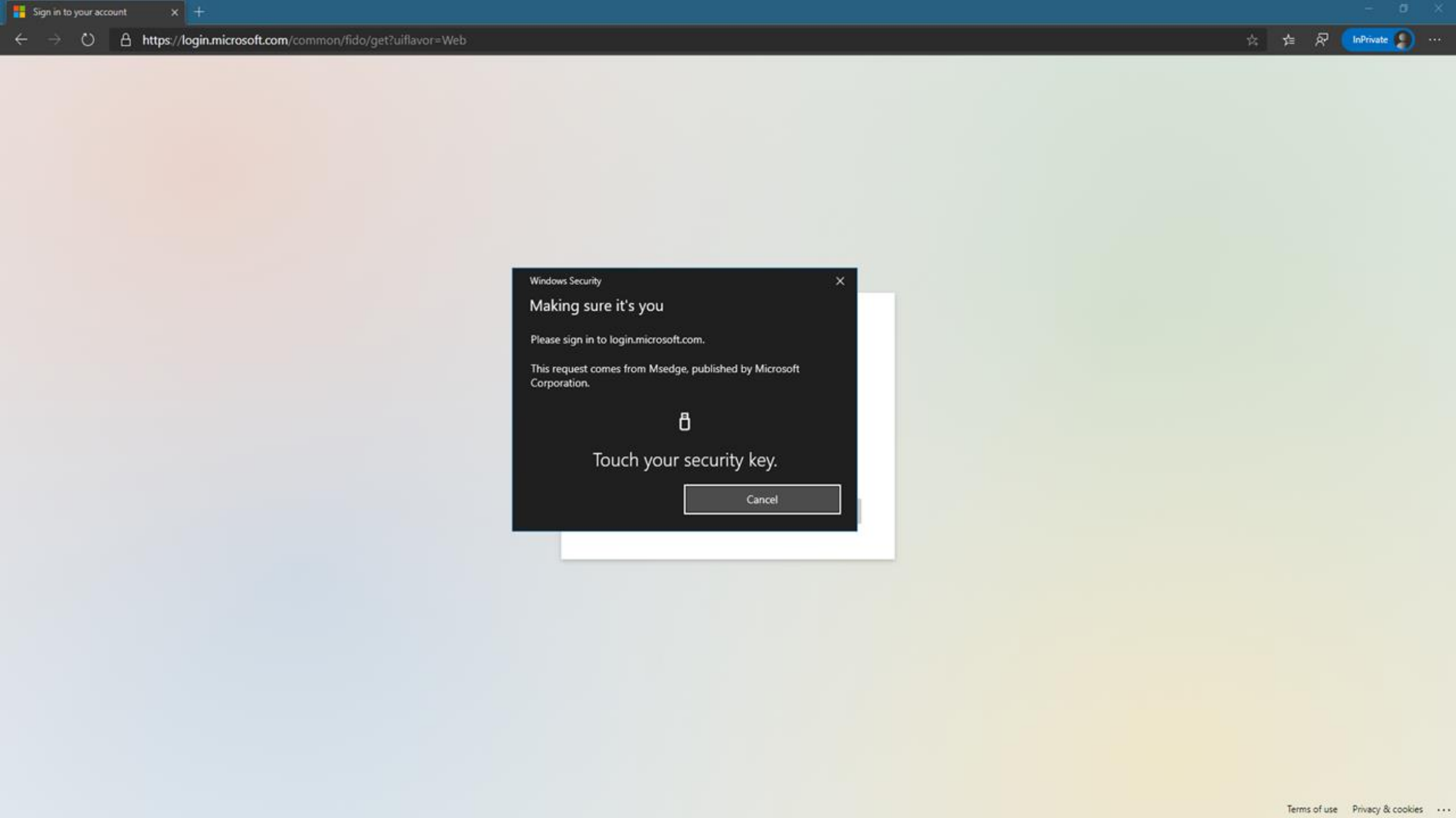
Add method

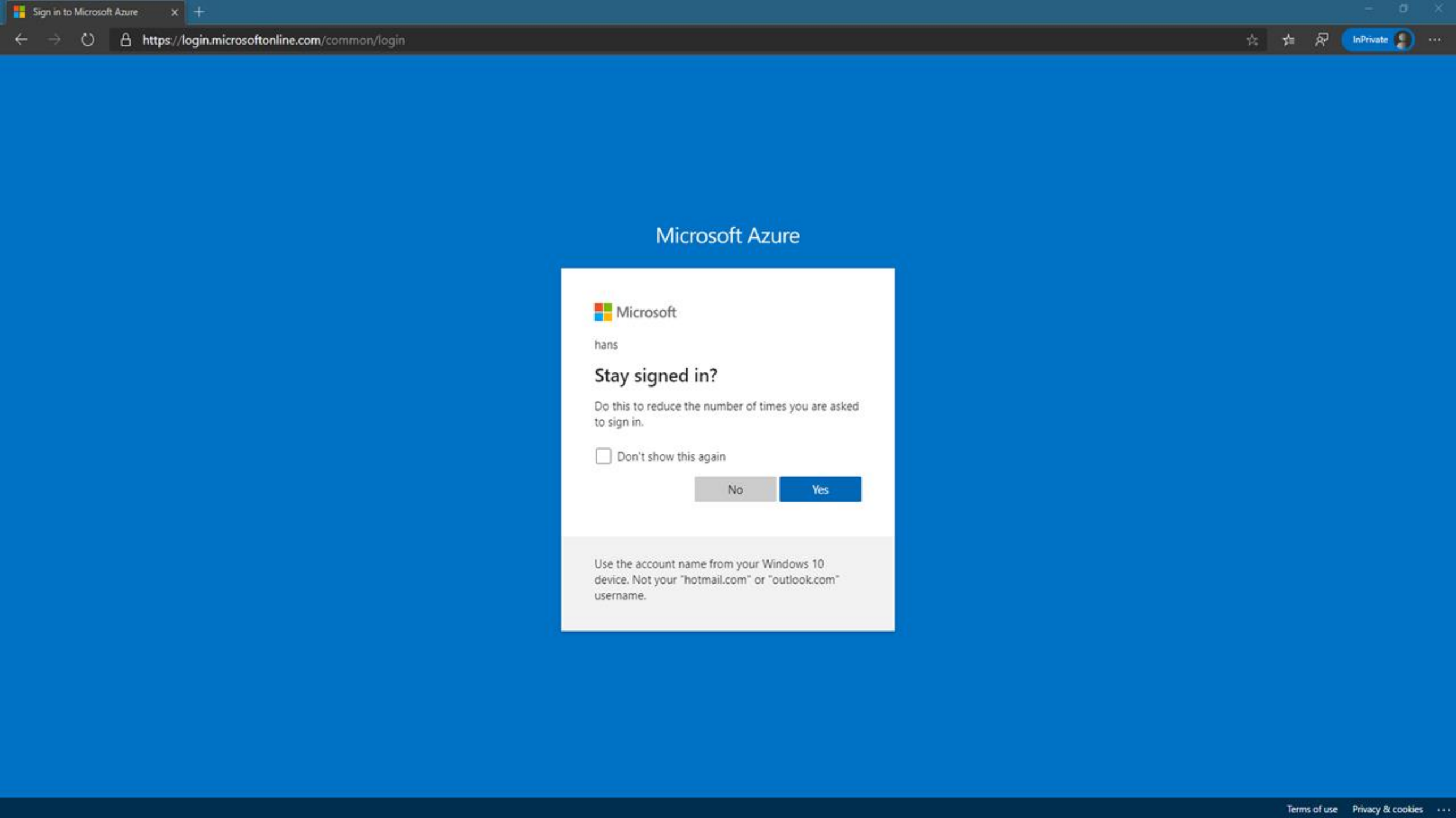
Alternate phone	+32	Change	Delete
Phone	+32	Change	Delete
Microsoft Authenticator	H's iPhone 11 Pro		Delete
Microsoft Authenticator	Hans's iPad Pro		Delete
Microsoft Authenticator	Hans's iPhone 8		Delete
Microsoft Authenticator	SM-T810		Delete
Security key	Feitian K26 (USB-C)		Delete
Security key	Security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


New tab
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


Sign in to Microsoft Azure
https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize?client_id=c44b4083-3bb0-49c1-b47d-974e53cbdf3c&response_mode=form_post&response_type=code+id_token&scope=ht...
InPrivate
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
Terms of use
Privacy & cookies


Sign in to your account
https://login.microsoft.com/common/fido/get?uiflavor=Web
InPrivate
Windows Security
Making sure it's you
Please sign in to login.microsoft.com.
This request comes from Msedge, published by Microsoft Corporation.
Insert your security key into the USB port.
Cancel
Terms of use
Privacy & cookies


Sign in to your account
https://login.microsoft.com/common/fido/get?uiflavor=Web
InPrivate
Windows Security
Making sure it's you
Please sign in to login.microsoft.com.
This request comes from Msedge, published by Microsoft Corporation.
Touch your security key.
Cancel
Terms of use
Privacy & cookies


Sign in to Microsoft Azure
https://login.microsoftonline.com/common/login
InPrivate
Microsoft Azure
Microsoft
hans
Stay signed in?
Do this to reduce the number of times you are asked to sign in.
Don't show this again
No
Yes
Use the account name from your Windows 10 device. Not your "hotmail.com" or "outlook.com" username.
Terms of use
Privacy & cookies

Dashboard - Azure Active Direct

https://aad.portal.azure.com

InPrivate

Azure Active Directory admin center

- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Groups
- Identity Governance
- App registrations
- Enterprise applications
- Azure AD Connect Health
- Azure AD Conditional Access
- Azure AD Identity Protection

Dashboard | New dashboard | Upload | Download | Edit | Full screen | Clone | Delete

Hans

Azure AD Premium P2

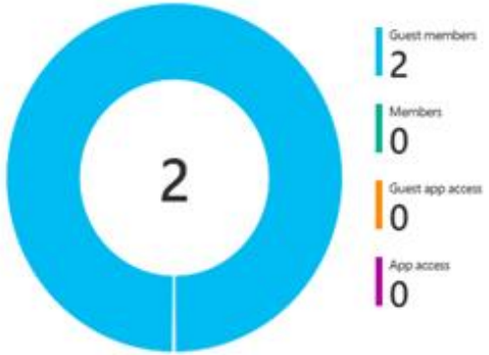
Welcome to the Azure AD admin center

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

Learn more about Azure AD

Risky users

Access reviews of



Access reviews status

Proxy

0

0

Quick tasks

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

Enterprise Mobility + Security

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

Azure portal

portal.azure.com

Audit Logs

View activity

What's new

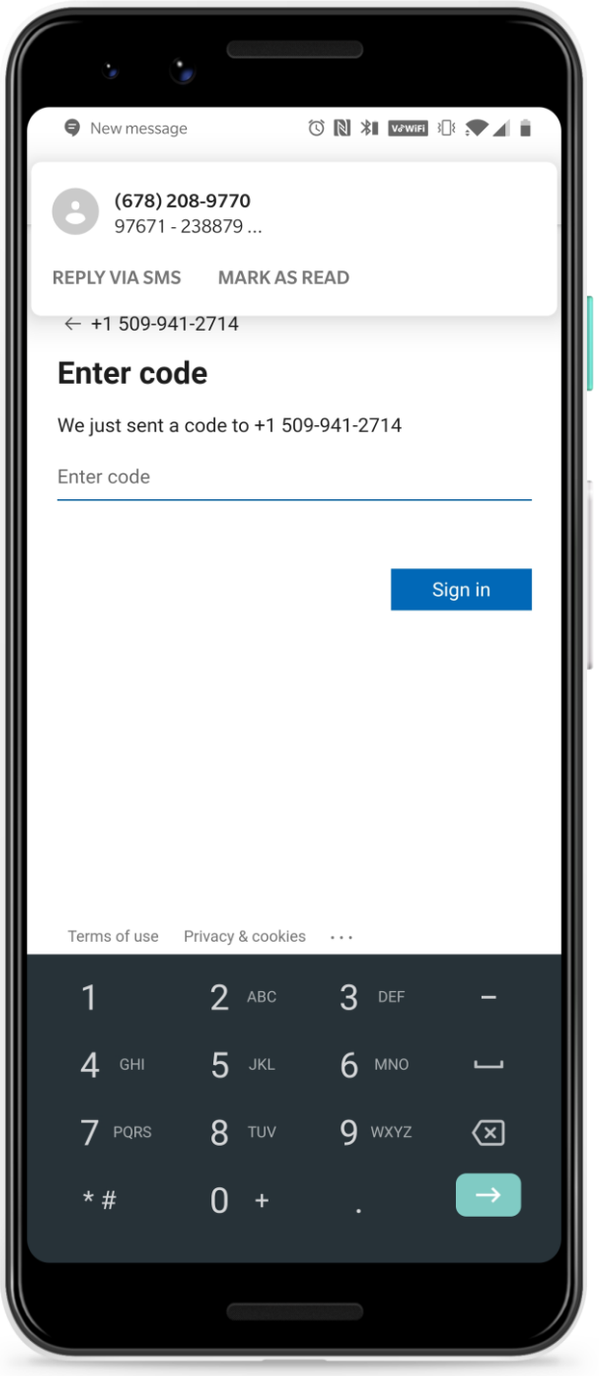
Azure AD makes the leaders quadrant in Gartner's 2017 Magic Quadrant for Access Management

Azure Information Protection (formerly Rights Management Service) is available in the Azure portal

The new Azure AD admin console is GA

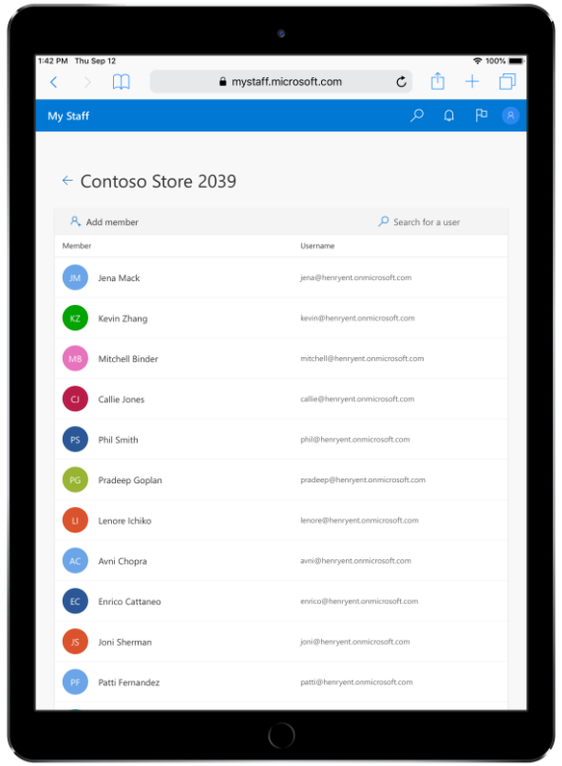
New! SMS Sign-In

Public Preview



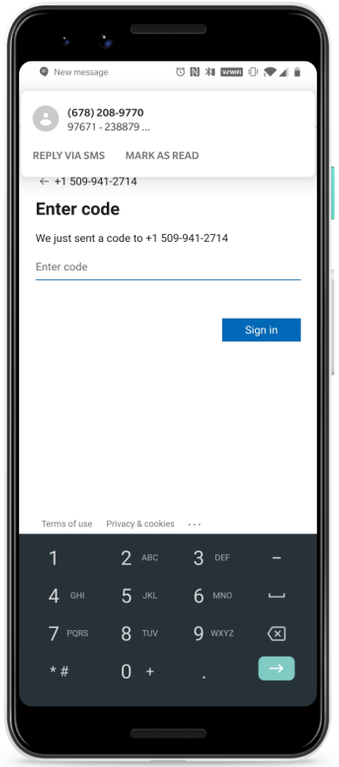
Azure AD · Firstline Worker

Public Preview



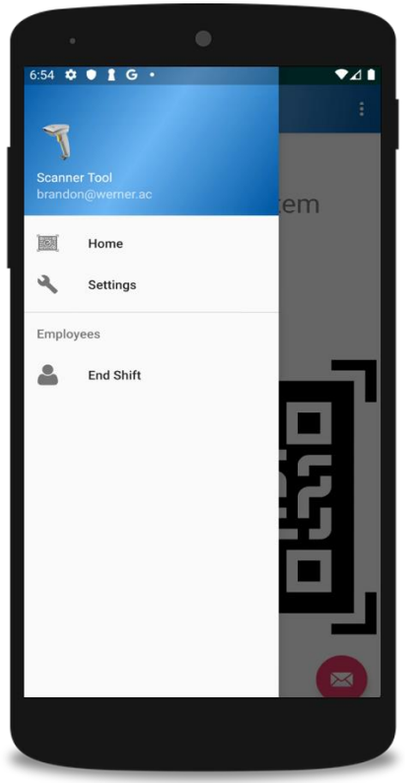
My Staff

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.

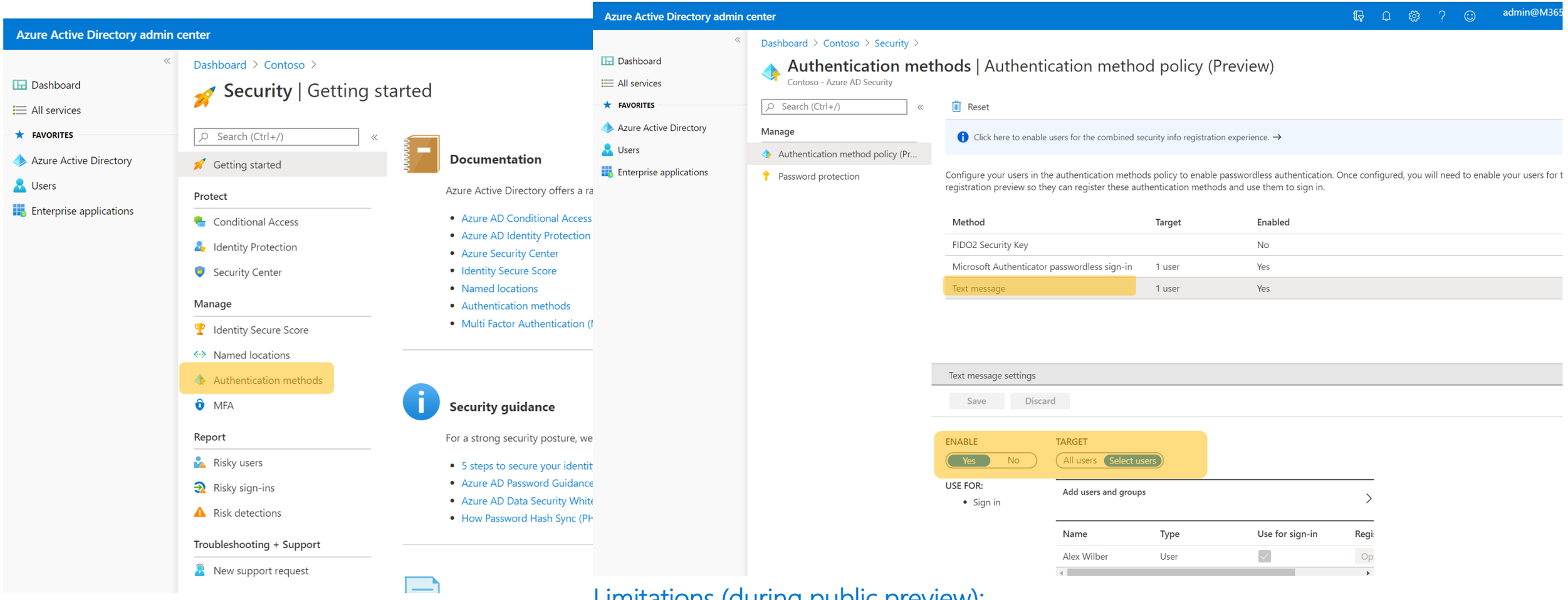


Global sign out

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

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/new-identity-features-help-empower-essential-firstline-workers/ba-p/1257356

How to enable SMS Sign-In?



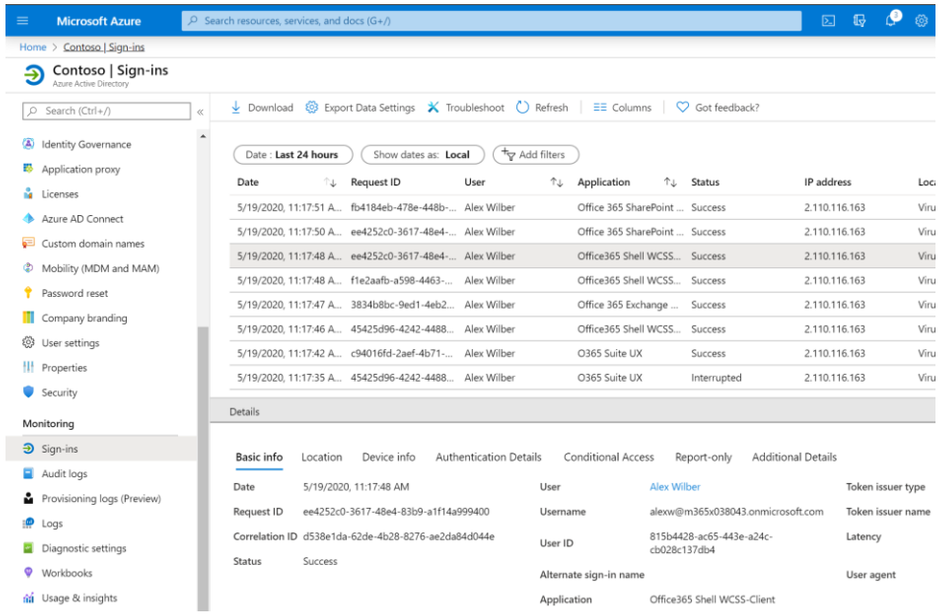
Limitations (during public preview):

- 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.

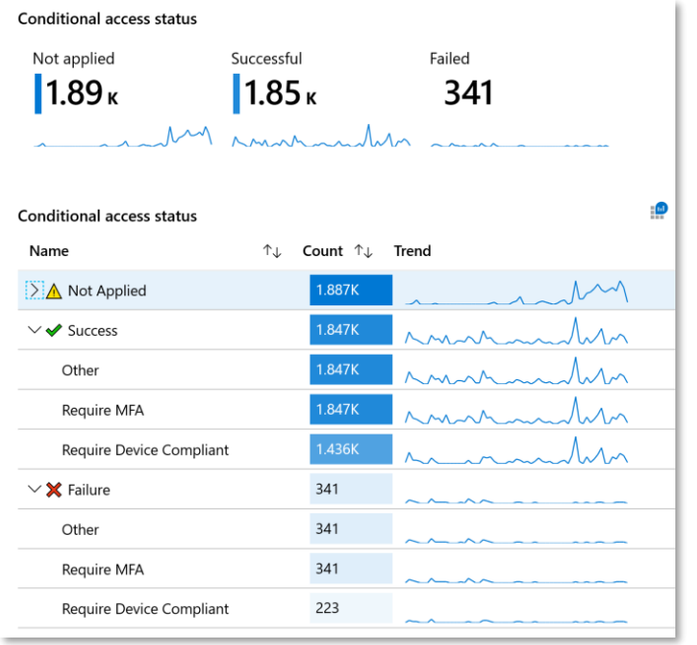
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-sms-signin

SMS sign-in is risky – Monitoring is key

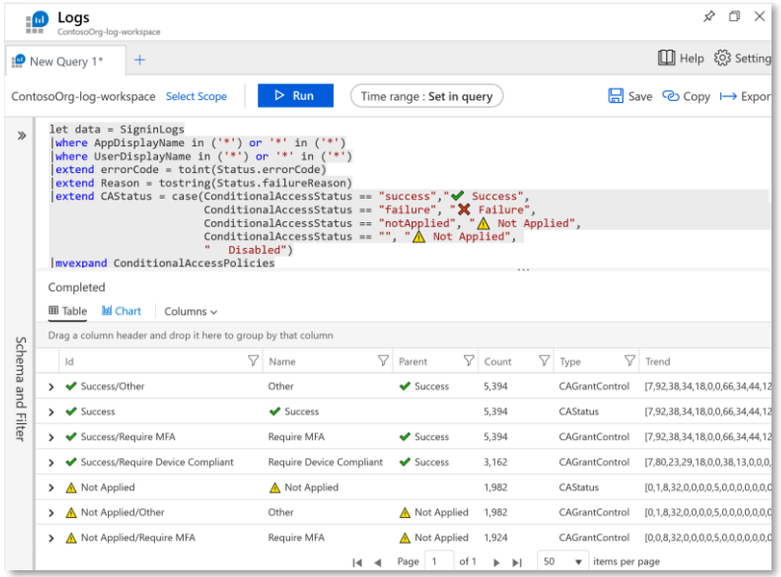
Azure AD sign-in logs



Azure Monitor built-in dashboards



Export Queries to use in Azure Sentinel



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.

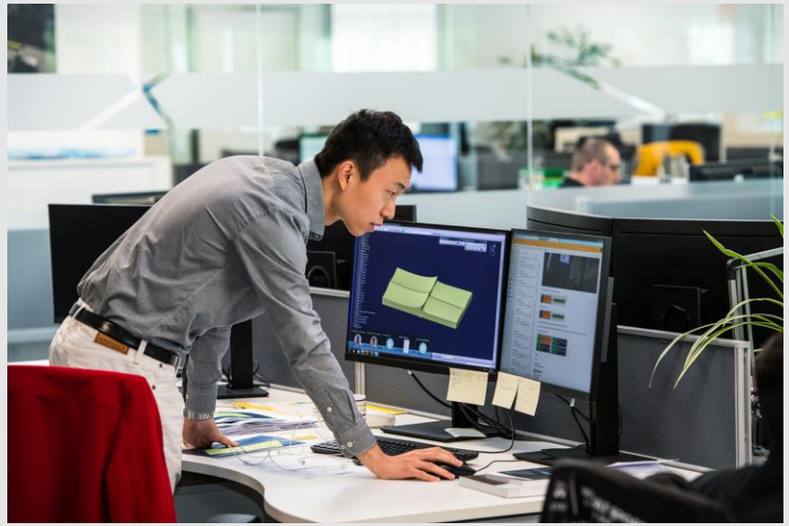
  Try Microsoft Authenticator phone sign-in for added mobility.

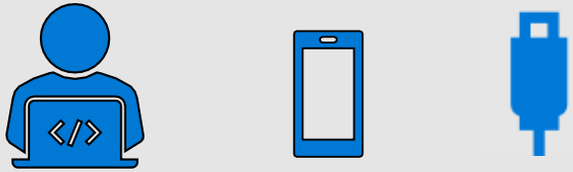
  Pilot FIDO2 security keys

  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
Computer sign in: From assigned Windows 10 device	No	Yes With biometric, PIN	Yes With biometric recognition and/or PIN
Computer sign in: From shared Windows 10 device	No	Yes With biometric, PIN	No
Web app sign-in: from a user-dedicated computer	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
Web app sign-in: from a mobile or non-windows device	Yes	No	No
Computer sign in: Non-Windows computer	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

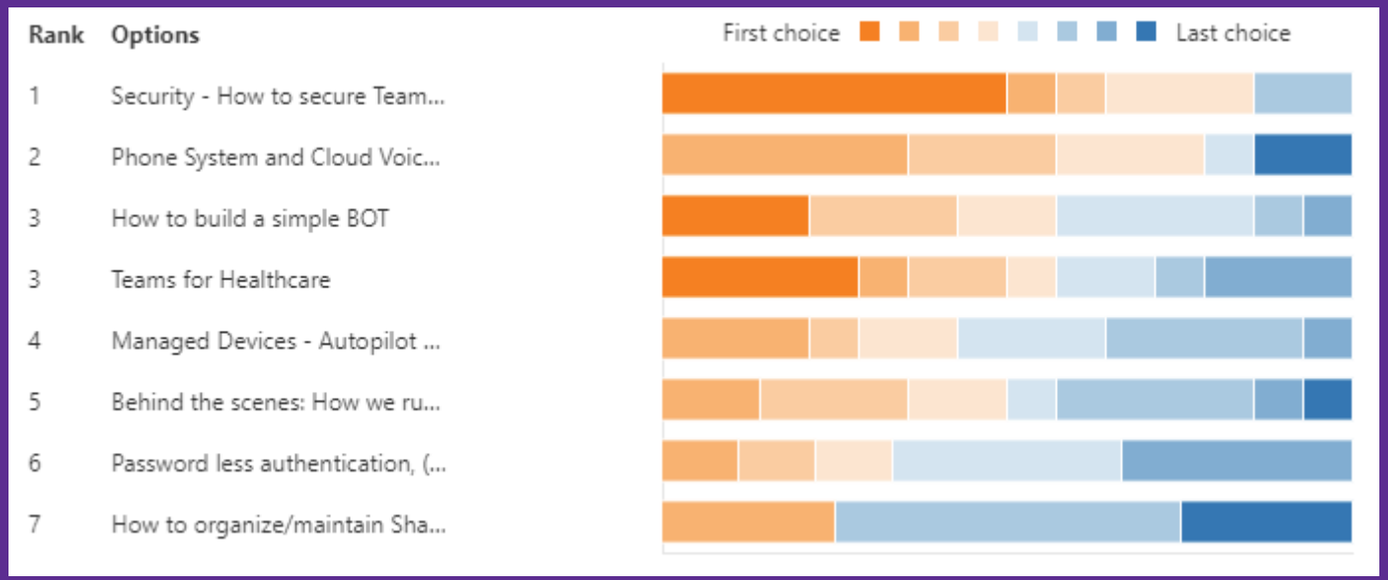
- https://aka.ms/gopasswordless

Open Q & A

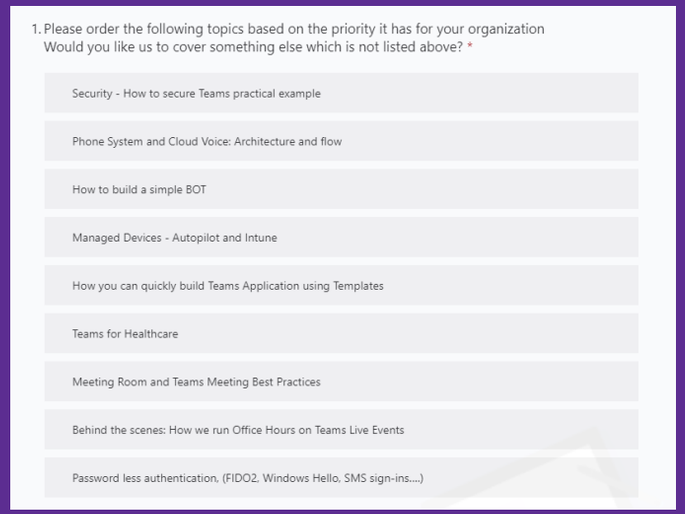
Please ask any question in the Q&A

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

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



Rank	Options
1	Security - How to secure Team...
2	Phone System and Cloud Voic...
3	How to build a simple BOT
3	Teams for Healthcare
4	Managed Devices - Autopilot ...
5	Behind the scenes: How we ru...
6	Password less authentication, (...
7	How to organize/maintain Sha...



1. Please order the following topics based on the priority it has for your organization
Would you like us to cover something else which is not listed above? *

- Security - How to secure Teams practical example
- Phone System and Cloud Voice: Architecture and flow
- How to build a simple BOT
- Managed Devices - Autopilot and Intune
- How you can quickly build Teams Application using Templates
- Teams for Healthcare
- Meeting Room and Teams Meeting Best Practices
- Behind the scenes: How we run Office Hours on Teams Live Events
- Password less authentication, (FIDO2, Windows Hello, SMS sign-ins....)

Sessions

Planned Sessions	Main Topics
Friday, May 29, 2020	The journey to Passwordless
Friday, June 5, 2020	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
  - **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**

https://aka.ms/WE-TechOfficeHours-Materials

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.

Microsoft

Thank You!