yubico

The key to trust

Entra ID Hybrid Quick Start

Introductions

Please share:

- Your entity
- Your role
- Number of YubiKeys you’re deploying
- Any specific needs of your deployment

Yubico’s Professional Services Team

Deployment Advisors

Molly Babcock

Laura Eppley

Jeff Olives

Engineers

Greg Whitney

Dante Melo

Mitchell Armenta

Kanchan Thakur

Scott Truger

Workshop Agenda

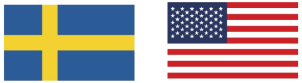
Topic	Estimated Duration
Welcome & Introductions	0:05
Concepts, YubiKey 101, and Entra Use Cases	0:15
Entra ID Tenant Configuration	0:25
Extending FIDO2 Authentication to Windows Logon	0:20
FIDO2 with RDP	0:05
Entra ID Sign-in Logs and Reporting	0:10
Redeeming Pro Services Hours Post-Workshop	0:05
Questions and Wrap-Up	0:05
Total	**1:30**

What is a YubiKey?

Technical Overview

Easy, Fast, & Reliable Authentication

YubiKey does not require a battery or network connection.



fido™ CERTIFIED FIDO2

Waterproof

Crush Resistant

Concepts and Use Cases

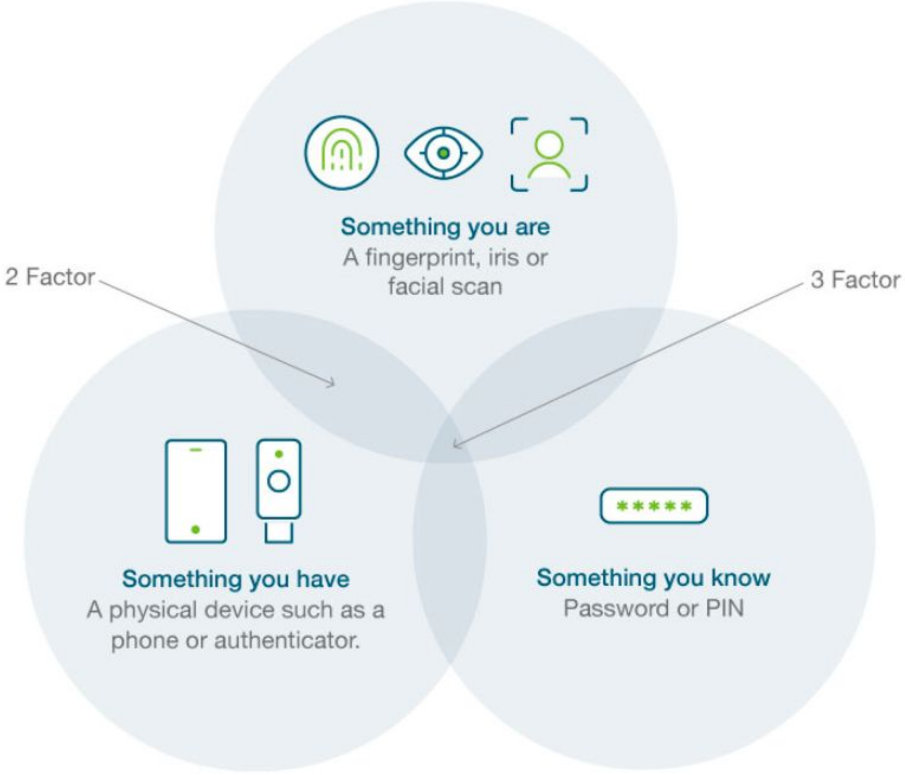
What is an Authentication Factor?

- Factors of authentication are something **you know** (knowledge), something **you have** (possession), and something **you are** (inherence)
- Something **you know** is most often a password or a PIN
- Something **you have** might be a bank card, OTP fob, or a YubiKey
- Something **you are** comprises biometric uniqueness, like your fingerprint or iris

What is Multi-Factor Authentication?

- Multi-factor authentication is a process of identifying yourself (proving you are who you say you are) that involves multiple authentication factors
- Although username and password authentication involves two components (the username and password) it is **not** multi-factor authentication because both components are something you know. This is instead single-factor authentication
- Performing a cash withdrawal at an ATM using a bank card typically involves multi-factor authentication, as it involves something you have (the bank card), and something you know (the card’s PIN)

Authentication Factors



Something you are
A fingerprint, iris or facial scan

Something you have
A physical device such as a phone or authenticator.

Something you know
Password or PIN

2 Factor

3 Factor

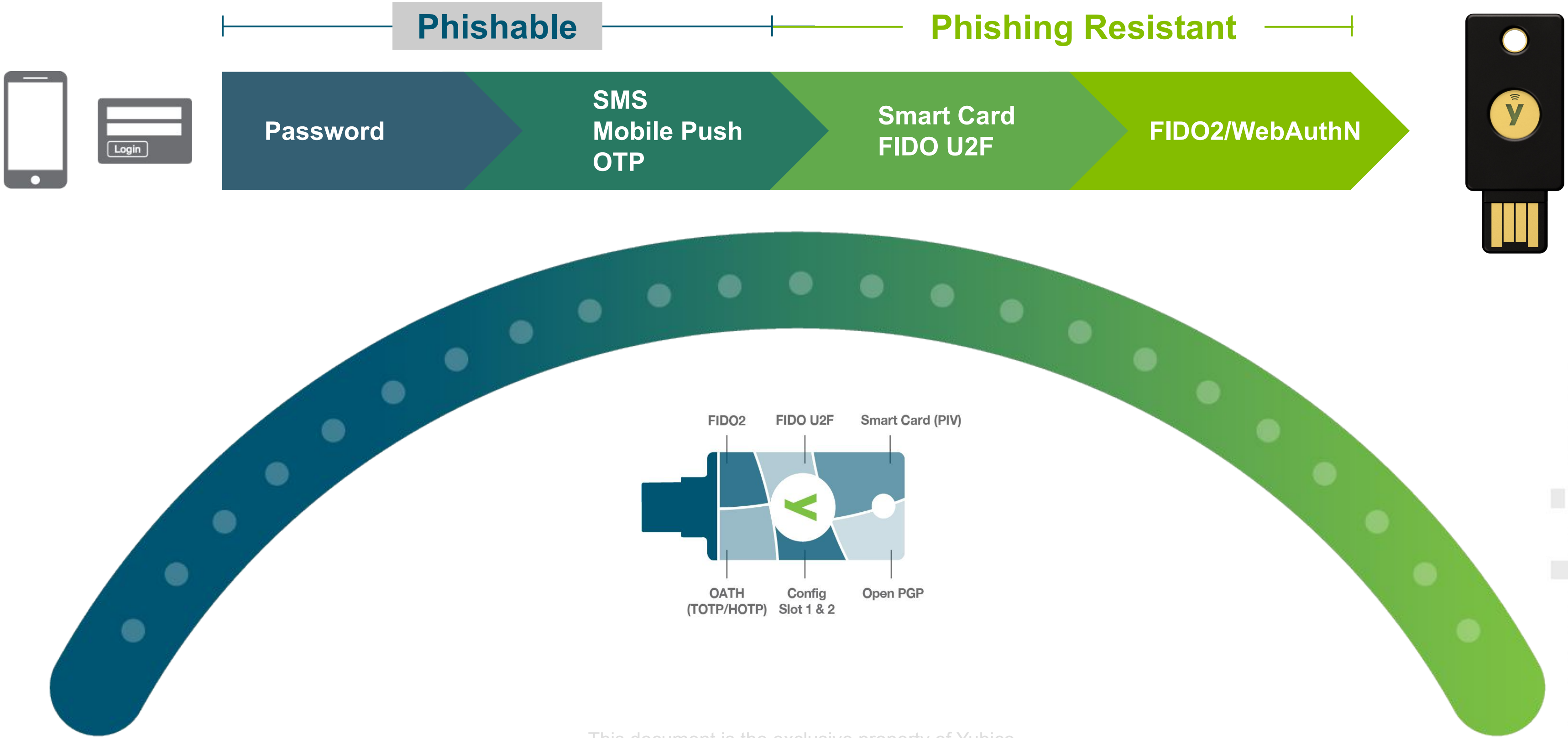
What is Phishing?

- Phishing is attempting to trick people into revealing personal information like passwords
- Phishing often comes in the form of email or text message, often written with a sense of urgency (you will lose access, your account will be terminated, etc.)

What is Phishing-Resistant MFA?

- Phishing-resistant MFA is a category of multi-factor authentication that is designed to be less vulnerable to phishing attacks
- As an example, FIDO/WebAuthn includes the domain name (origin) of the service being registered with in the registration
    - As a result, a FIDO/WebAuthn authentication request will not be successful if the domain name does not match that established at the time of registration
    - This is passive phishing protection. Even if users do not realize they are being phished, FIDO will not allow them to complete authentication, because the domain name will not match, as is often the case with phishing attempts

Phishing-Resistant MFA Illustrated



Phishable

Phishing Resistant

Password

SMS
Mobile Push
OTP

Smart Card
FIDO U2F

FIDO2/WebAuthN

FIDO2

FIDO U2F

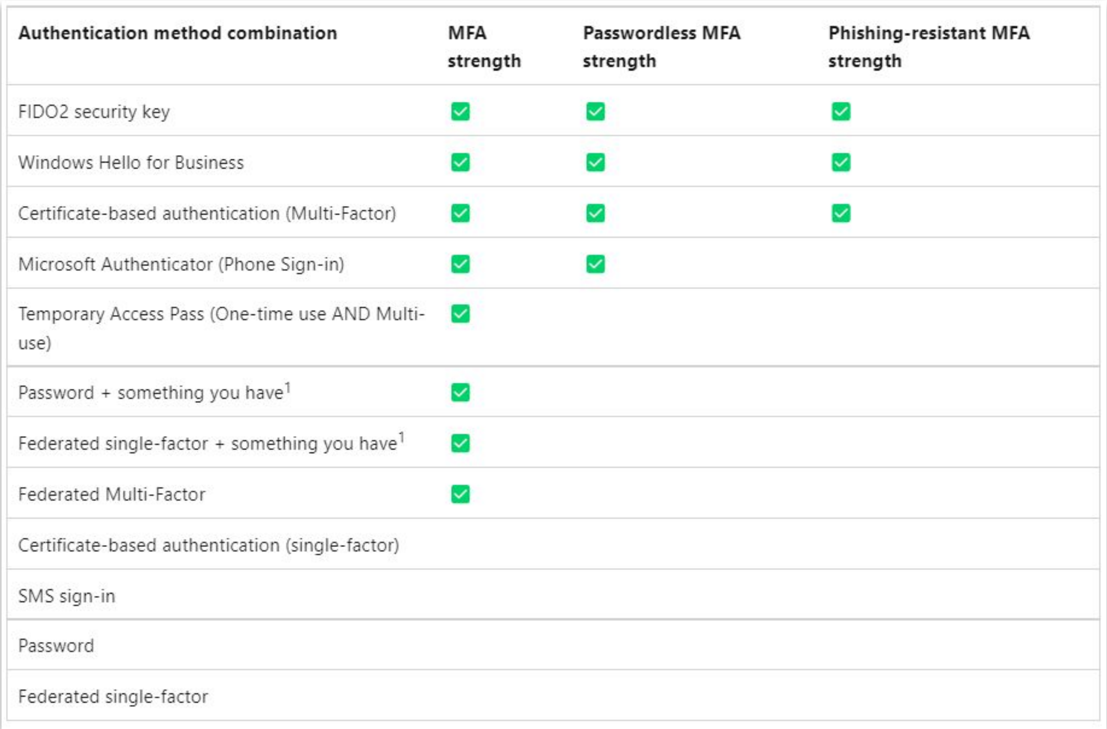
Smart Card (PIV)

OATH (TOTP/HOTP)

Config Slot 1 & 2

Open PGP

Strength of Various MFA in Entra ID



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

Source: Authentication methods

What is FIDO2?

- FIDO stands for **F**ast **ID**entity **O**nline, and began as a standard developed by multiple companies, including Yubico, with the vision of bringing strong public key cryptography to the mass market
- Originally, FIDO was FIDO U2F, or Universal **2**nd **F**actor
- FIDO2 builds upon U2F, facilitating the possibility of passwordless multi-factor authentication
- Based on public key cryptography, FIDO2 offers strong, phishing resistant authentication that does not depend on a public key infrastructure or other on-premises resources
- In Entra ID, FIDO2 registration can be:
  - Self-service - an existing method of MFA must be registered in order for a user to be able to register a FIDO2 authenticator
  - Done nn behalf of a user by using the YubiEnroll tool
  - Delivered pre-registered - For YubiKey Subscription customers only
- A FIDO2 credential is also known as a **Passkey**
- **Additional resources:**
  - WebAuthn Introduction and FIDO building blocks
  - What is FIDO2?
  - What is a Passkey?

Identity Provider (IdP)

- An **Identity Provider (IdP)** is a system that stores users' information, verifies their identity, and provides that information to other applications or services
- Benefits:
  - **Improved security** - IdPs often support advanced authentication methods like FIDO2 or passkeys, making it harder for hackers to gain access
  - **Single Sign-On (SSO)** - Users can access multiple applications with a single login, saving time and frustration
  - **Simplified User Management** - Administrators can easily manage user accounts, permissions, and access policies from a central location
- **Examples:** Entra ID, Okta, Google, Active Directory

YubiKey 101

YubiKey Authentication Protocols

- The YubiKey is an authenticator
- It supports several authentication protocols

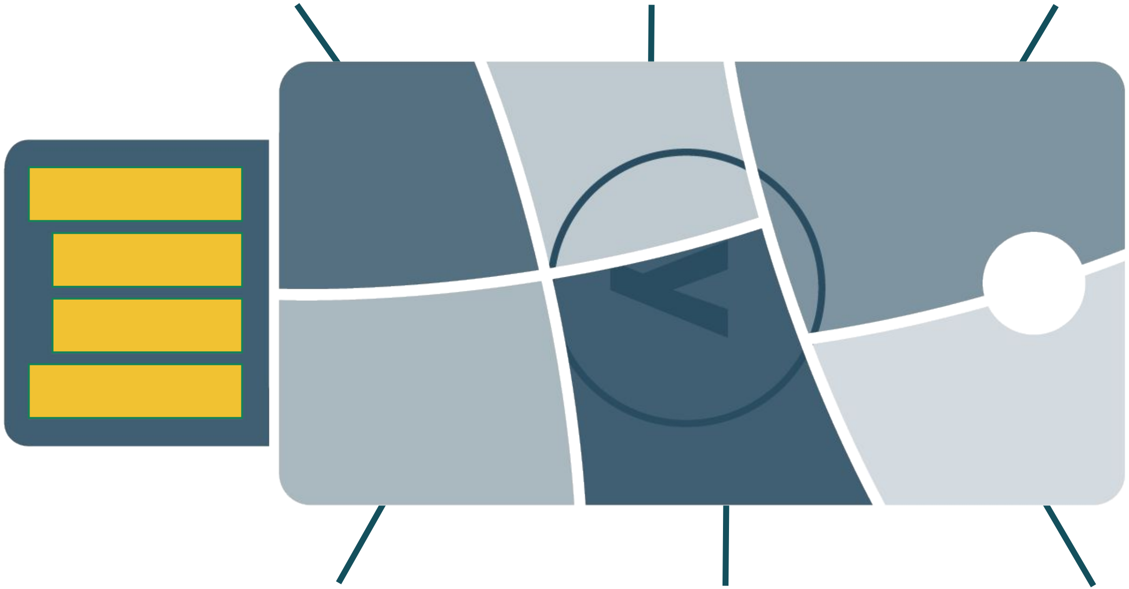
Shared secrets/symmetric crypto	**Asymmetric crypto**
Challenge-Response	OpenPGP
OATH TOTP, HOTP	PIV smart card
Yubico OTP	FIDO U2F, **FIDO2**

YubiKey Multiple Protocol Support

FIDO2

FIDO U2F

Smart Card (PIV)



OATH (TOTP/HOTP)

Config Slot 1 and 2

OpenPGP

Config Slot 1 + 2
Yubico OTP
OATH-HOTP
Challenge-Response
Static Credential

YubiKey Interfaces

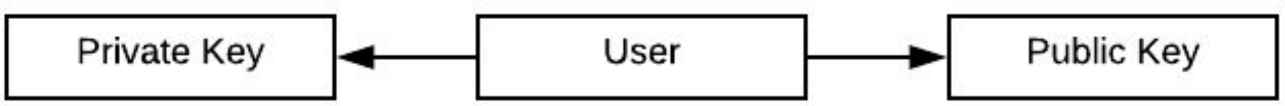
- The YubiKey is a hardware security device
- The physical interfaces are Universal Serial Bus (USB) and Near-FIeld Communication (NFC)
- The USB interface provides 3 types of channels:
  - The OTP interface presents itself to the operating system as a USB keyboard
  - The FIDO interface presents itself as a generic Human Interface Device (HID)
  - The CCID interface presents itself to the operating system as a USB Smart Card Reader
- The NFC interface provides all applications (in a slightly different way, since an NFC reader is in the middle)

Symmetric Cryptography

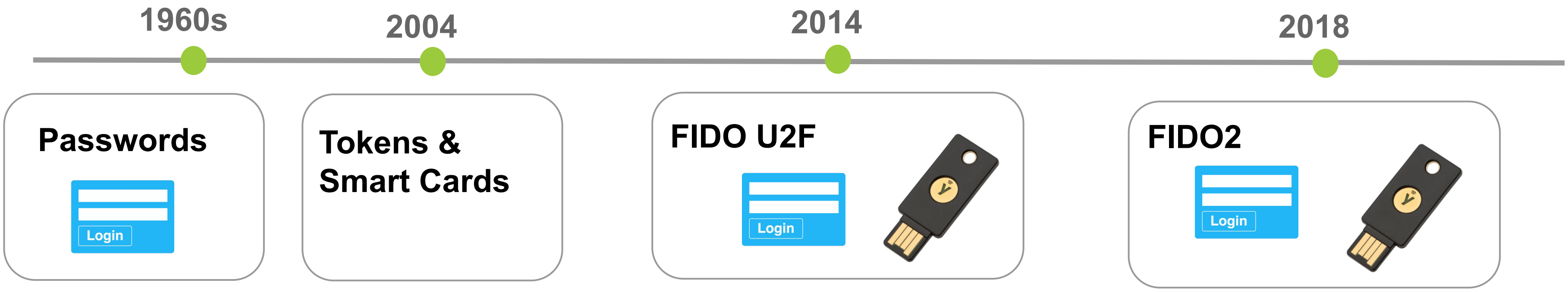
- Symmetric cryptography: same key is used to encrypt and decrypt
- Both parties need to have a copy of the key
- This means both the user and the Credential Service must have a copy of the key

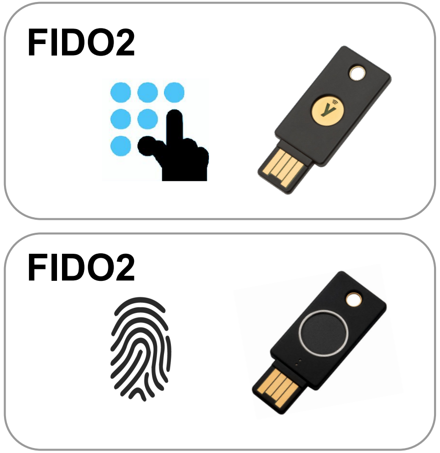
Public Key Cryptography

- Here the parties have key pairs (public, private)
- Also known as “asymmetric cryptography”
- It is not feasible to find the private key from the public key
- The user keeps the private key protected, and shares the public key with Relying Parties



Authentication Progression





FIDO (Fast Identity Online)

- Strong two factor authentication
- One key to many services
- Strong phishing defense
- No client software, native support
- Deprecated 2022

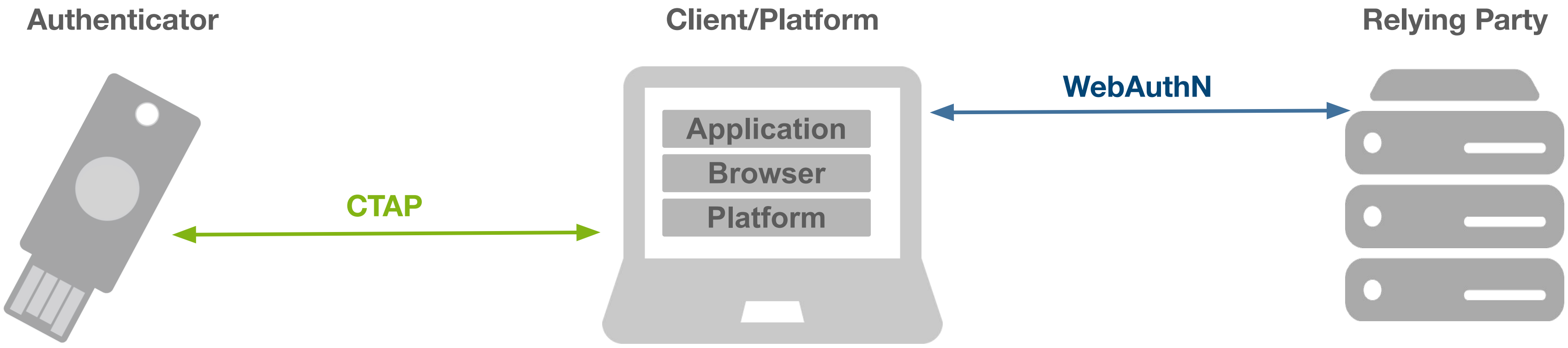
Google yubico

yubico
Microsoft Google

FIDO2 Summary

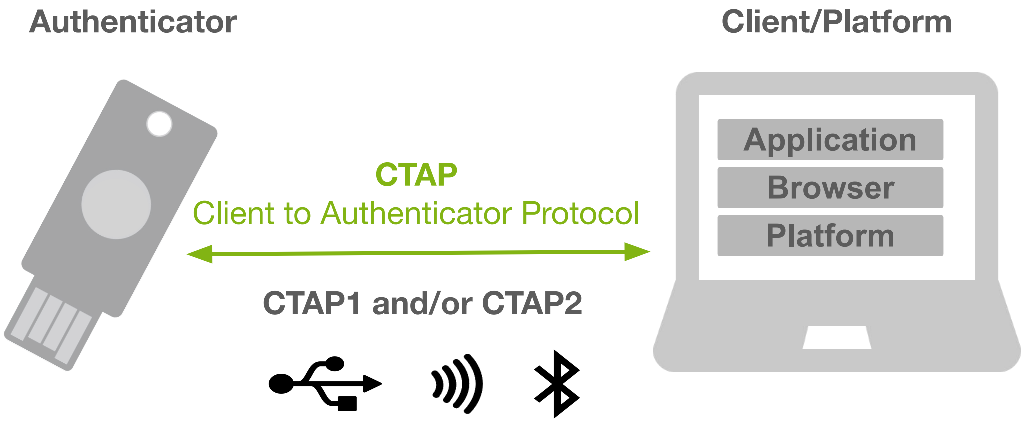
- Allows login securely without a password
  - Strong layered security multi-factor authentication
  - Strong defense against phishing and Man in the Middle (MitM) attacks
  - High usability with rapid login (usernameless and passwordless)
- Built into widely adopted platforms (e.g. Windows) and on track for standardization via W3C, with support by all major browsers (e.g. Google, Mozilla, Edge, etc.)
- Includes the features of the original FIDO U2F

How FIDO2 Authentication Works



- **FIDO2 = CTAP + WebAuthn**
- A set of open standards utilizing public-key cryptography to enable strong first factor, second and multi-factor authentication

What is CTAP?



Authenticator

Client/Platform

CTAP

Client to Authenticator Protocol

CTAP1 and/or CTAP2

Application

Browser

Platform

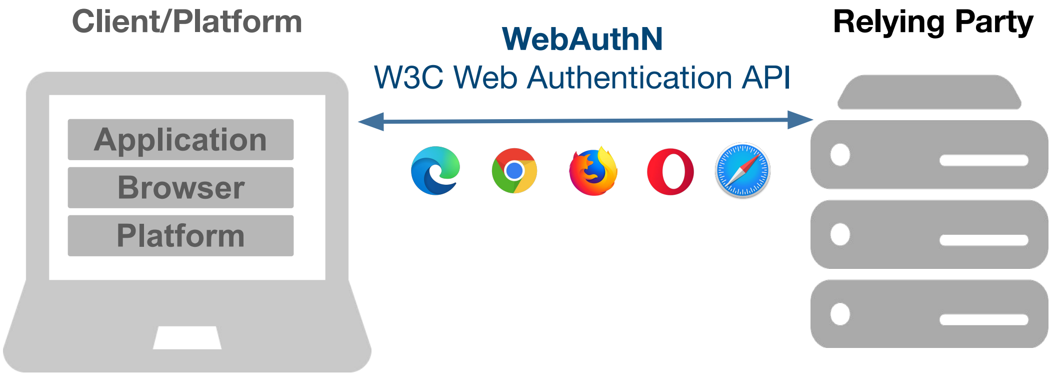
Application layer protocol used to communicate between an external authenticator (i.e. security key) and a client (desktop) or a platform (OS)

Authenticator generates and securely stores credentials

Private keys, PINs, and biometric information never leave the authenticator

Communicates over USB, NFC, and Bluetooth

What is WebAuthn?



Specification that enables the creation and use of strong public key-based credentials by web applications

Strongly authenticate users

Major browsers are on track to implement full Web Authentication APIs

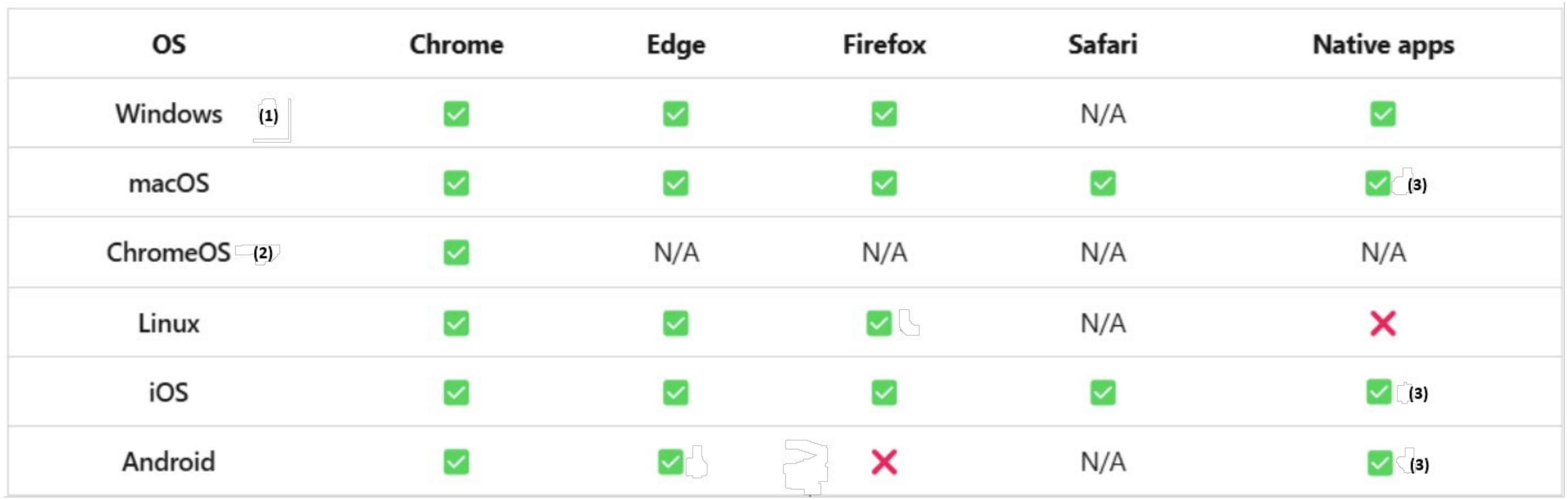
Includes FIDO2, allowing backwards compatibility of FIDO U2F with capable authenticators

Entra ID FIDO2 Authentication Use Cases and Requirements

Entra ID Use Cases

- In-browser logon to applications that use Entra ID as their IdP
- Logon to Windows 10/11 machines, either natively or hybrid joined to Entra ID
  - On-prem AD-joined only machines are not eligible for FIDO2 OS logon
- RDP logon to Windows 10/11, Windows Server 2022/2025 machines joined to Entra ID either natively or hybrid
- Mobile devices in-browser logon
- Mobile devices native apps logon

Prerequisites - Browser Authentication



OS	Chrome	Edge	Firefox	Safari	Native apps
Windows (1)	✓	✓	✓	N/A	✓
macOS	✓	✓	✓	✓	✓ (3)
ChromeOS (2)	✓	N/A	N/A	N/A	N/A
Linux	✓	✓	✓	N/A	✗
iOS	✓	✓	✓	✓	✓ (3)
Android	✓	✓	✗	N/A	✓ (3)

- (1) Requires Windows 10 version 1903 or higher
- (2) Security key registration is currently not supported with ChromeOS. NFC is not supported.
- (3) Requires an authentication broker to be installed on the user's device. Some Microsoft native apps support passkey authentication without an authentication broker.
- Source: [Passkey (FIDO2) authentication matrix with Microsoft Entra ID]

Windows and macOS Support

Windows:

- Best sign-in experience with Windows 11 version 22H2 or later.
- Requires:
  - Windows 10 version 1903 or later
  - Chromium-based Microsoft Edge
  - Chrome 76 or later
  - Firefox 66 or later
- Microsoft Graph PowerShell supports passkey.
- Some PowerShell modules that use IE do not support FIDO2:
  - PS module for SharePoint Online
  - PS module for Teams
  - Any PS scripts that require admin credentials
  - Workaround: Use CBA

macOS:

- Requires macOS Catalina 11.1 or later with Safari 14 or later for autnetication (user verification (UV) support = PIN or biometrics)
- NFC and BLE security keys are not supported on macOS by Apple.
  - Note: YubiKeys don’t support BLE
- New Security key registration is currently not supported:
  - No UV support during registration
  - Only supported if the key already has a PIN set
- If you registered more than 3 passkeys, sign in with a passkey might not work on Safari

Linux and Chrome OS Support

Linux:

- Sign-in with passkey in Microsoft Authenticator isn't supported in Firefox on Linux

ChromeOS:

- NFC and BLE security keys are not supported
  - Note: YubiKeys don’t support BLE
- Security key registration is not supported

iOS and Android Support

iOS:

- Passkey authentication requires iOS 14.3 or later (UV support)
- BLE security keys aren't supported on iOS by Apple:
  - Note: YubiKeys don’t support BLE
- New Security key registration is currently not supported:
  - No UV support during registration
  - Only supported if the key already has a PIN set
- If you registered more than 3 passkeys, sign in with a passkey might not work
- NFC with FIPS 140-3 certified security keys isn't supported on iOS by Apple

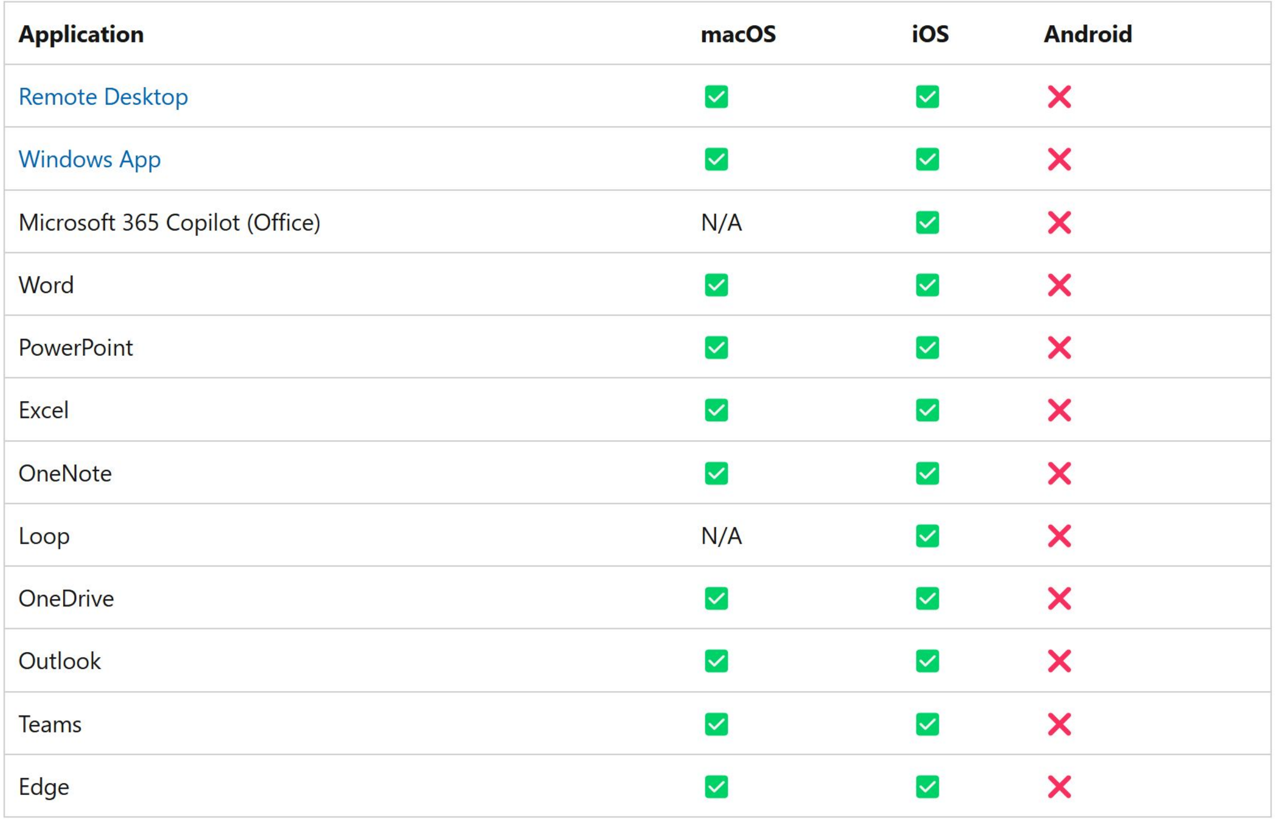
Android:

- Requires Google Play Services 21 or later (UV support)
- BLE security keys aren't supported on Android by Google:
  - Note: YubiKeys don’t support BLE
- Security key registration with Microsoft Entra ID is not currently supported
- Sign-in with passkey isn't supported in Firefox

Native Application

- Passkey authentication for native applications may require an “authentication broker”:
  - iOS: Microsoft Authenticator
  - macOS: Microsoft Intune Company Portal
  - Android: Authenticator or Microsoft Intune Company Portal
- macOS:
  - Microsoft Enterprise Single Sign On (SSO) plug-in is required to enable Company Portal as an authentication broker.
  - SSO plug-in requires macOS 14.0 or later
- iOS:
  - Sign-in with passkey in native apps without Microsoft Enterprise Single Sign On (SSO) plug-in requires iOS 16.0 or later.
  - Sign-in with passkey in native apps with the SSO plug-in requires iOS 17.1 or later.
- Android:
  - Sign-in with FIDO2 security key to native apps requires Android 13 or later.
  - Sign-in with passkey in Microsoft Authenticator to native apps requires Android 14 or later.
  - Sign-in with YubIKeys with YubiOTP enabled might not work on Samsung Galaxy devices. Workaround: Disable YubiOTP.

Microsoft Native Application Support Without Authentication Broker



Application	macOS	iOS	Android
Remote Desktop	✅	✅	❌
Windows App	✅	✅	❌
Microsoft 365 Copilot (Office)	N/A	✅	❌
Word	✅	✅	❌
PowerPoint	✅	✅	❌
Excel	✅	✅	❌
OneNote	✅	✅	❌
Loop	N/A	✅	❌
OneDrive	✅	✅	❌
Outlook	✅	✅	❌
Teams	✅	✅	❌
Edge	✅	✅	❌

Entra ID Tenant Configuration

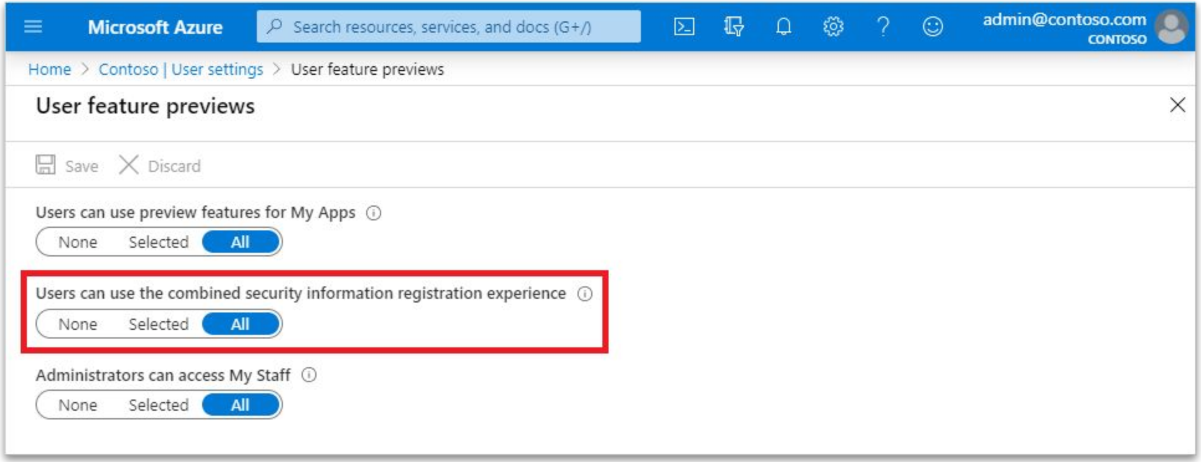
Enabling FIDO2 Authentication in Entra ID

- Combined Registration Experience must be enabled:
  - Combines the registration of authentication methods for Entra ID MFA and Self-Service Password Reset (SSPR)
  - Effective October 1st, 2022, Microsoft started enabling combined registration experience in Entra ID tenants created before August 15th, 2020
  - Tenants created on or after August 15th, 2020 are enabled with combined registration experience enabled for all users
- **Instructions**: Enable combined security information registration in Entra ID

Enabling FIDO2 Authentication in Entra ID

Enable Combined Registration Experience:

1. Sign in to the Azure portal as a User Administrator or Global Administrator
2. Go to Microsoft Entra ID > Users> User settings > Manage user feature settings
3. Under Users can use the combined security information registration experience, choose to enable for a Selected group of users or for All users


Microsoft Azure
Search resources, services, and docs (G+/)
admin@contoso.com
CONTOSO
Home > Contoso | User settings > User feature previews
Save
Discard

User feature previews

Users can use preview features for My Apps: None Selected [✓ All]

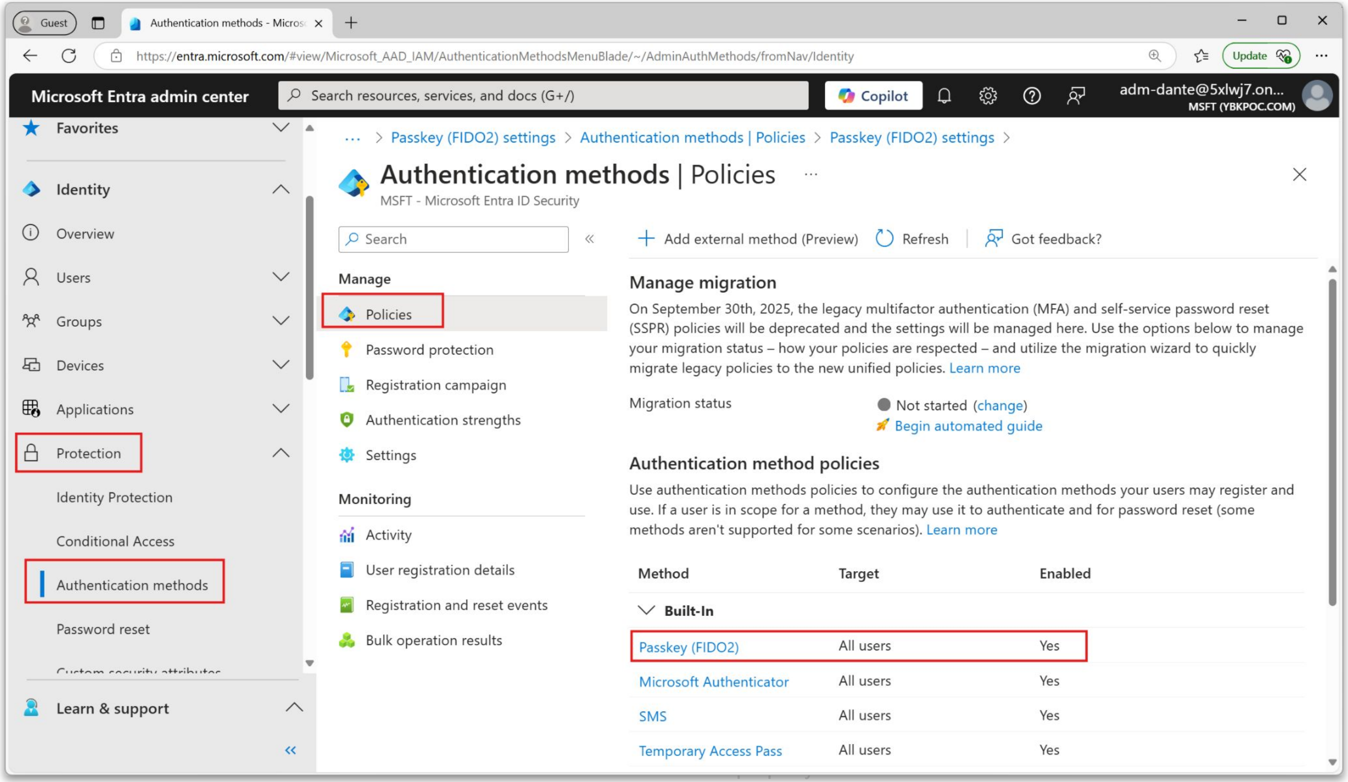
Users can use the combined security information registration experience: None Selected [✓ All]

Administrators can access My Staff: None Selected [✓ All]

Note: If the tenant has already been enabled for Combined Registration Experience, you might not see the configuration option or it might be grayed out.

Enabling FIDO2 Authentication in Entra ID

https://entra.microsoft.com


Guest
Authentication methods - Micros
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/AdminAuthMethods/fromNav/Identity
Update
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
adm-dante@5xlwj7.on...
MSFT (YBKPOC.COM)
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Learn & support
... > Passkey (FIDO2) settings > Authentication methods | Policies > Passkey (FIDO2) settings >
Authentication methods | Policies
MSFT - Microsoft Entra ID Security
Search
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results
Add external method (Preview)
Refresh
Got feedback?

Manage migration

On September 30th, 2025, the legacy multifactor authentication (MFA) and self-service password reset (SSPR) policies will be deprecated and the settings will be managed here. Use the options below to manage your migration status – how your policies are respected – and utilize the migration wizard to quickly migrate legacy policies to the new unified policies. Learn more

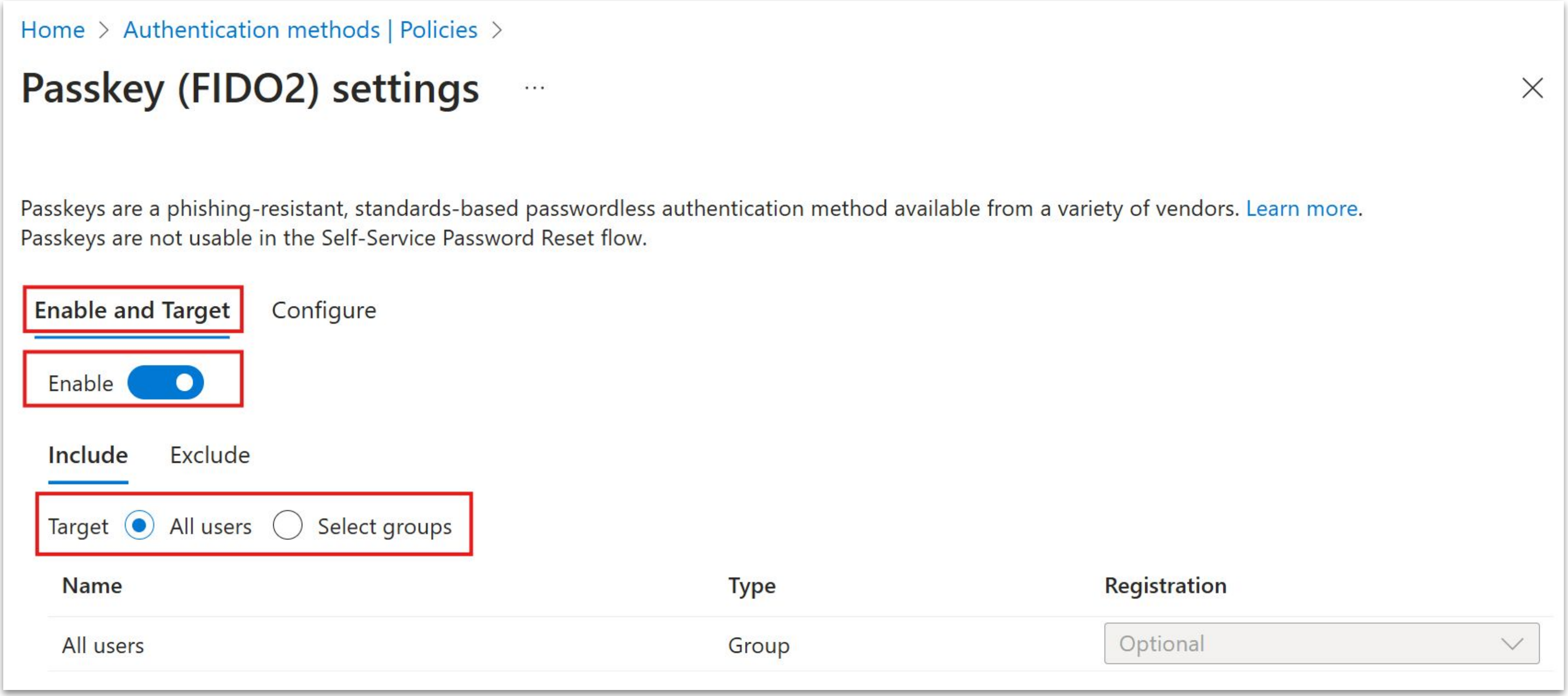
Migration status: ● Not started (change)
Begin automated guide

Authentication method policies

Use authentication methods policies 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

Method	Target	Enabled
Built-In		
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users	Yes
SMS	All users	Yes
Temporary Access Pass	All users	Yes

Enabling FIDO2 Authentication in Entra ID



Home > Authentication methods | Policies >

Passkey (FIDO2) settings ...

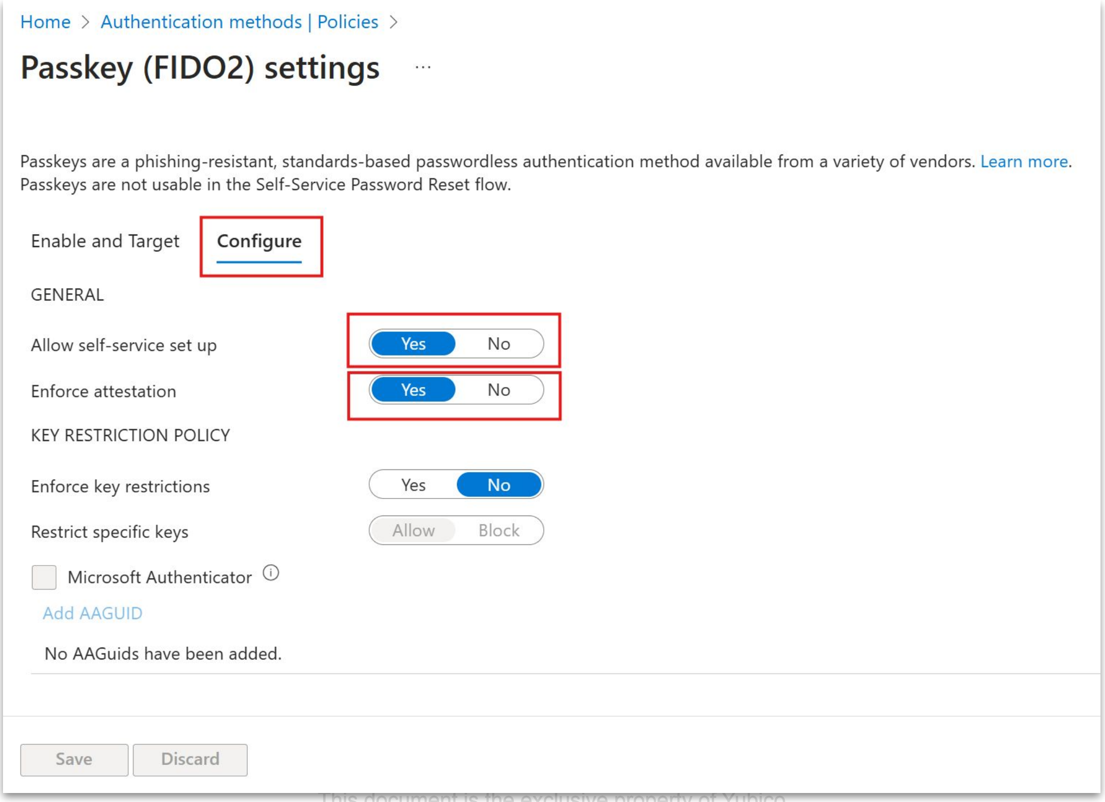
Passkeys are a phishing-resistant, standards-based passwordless authentication method available from a variety of vendors. Learn more.
Passkeys are not usable in the Self-Service Password Reset flow.

Enable: on

Target ● All users ○ Select groups

Name	Type	Registration
All users	Group	Optional

Enabling FIDO2 Authentication in Entra ID



Home > Authentication methods | Policies >

Passkey (FIDO2) settings ...

Passkeys are a phishing-resistant, standards-based passwordless authentication method available from a variety of vendors. Learn more.
Passkeys are not usable in the Self-Service Password Reset flow.

Enable and Target | [✓ Configure]

GENERAL

Allow self-service set up [✓ Yes] No

Enforce attestation [✓ Yes] No

KEY RESTRICTION POLICY

Enforce key restrictions Yes [✓ No]

Restrict specific keys Allow Block

□ Microsoft Authenticator ⓘ

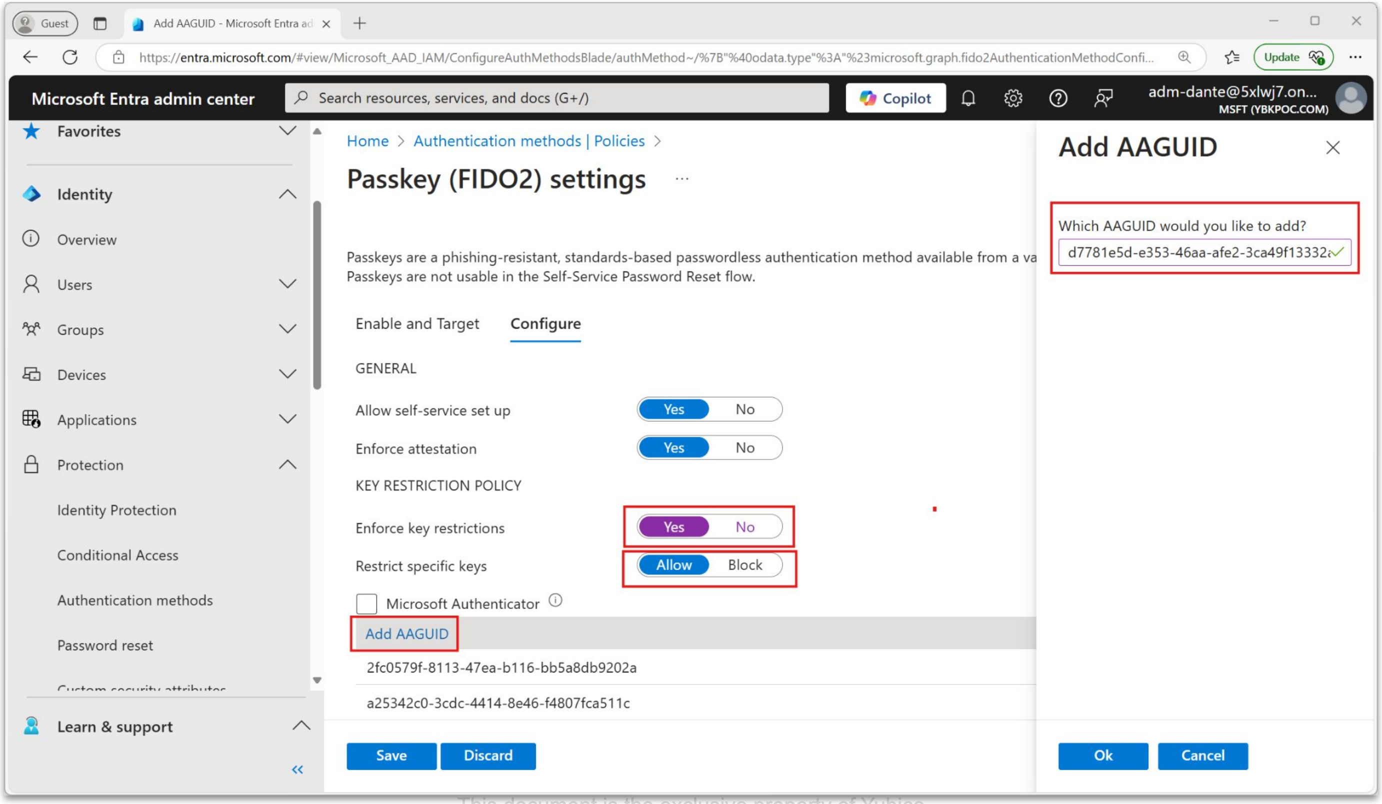
Add AAGUID

No AAGuids have been added.

AAGUID Filtering

- Authenticator Attestation Globally Unique IDentifier
  - 128-bit identifier indicating the type of the authenticator and firmware version
  - Examples:
    - Non-FIPS YubiKey 5 NFC (Firmware 5.2 & 5.4): 2fc0579f-8113-47ea-b116-bb5a8db9202a
    - Non-FIPS YubiKey 5 NFC (Firmware 5.7): a25342c0-3cdc-4414-8e46-f4807fca511c & d7781e5d-e353-46aa-afe2-3ca49f13332a
- Entra ID allows you to control which FIDO2 Security Keys can be used by either:
  - Only Allowing Keys with specific AAGUID
  - Blocking Keys with specific AAGUID
- You can only Allow or Block a list, not both
- **Reference: YubiKey Hardware FIDO2 AAGUIDs**

AAGUID Filtering


Guest
Add AAGUID - Microsoft Entra ad
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/ConfigureAuthMethodsBlade/authMethod~/%7B"%40odata.type"%3A"%23microsoft.graph.fido2AuthenticationMethodConfi...
Update
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
adm-dante@5xlwj7.on...
MSFT (YBKPOC.COM)
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Learn & support
Home > Authentication methods | Policies >

Passkey (FIDO2) settings

Passkeys are a phishing-resistant, standards-based passwordless authentication method available from a va
Passkeys are not usable in the Self-Service Password Reset flow.

Enable and Target | Configure

GENERAL

Allow self-service set up: [✓ Yes] No

Enforce attestation: [✓ Yes] No

KEY RESTRICTION POLICY

Enforce key restrictions: [✓ Yes] No

Restrict specific keys: [✓ Allow] Block

□ Microsoft Authenticator ⓘ

Add AAGUID

2fc0579f-8113-47ea-b116-bb5a8db9202a

a25342c0-3cdc-4414-8e46-f4807fca511c

Save | Discard

Add AAGUID

Which AAGUID would you like to add?

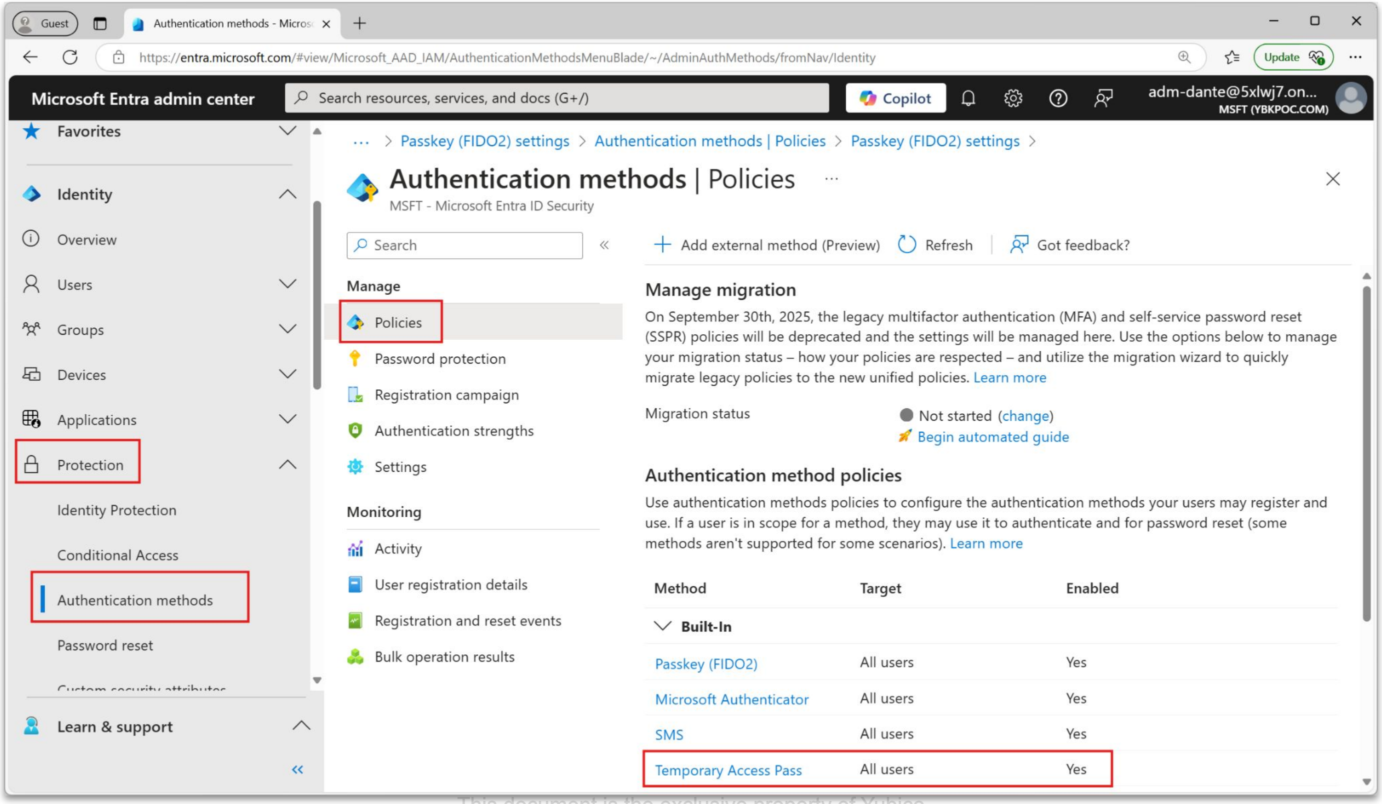
d7781e5d-e353-46aa-afe2-3ca49f13332a ✓

Ok | Cancel

Temporary Access Pass - TAP

- TAP is a time-limited passcode that can be configured for multi or single use to allow users to onboard other authentication methods
- Registering a FIDO2 security key requires an initial form of MFA be set up
- TAP can satisfy this, in addition to other Entra ID MFA methods like the Microsoft Authenticator App
- Can also be used in account recovery scenarios (e.g. lost YubiKey)
- Typically used in-browser, but can also be used in a limited scope for Windows authentication (e.g. new device setup)
- **Instructions:** Configure Temporary Access Pass in Entra ID to register Passwordless authentication methods

Enabling TAP


Guest
Authentication methods - Micros
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/AdminAuthMethods/fromNav/Identity
Update
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
adm-dante@5xlwj7.on...
MSFT (YBKPOC.COM)
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Learn & support
... > Passkey (FIDO2) settings > Authentication methods | Policies > Passkey (FIDO2) settings >
Search
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results
Add external method (Preview)
Refresh
Got feedback?

Authentication methods | Policies

MSFT - Microsoft Entra ID Security

Manage migration

On September 30th, 2025, the legacy multifactor authentication (MFA) and self-service password reset (SSPR) policies will be deprecated and the settings will be managed here. Use the options below to manage your migration status – how your policies are respected – and utilize the migration wizard to quickly migrate legacy policies to the new unified policies. Learn more

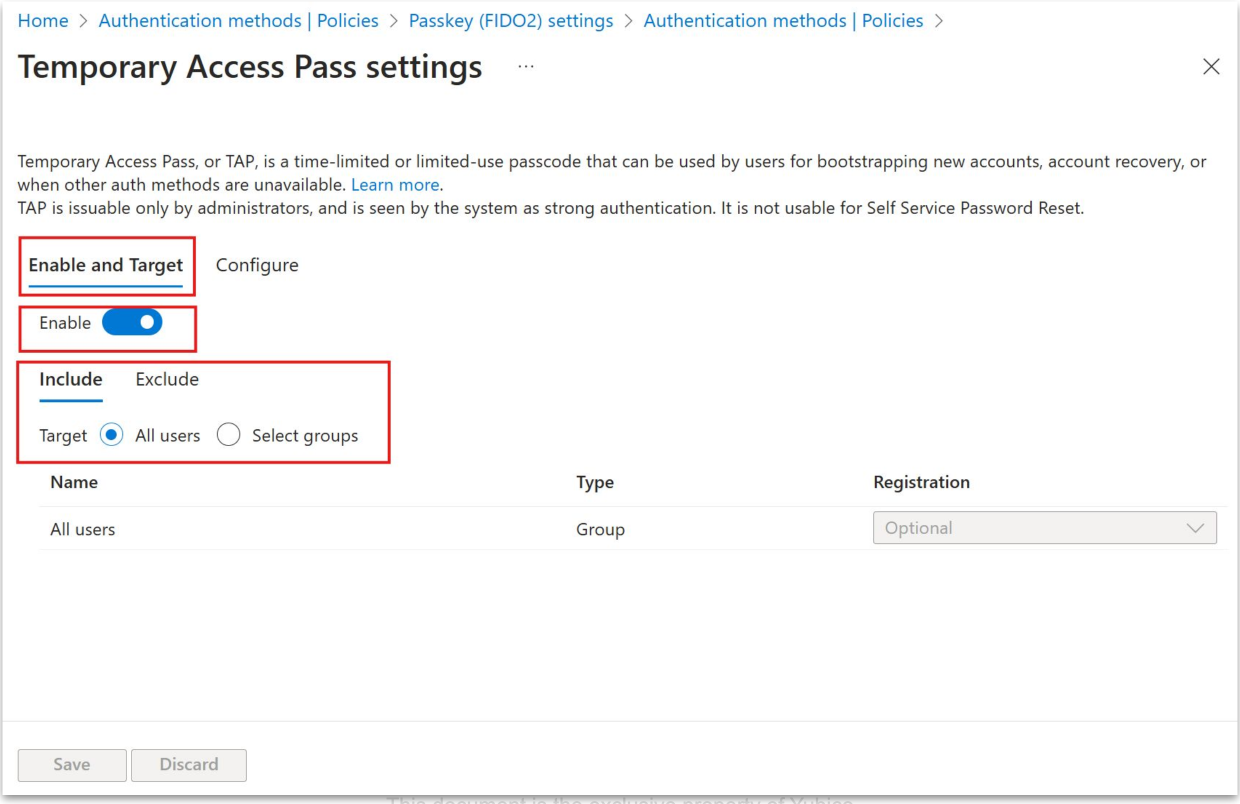
Migration status: ● Not started (change)
Begin automated guide

Authentication method policies

Use authentication methods policies 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

Method	Target	Enabled
Built-In		
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users	Yes
SMS	All users	Yes
Temporary Access Pass	All users	Yes

Enabling TAP



Home > Authentication methods | Policies > Passkey (FIDO2) settings > Authentication methods | Policies >

Temporary Access Pass settings

Temporary Access Pass, or TAP, is a time-limited or limited-use passcode that can be used by users for bootstrapping new accounts, account recovery, or when other auth methods are unavailable. Learn more.

TAP is issuable only by administrators, and is seen by the system as strong authentication. It is not usable for Self Service Password Reset.

Enable and Target | Configure

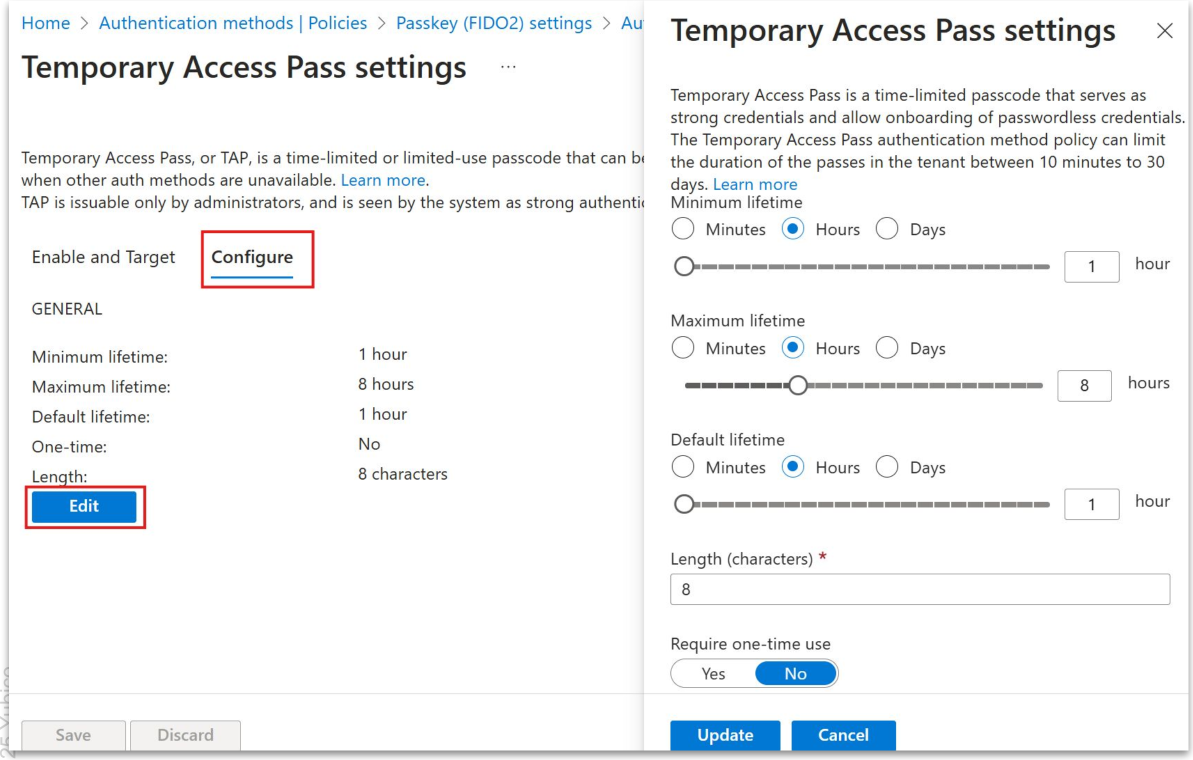
Enable: on

Include | Exclude

Target ● All users ○ Select groups

Name	Type	Registration
All users	Group	Optional

Enabling TAP



Home > Authentication methods | Policies > Passkey (FIDO2) settings > Au

Temporary Access Pass settings ...

Temporary Access Pass, or TAP, is a time-limited or limited-use passcode that can be when other auth methods are unavailable. Learn more.
TAP is issuable only by administrators, and is seen by the system as strong authenti

Enable and Target | Configure

GENERAL

Minimum lifetime:	1 hour
Maximum lifetime:	8 hours
Default lifetime:	1 hour
One-time:	No
Length:	8 characters

Edit

Save Discard

Temporary Access Pass settings

Temporary Access Pass is a time-limited passcode that serves as strong credentials and allow onboarding of passwordless credentials. The Temporary Access Pass authentication method policy can limit the duration of the passes in the tenant between 10 minutes to 30 days. Learn more

Minimum lifetime
○ Minutes ● Hours ○ Days
1 hour

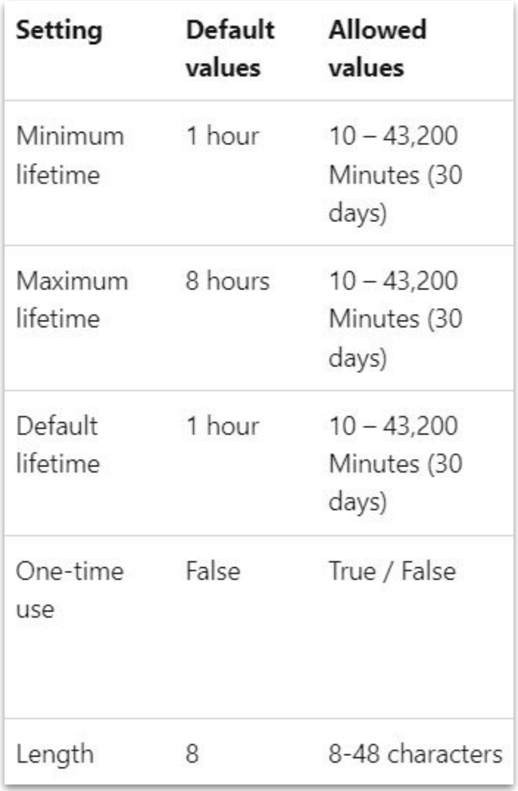
Maximum lifetime
○ Minutes ● Hours ○ Days
8 hours

Default lifetime
○ Minutes ● Hours ○ Days
1 hour

Length (characters) *
8

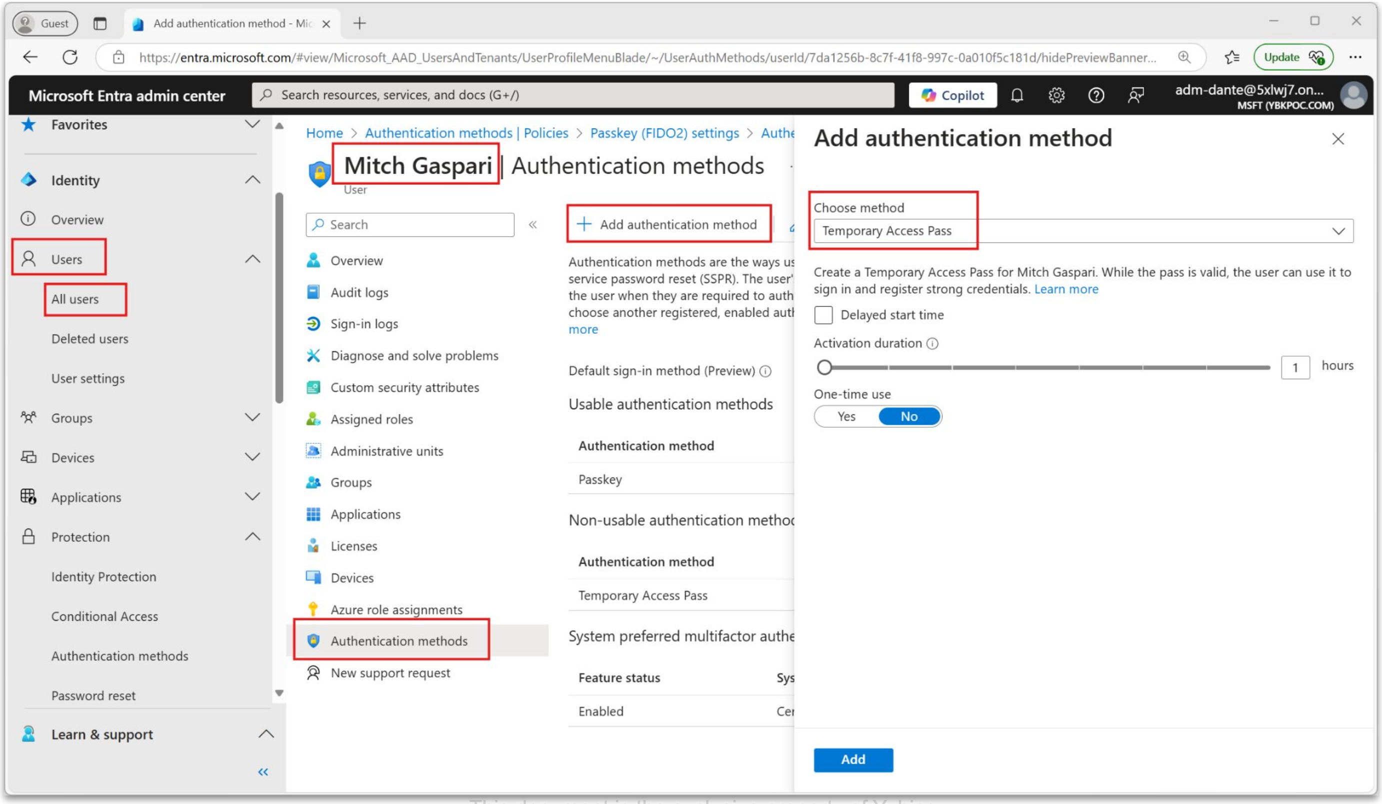
Require one-time use
Yes [✓ No]

Update Cancel



Setting	Default values	Allowed values
Minimum lifetime	1 hour	10 – 43,200 Minutes (30 days)
Maximum lifetime	8 hours	10 – 43,200 Minutes (30 days)
Default lifetime	1 hour	10 – 43,200 Minutes (30 days)
One-time use	False	True / False
Length	8	8-48 characters

Creating a TAP


Guest
Add authentication method - Mic
https://entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/UserAuthMethods/userId/7da1256b-8c7f-41f8-997c-0a010f5c181d/hidePreviewBanner...
Update
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
adm-dante@5xlwj7.on...
MSFT (YBKPOC.COM)
Favorites
Identity
Overview
Users
All users
Deleted users
User settings
Groups
Devices
Applications
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Learn & support
Home > Authentication methods | Policies > Passkey (FIDO2) settings > Authe
Mitch Gaspari | Authentication methods
User
Search
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
New support request
+ Add authentication method

Authentication methods are the ways us
service password reset (SSPR). The user'
the user when they are required to auth
choose another registered, enabled auth
more

Default sign-in method (Preview)

Usable authentication methods

Authentication method
Passkey

Non-usable authentication methoc

Authentication method
Temporary Access Pass

System preferred multifactor authe

Feature status	Sys
Enabled	Cer

Add authentication method

Choose method: Temporary Access Pass

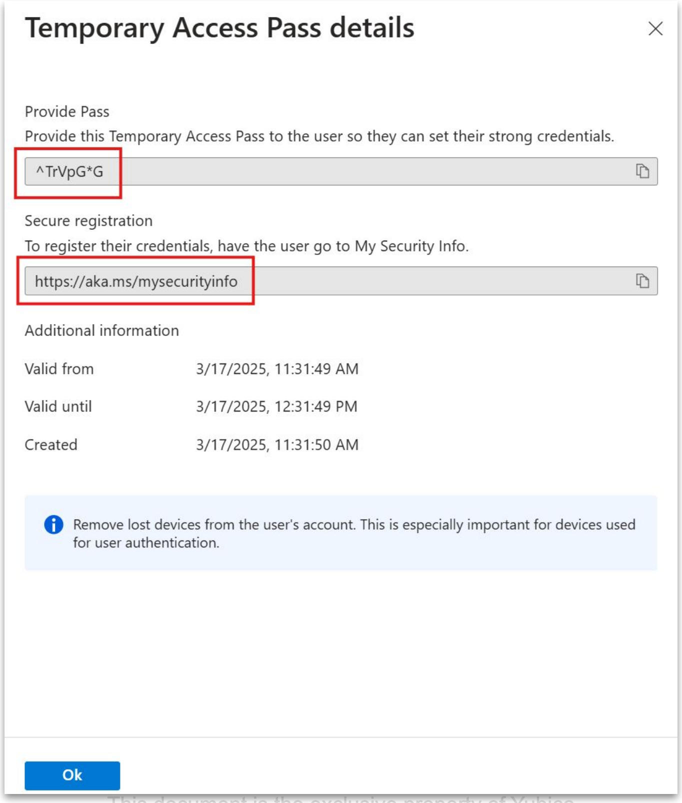
Create a Temporary Access Pass for Mitch Gaspari. While the pass is valid, the user can use it to sign in and register strong credentials. Learn more

□ Delayed start time

Activation duration: 1 hours

One-time use: Yes [✓ No]

Creating a TAP



Temporary Access Pass details

Provide Pass

Provide this Temporary Access Pass to the user so they can set their strong credentials.

^TrVpG*G

Secure registration

To register their credentials, have the user go to My Security Info.

https://aka.ms/mysecurityinfo

Additional information

Valid from 3/17/2025, 11:31:49 AM

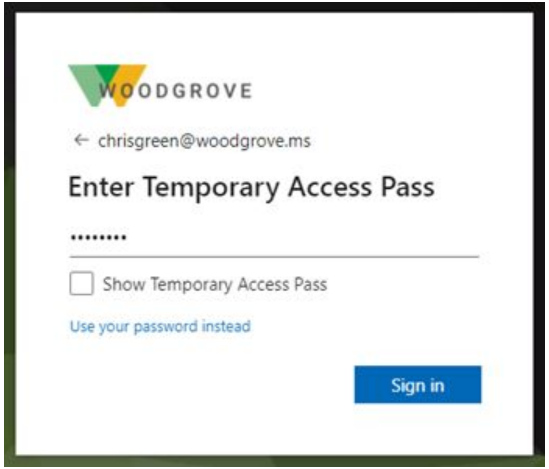
Valid until 3/17/2025, 12:31:49 PM

Created 3/17/2025, 11:31:50 AM

Remove lost devices from the user's account. This is especially important for devices used for user authentication.

TAP End-User Experience

1. Open a web browser to https://aka.ms/mysecurityinfo
2. Enter the UPN of the account for which you created the TAP
3. A dialog to enter the Temporary Access Pass will show up
4. Enter the TAP



WOODGROVE

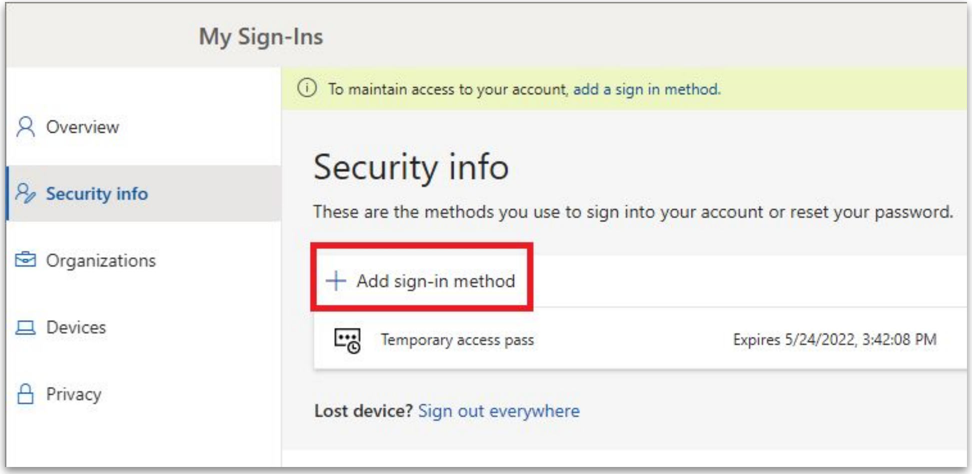
← chrisgreen@woodgrove.ms

Enter Temporary Access Pass

••••••••

□ Show Temporary Access Pass

Use your password instead



My Sign-Ins

ⓘ To maintain access to your account, add a sign in method.

Security info

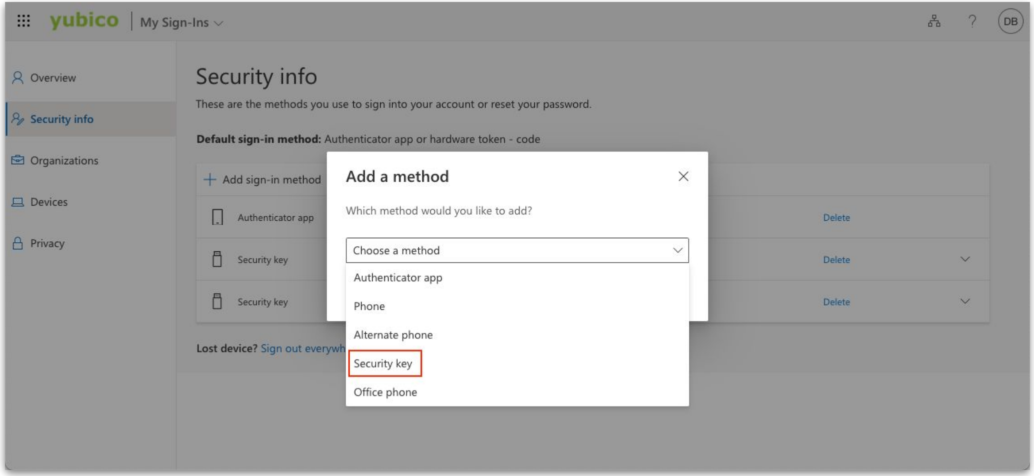
These are the methods you use to sign into your account or reset your password.

Temporary access pass — Expires 5/24/2022, 3:42:08 PM

Lost device? Sign out everywhere

YubiKey FIDO2 (Self) Registration

1. Open a web browser to https://aka.ms/mysecurityinfo
2. Authenticate using an existing MFA method
3. Click **Add sign-in method**
4. Select **Security key** and click **Add**
5. Select USB or NFC device, depending on how you are connecting your YubiKey
6. Click **Next**, then follow the on-screen prompts to create or enter your key's FIDO2 PIN, touch the key, provide it an identifying name (to be stored in Entra ID - up to 30 characters), and complete registration



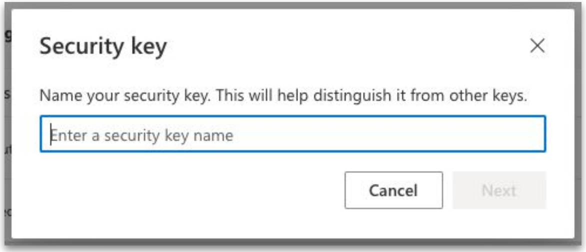
Security info

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

Default sign-in method: Authenticator app or hardware token - code

Which method would you like to add?

Lost device? Sign out everywh



Name your security key. This will help distinguish it from other keys.

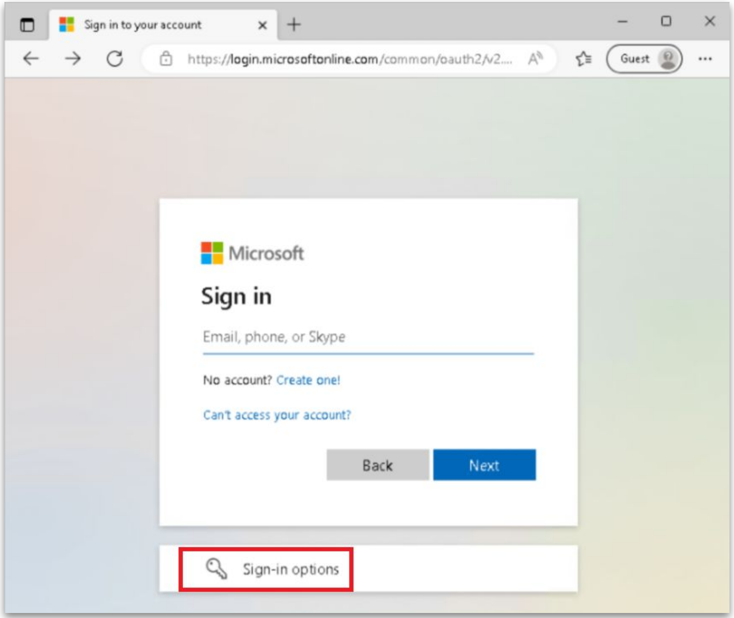
Enter a security key name

- Free-form field
- Recommend format:

  Key Model - Serial Number

YubiKey FIDO2 Web Sign-in

1. Open a web browser to the application using Entra ID as its IdP, e.g. https://portal.office.com
2. Click Sign-in options > Sign in with a security key
3. Follow the on-screen instructions to connect your key, enter its FIDO2 PIN, touch it and complete sign-in



Microsoft

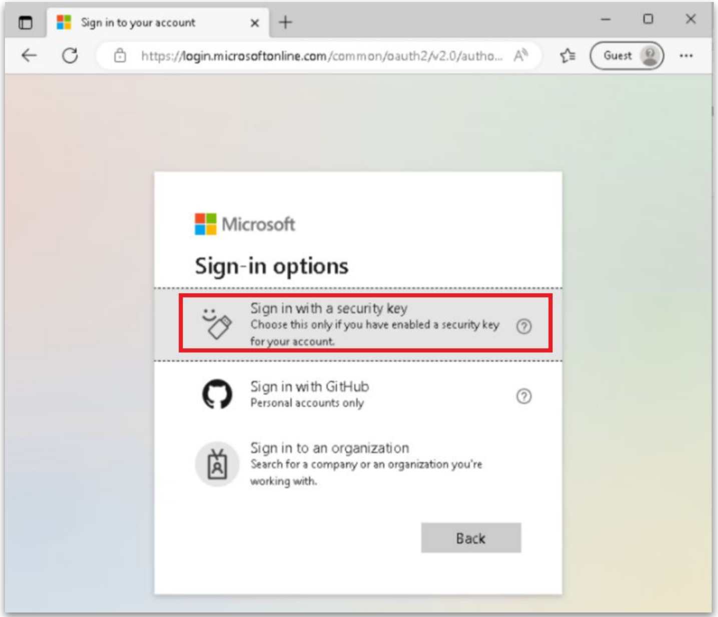
Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Sign-in options


Sign in to your account
https://login.microsoftonline.com/common/oauth2/v2.0/autho...
Guest

Microsoft

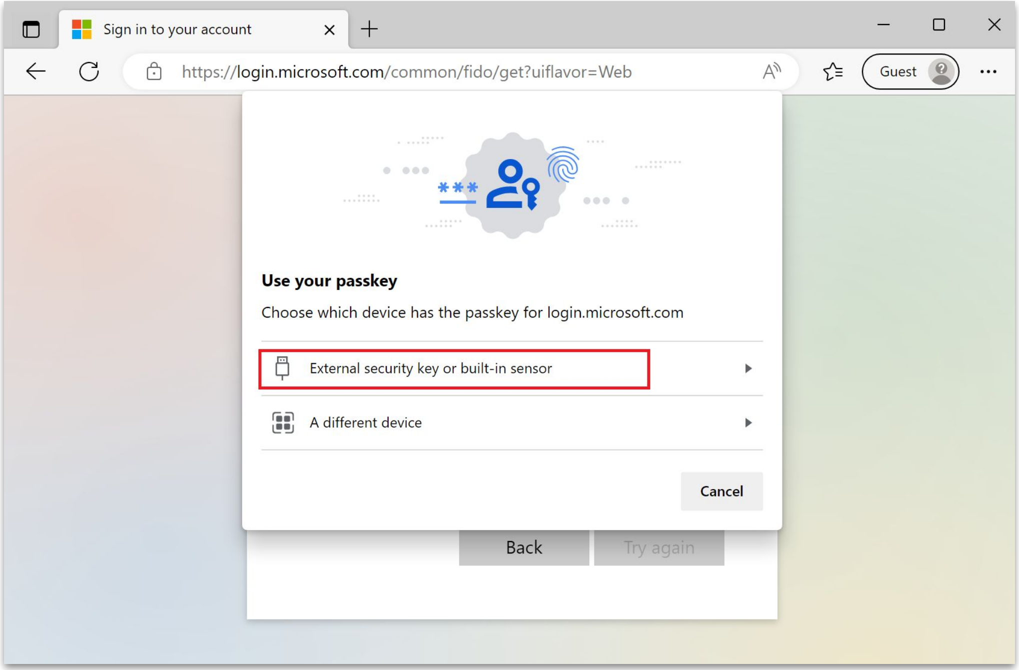
Sign-in options

Sign in with a security key
Choose this only if you have enabled a security key for your account.

Sign in with GitHub
Personal accounts only

Sign in to an organization
Search for a company or an organization you're working with.

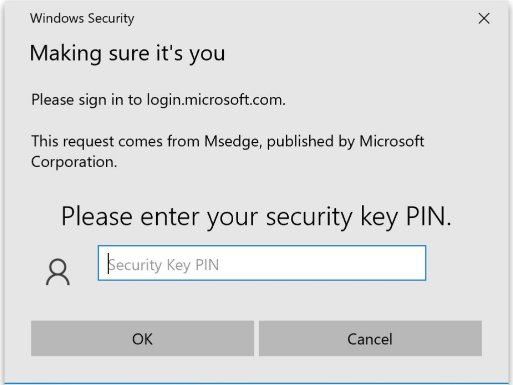
YubiKey FIDO2 Web Sign-in


Sign in to your account
https://login.microsoft.com/common/fido/get?uiflavor=Web
Guest

Use your passkey

Choose which device has the passkey for login.microsoft.com

External security key or built-in sensor
A different device
Cancel
Back
Try again

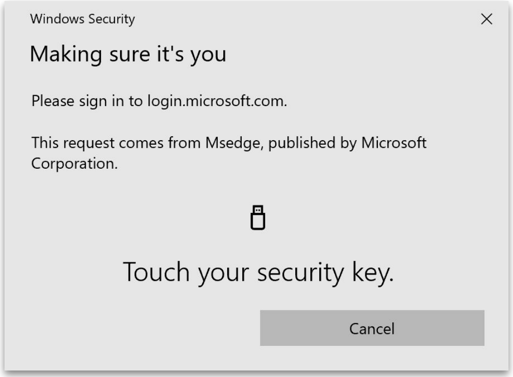


Making sure it's you

Please sign in to login.microsoft.com.

This request comes from Msedge, published by Microsoft Corporation.

Please enter your security key PIN.



Making sure it's you

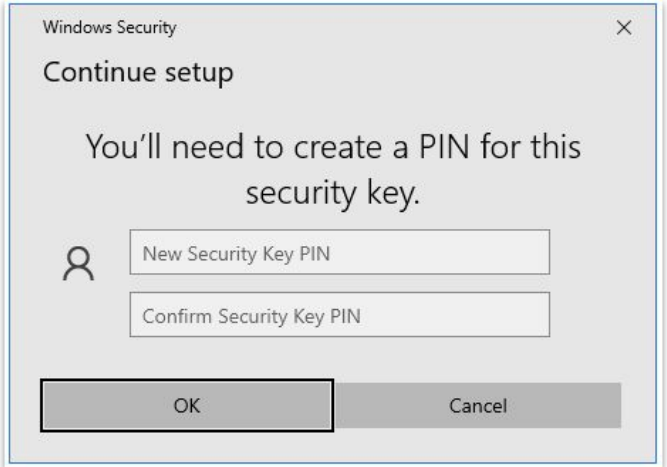
Please sign in to login.microsoft.com.

This request comes from Msedge, published by Microsoft Corporation.

Touch your security key.

FIDO2 PIN

- When registering a new YubiKey users will be prompted to set a PIN
- FIDO2 PINs can be up to **63** characters (letters, numbers, and special characters)
- Non-FIPS YubiKeys minimum length is **4**
- FIPS YubiKeys minimum length is **6**
- Although the FIDO2 PIN can include special characters, we recommend sticking to letters and numbers, as not all browsers/platforms will support special characters



Windows Security

Continue setup

You'll need to create a PIN for this security key.

New Security Key PIN

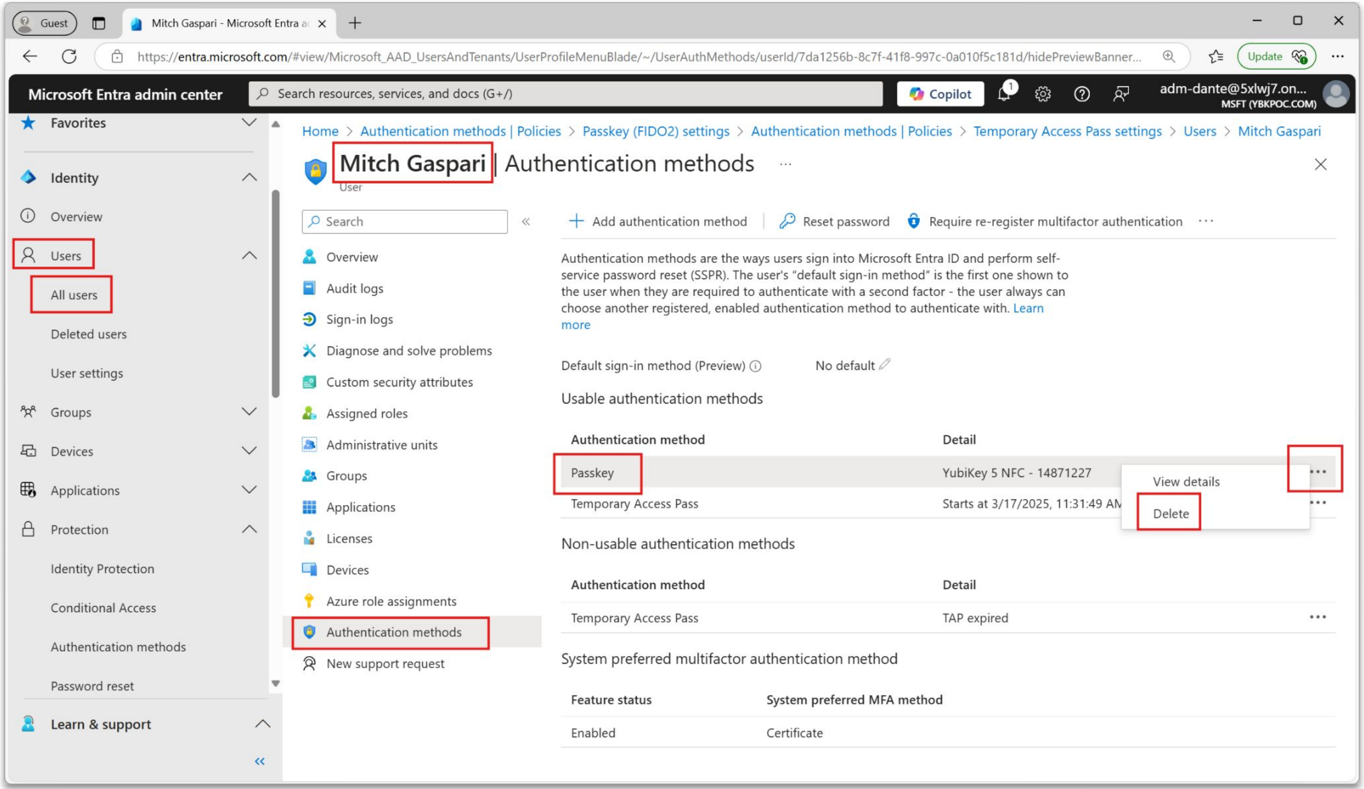
Confirm Security Key PIN

Remove a FIDO2 Security Key From a User

- **Scenarios:**
  - Lost key
  - Repurposed Key
- **Administrator:**
  - Via Entra ID Portal
  - Requires one of the following roles:
    - User Administrator
    - Global Administrator
- **End-User:**
  - Via the **MySecurityInfo** page:
    - https://myprofile.microsoft.com/, then click on **Update Info**
    - Or https://aka.ms/mysecurityinfo

Remove a FIDO2 Security Key From a User

Administrator:



Guest
Mitch Gaspari - Microsoft Entra a
https://entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/UserAuthMethods/userId/7da1256b-8c7f-41f8-997c-0a010f5c181d/hidePreviewBanner...
Update
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
adm-dante@5xlwj7.on...
MSFT (YBKPOC.COM)
Favorites
Identity
Overview
Users
All users
Deleted users
User settings
Groups
Devices
Applications
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Learn & support
Home > Authentication methods | Policies > Passkey (FIDO2) settings > Authentication methods | Policies > Temporary Access Pass settings > Users > Mitch Gaspari
Search
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
New support request
Add authentication method
Reset password
Require re-register multifactor authentication
View details
Delete

Mitch Gaspari | Authentication methods

User

Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. Learn more

Default sign-in method (Preview) No default

Usable authentication methods

Authentication method	Detail
Passkey	YubiKey 5 NFC - 14871227
Temporary Access Pass	Starts at 3/17/2025, 11:31:49 AM

Non-usable authentication methods

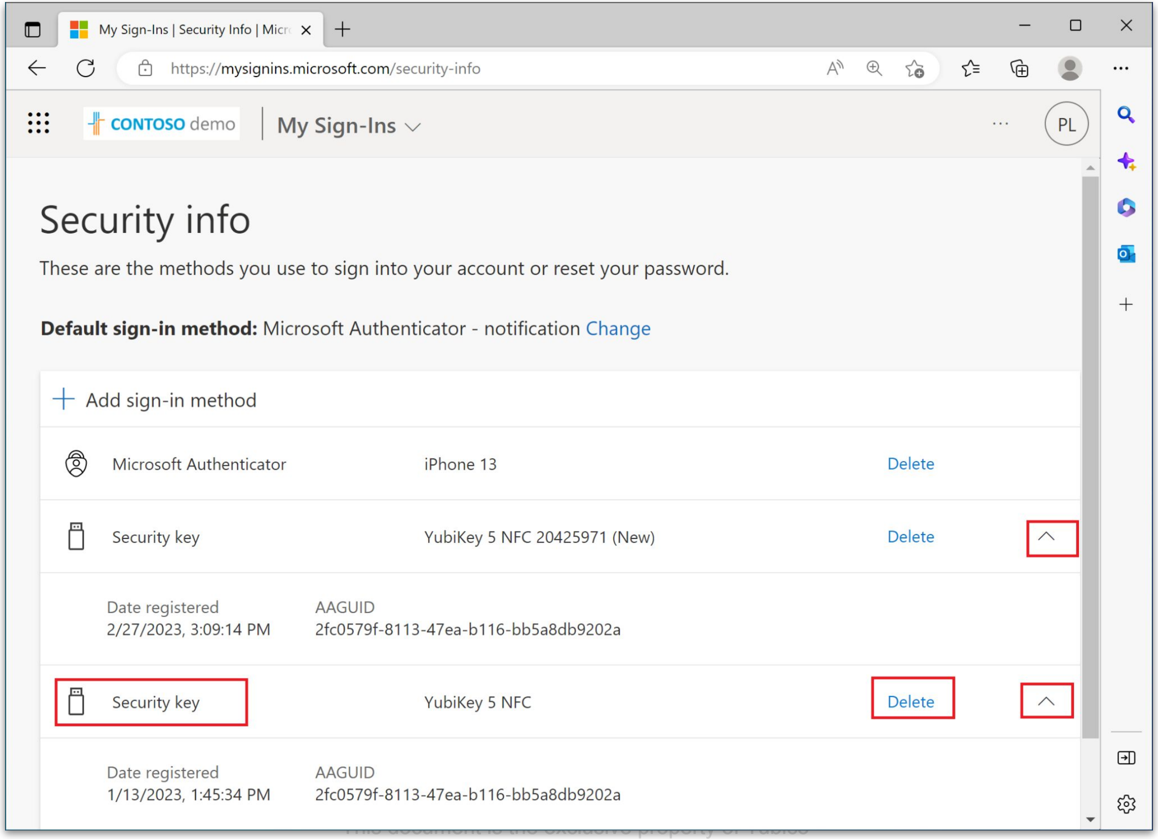
Authentication method	Detail
Temporary Access Pass	TAP expired

System preferred multifactor authentication method

Feature status	System preferred MFA method
Enabled	Certificate

Remove a FIDO2 Security Key From a User

End-user:


My Sign-Ins | Security Info | Micr
https://mysignins.microsoft.com/security-info
CONTOSO demo
My Sign-Ins
PL

Security info

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

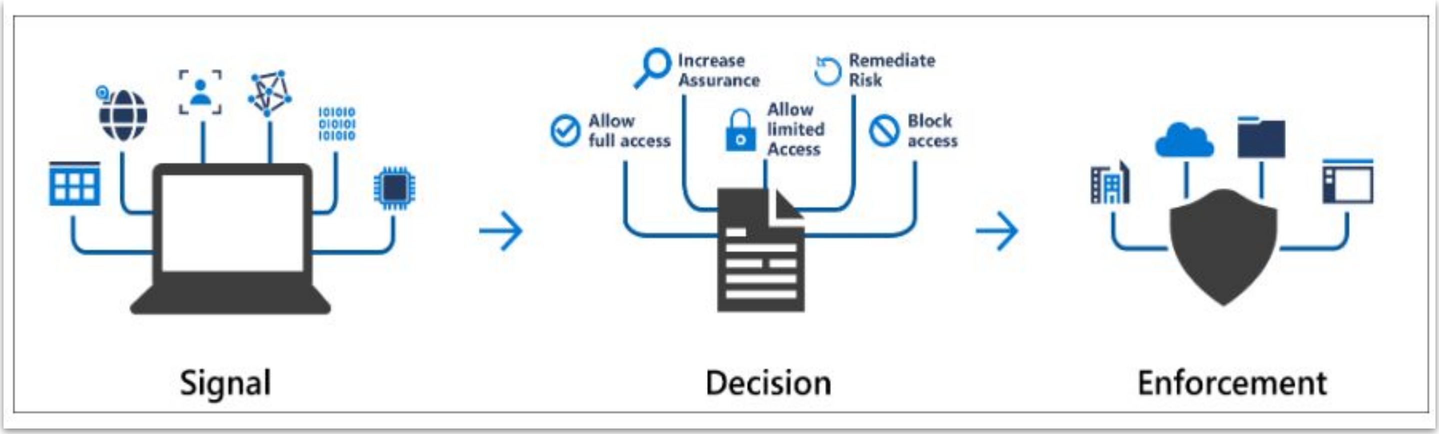
Default sign-in method: Microsoft Authenticator - notification Change

+ Add sign-in method

Microsoft Authenticator	iPhone 13	Delete
Security key	YubiKey 5 NFC 20425971 (New)	Delete
Date registered 2/27/2023, 3:09:14 PM	AAGUID 2fc0579f-8113-47ea-b116-bb5a8db9202a	
Security key	YubiKey 5 NFC	Delete
Date registered 1/13/2023, 1:45:34 PM	AAGUID 2fc0579f-8113-47ea-b116-bb5a8db9202a	

Conditional Access Policies

Conditional Access Policies apply the right access controls when needed by utilizing more than just a typical authentication flow. They bring signals together, to make decisions, and enforce organizational policies by considering other conditions at the time of access request.



Note: Conditional Access Policies require Entra ID Premium P1 license.

Conditional Access-- A Closer Look

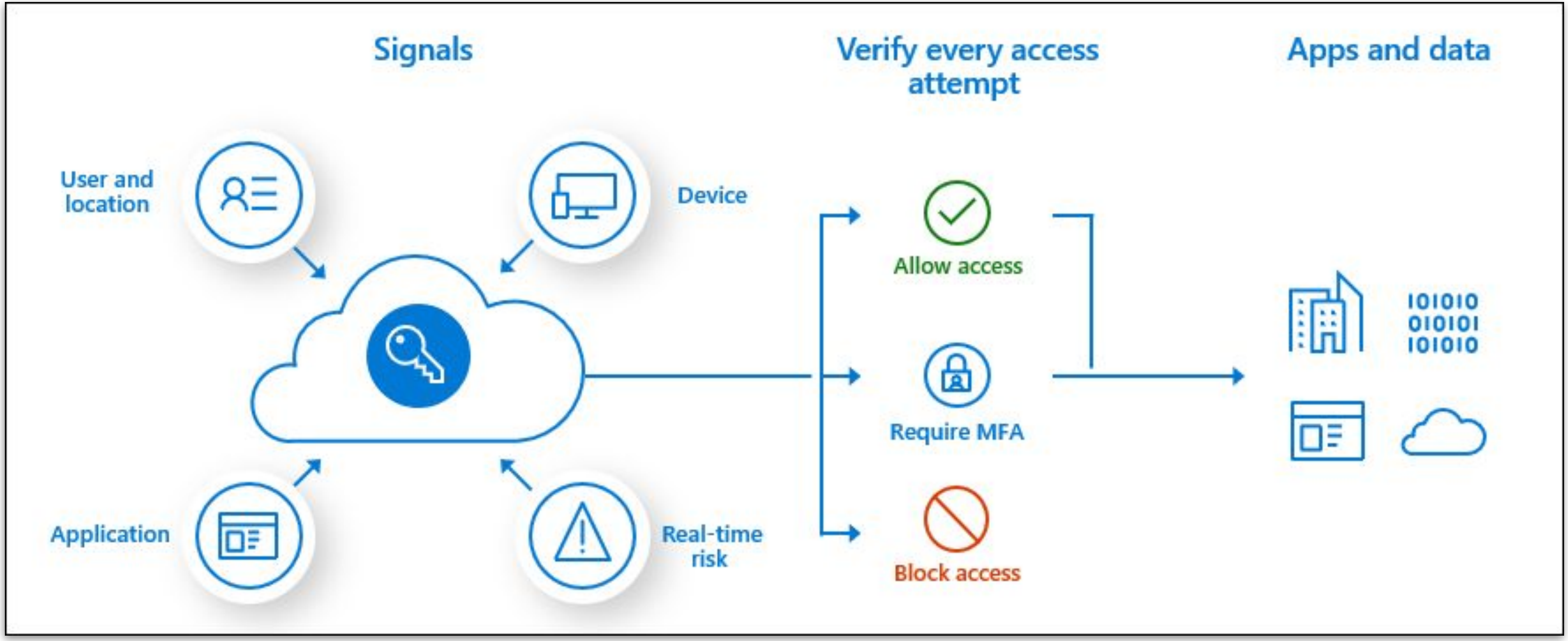
Conditions = Signals

- User or group membership
- IP Location information
- Device association and/or condition
- Application attempting to be accessed
- Real-time and calculated risk detection

Decisions

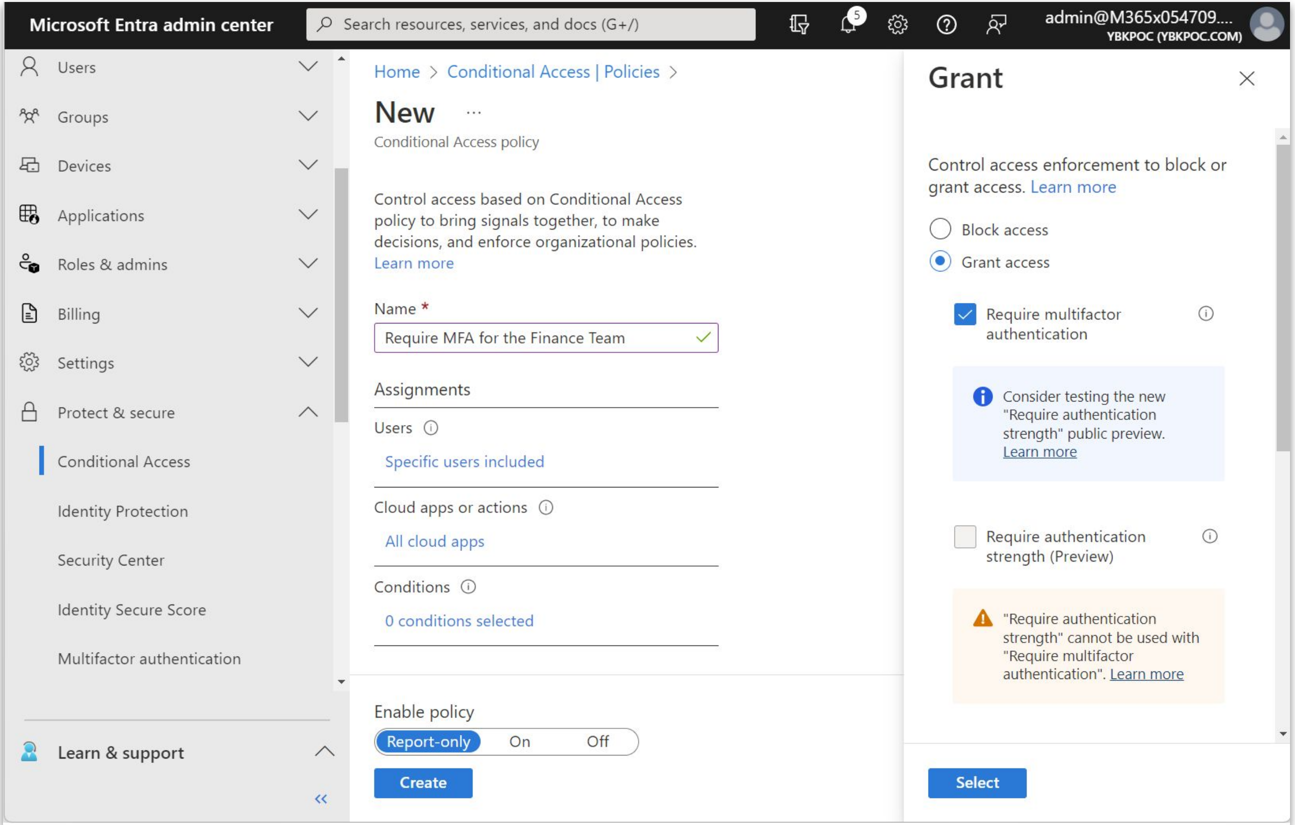
- **Block access**
  - Most restrictive decision
- **Grant access**
  - Least restrictive decision, can still require one or more of the following options:
    - Multi-factor authentication
    - Device to be marked as compliant
    - Hybrid Entra ID joined device
    - Approved client app
    - App protection policy (preview)

Conditional Access Illustrated



Multiple Conditional Access (CA) policies may apply to an individual user at any time. In this case, all policies that apply must be satisfied.

Creating a CA Policy



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 *
Require MFA for the Finance Team ✓

Assignments

Users ⓘ
Specific users included

Cloud apps or actions ⓘ
All cloud apps

Conditions ⓘ
0 conditions selected

Enable policy
[✓ Report-only] On Off

Create

Grant

Control access enforcement to block or grant access. Learn more

○ Block access
● Grant access

☑ Require multifactor authentication ⓘ

Consider testing the new "Require authentication strength" public preview. Learn more

□ Require authentication strength (Preview) ⓘ

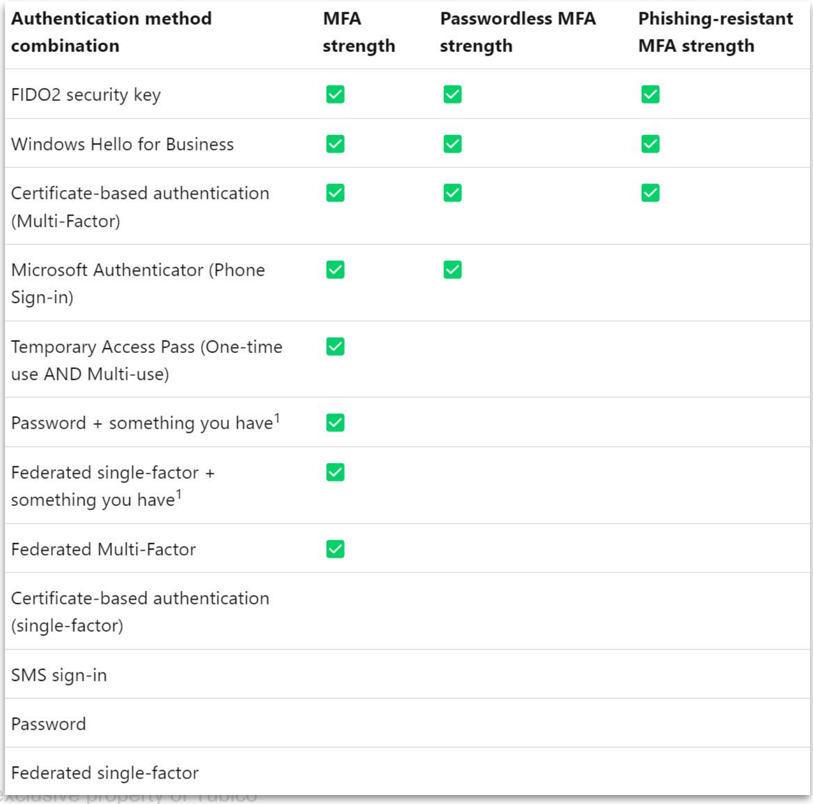
⚠ "Require authentication strength" cannot be used with "Require multifactor authentication". Learn more

Select

Authentication Strength Policies

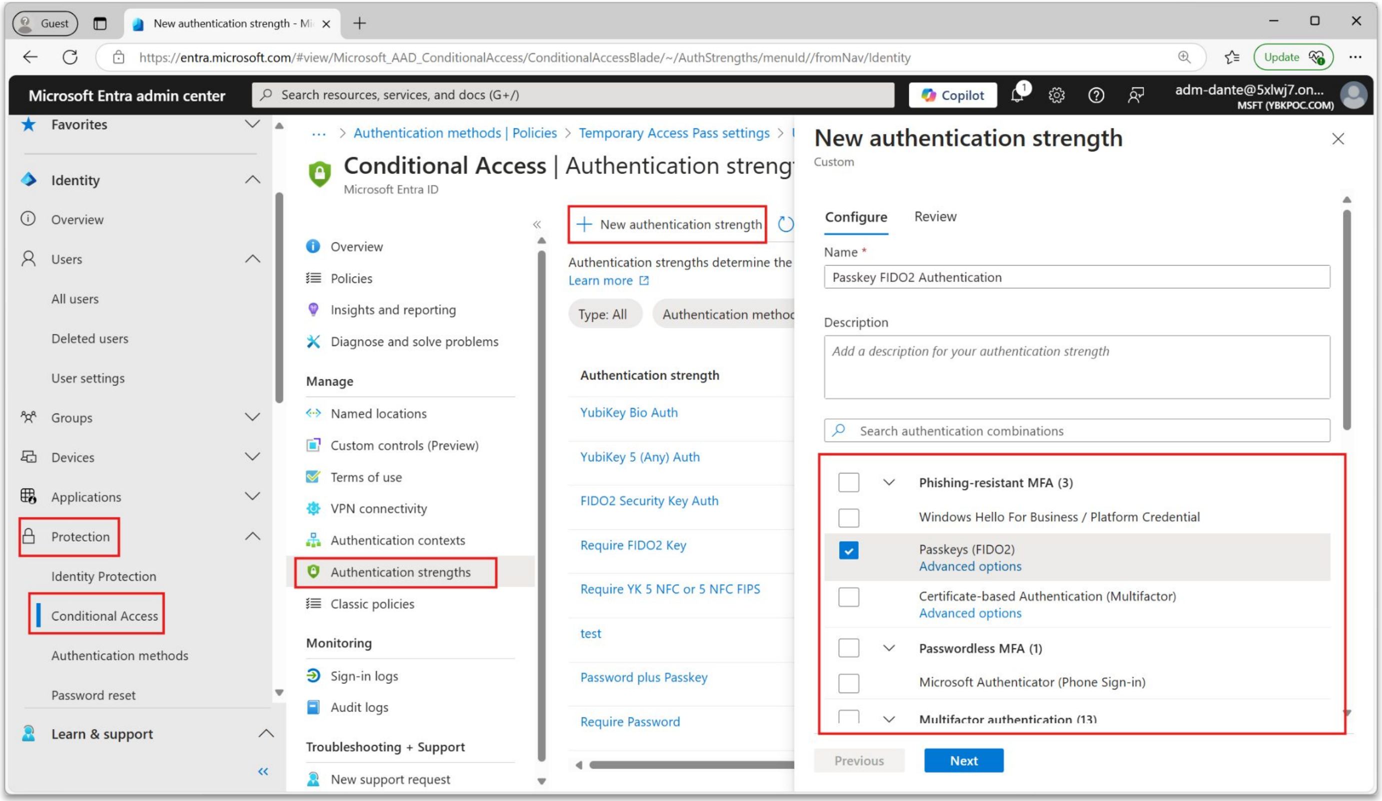
Authentication Strength is a Conditional Access control that allows administrators to specify which combination of authentication methods can be used to access a resource

- Built-in Authentication Strengths
    - Multi-Factor authentication strength
    - Passwordless MFA strength
    - Phishing-resistant MFA strength
- Custom Authentication Strengths can be created to meet specific requirements
- Assess to more sensitive assets/applications can be granted with higher authentication strengths



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

Creating an Auth Strength Policy



New authentication strength

Custom

Configure | Review

Name *

Passkey FIDO2 Authentication

Description

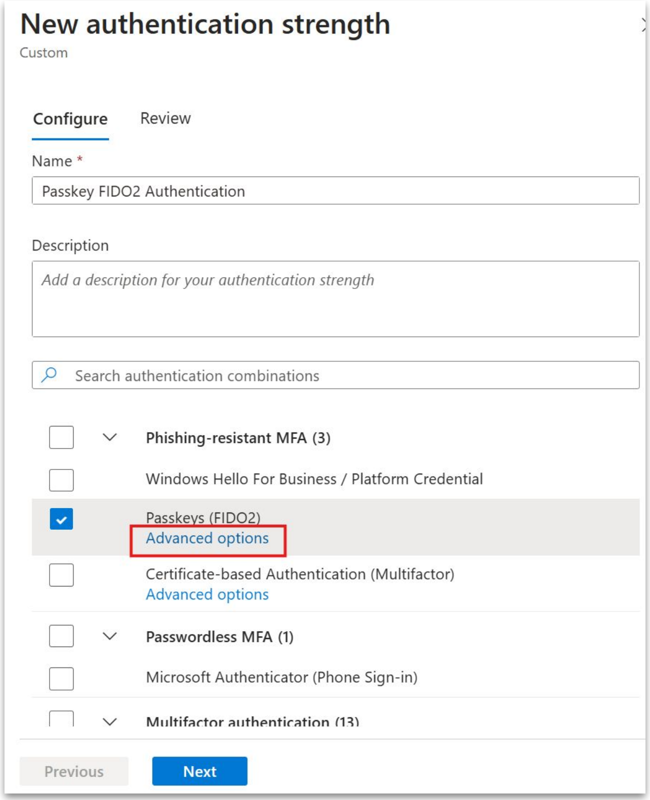
Add a description for your authentication strength

Search authentication combinations

- □ Phishing-resistant MFA (3)
  - □ Windows Hello For Business / Platform Credential
  - ☑ Passkeys (FIDO2) — Advanced options
  - □ Certificate-based Authentication (Multifactor) — Advanced options
- □ Passwordless MFA (1)
  - □ Microsoft Authenticator (Phone Sign-in)
- □ Multifactor authentication (13)

Previous | Next

Auth Strength - Advanced Options



New authentication strength

Custom

Configure | Review

Name *

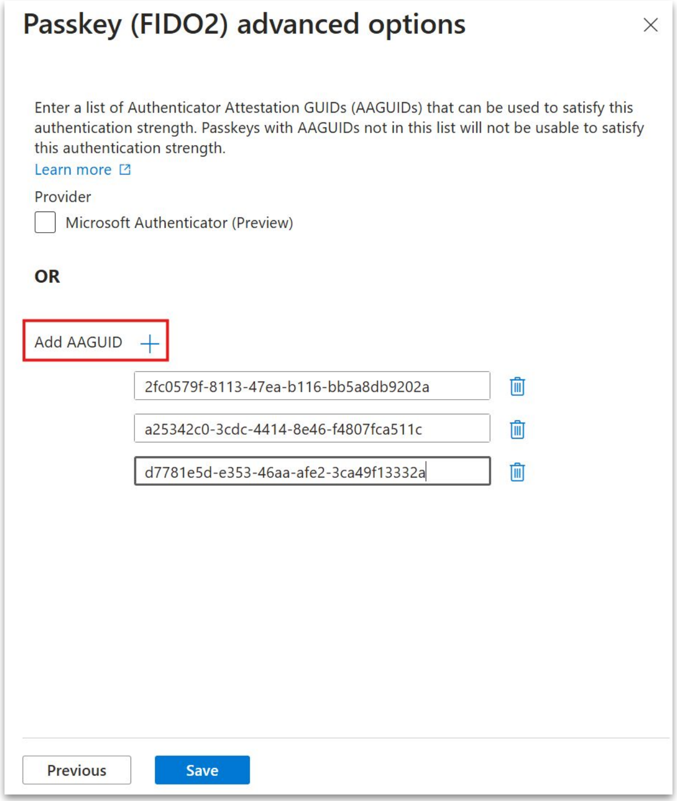
Passkey FIDO2 Authentication

Description

Add a description for your authentication strength

Search authentication combinations

- □ Phishing-resistant MFA (3)
- □ Windows Hello For Business / Platform Credential
- ☑ Passkeys (FIDO2)
  Advanced options
- □ Certificate-based Authentication (Multifactor)
  Advanced options
- □ Passwordless MFA (1)
- □ Microsoft Authenticator (Phone Sign-in)
- □ Multifactor authentication (13)



Passkey (FIDO2) advanced options

Enter a list of Authenticator Attestation GUIDs (AAGUIDs) that can be used to satisfy this authentication strength. Passkeys with AAGUIDs not in this list will not be usable to satisfy this authentication strength.

Learn more

Provider

□ Microsoft Authenticator (Preview)

OR

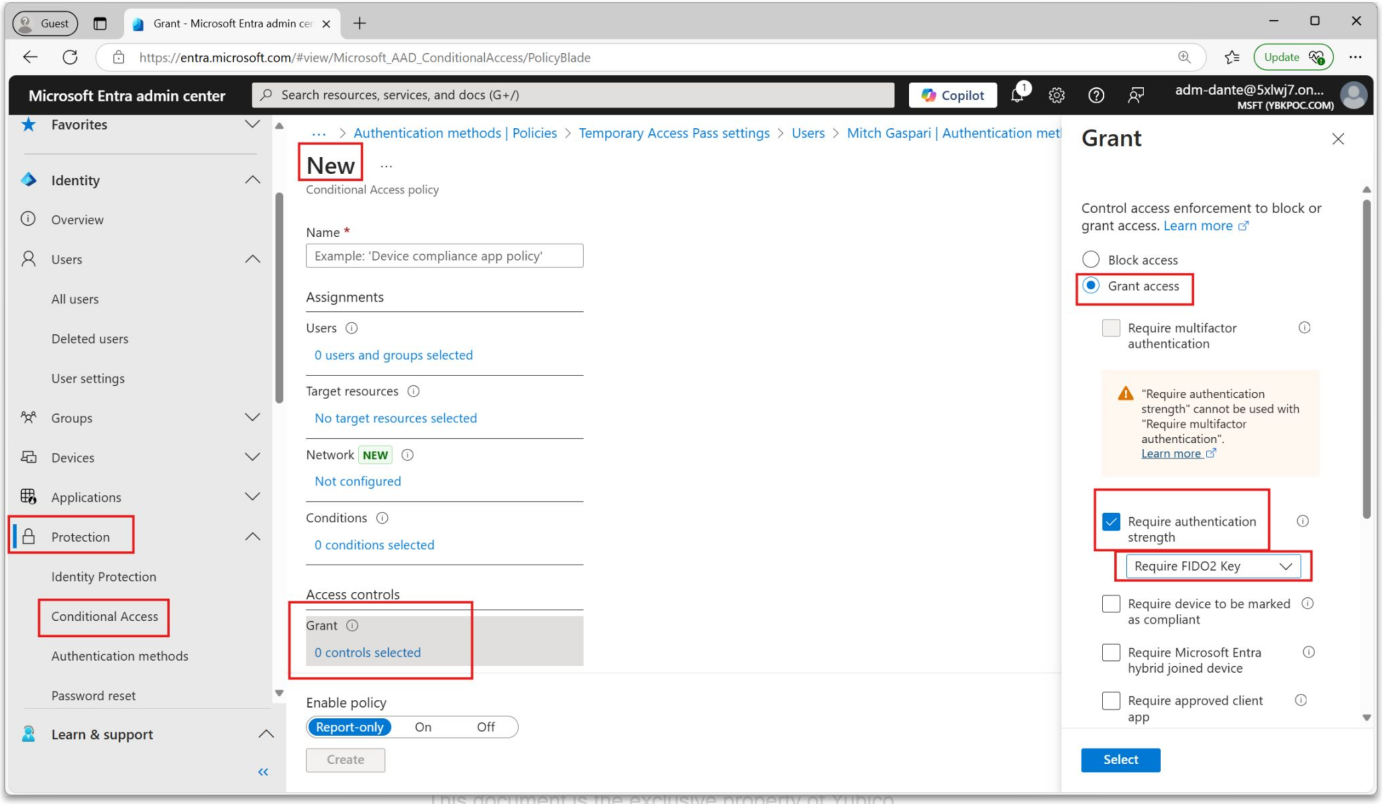
Add AAGUID +

2fc0579f-8113-47ea-b116-bb5a8db9202a

a25342c0-3cdc-4414-8e46-f4807fca511c

d7781e5d-e353-46aa-afe2-3ca49f13332a

Configuring a CA Policy to Use Auth Strength


Guest
Grant - Microsoft Entra admin cer
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade
Update
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
adm-dante@5xlwj7.on...
MSFT (YBKPOC.COM)
Favorites
Identity
Overview
Users
All users
Deleted users
User settings
Groups
Devices
Applications
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Learn & support
... > Authentication methods | Policies > Temporary Access Pass settings > Users > Mitch Gaspari | Authentication met

New ...

Conditional Access policy

Name *

Example: 'Device compliance app policy'

Assignments

Users

0 users and groups selected

Target resources

No target resources selected

Network NEW

Not configured

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Enable policy

[✓ Report-only] On Off

Create

Grant

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

□ Require multifactor authentication

"Require authentication strength" cannot be used with "Require multifactor authentication". Learn more

☑ Require authentication strength

Require FIDO2 Key

□ Require device to be marked as compliant

□ Require Microsoft Entra hybrid joined device

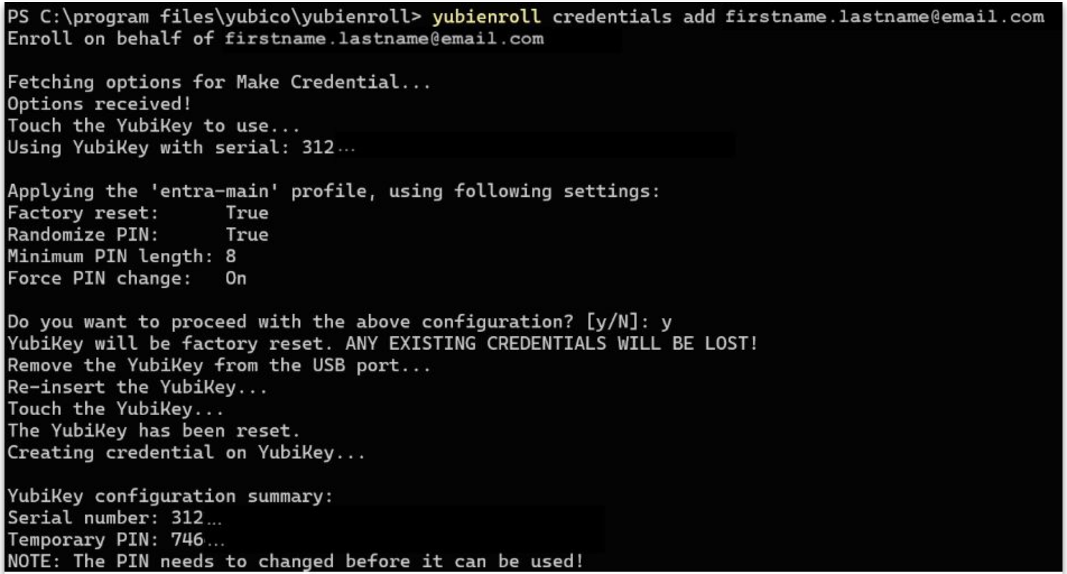
□ Require approved client app

Select

YubiEnroll Tool

YubiEnroll Tool

- FIDO2 Enrollment on Behalf of a user with Entra ID
- Currently a Command Line Tool
- Removes the need for self-enrollment



```
PS C:\program files\yubico\yubienroll> yubienroll credentials add firstname.lastname@email.com
Enroll on behalf of firstname.lastname@email.com

Fetching options for Make Credential...
Options received!
Touch the YubiKey to use...
Using YubiKey with serial: 312...

Applying the 'entra-main' profile, using following settings:
Factory reset:      True
Randomize PIN:      True
Minimum PIN length: 8
Force PIN change:   On

Do you want to proceed with the above configuration? [y/N]: y
YubiKey will be factory reset. ANY EXISTING CREDENTIALS WILL BE LOST!
Remove the YubiKey from the USB port...
Re-insert the YubiKey...
Touch the YubiKey...
The YubiKey has been reset.
Creating credential on YubiKey...

YubiKey configuration summary:
Serial number: 312...
Temporary PIN: 746...
NOTE: The PIN needs to changed before it can be used!
```

Extending FIDO2 Authentication to Windows Logon

Prerequisites - Windows Logon

Native Entra ID joined (non-hybrid):

- YubiKeys with FIDO2 support:
  - YubiKey 5 Series
  - YubiKey 5 FIPS Series
  - YubiKey Bio Series
  - Security Key Series
- Windows 10 1909 or higher, or Windows 11
- Combined security information registration:
  - Enable combined security information registration in Azure Active Directory
- To enable FIDO2 authentication for Windows logon:
  - Intune, or
  - Provisioning package

Source: Enable passwordless security key sign-in to Windows 10 devices with Azure Active Directory

Prerequisites - Windows Logon

Entra ID Hybrid joined - All prereqs of Entra ID joined, plus:

- Windows 10 2004 or higher or Windows 11 with the latest updates installed
- Domain controllers must have these patches installed:
  - Windows Server 2016: January 23, 2020—KB4534307 (OS Build 14393.3474)
  - Windows Server 2019: January 23, 2020—KB4534321 (OS Build 17763.1012)
- AES256_HMAC_SHA1 must be enabled when Network security: Configure encryption types allowed for Kerberos policy is configured on domain controllers:
  - Network security: Configure encryption types allowed for Kerberos
- Credentials required for setup:
  - User member of the Domain Admins or Enterprise Admins groups.
  - Entra ID user member of the Global Administrators role.
- Entra Connect 1.4.32.0 or later
- To enable FIDO2 authentication for Windows logon:
  - GPO, Intune, or Provisioning package
- Members of on-prem AD privileged groups can't use FIDO2 authentication by default.

Source: Enable passwordless security key sign-in to Windows 10 devices with Azure Active Directory

Unsupported Scenarios - Windows Logon

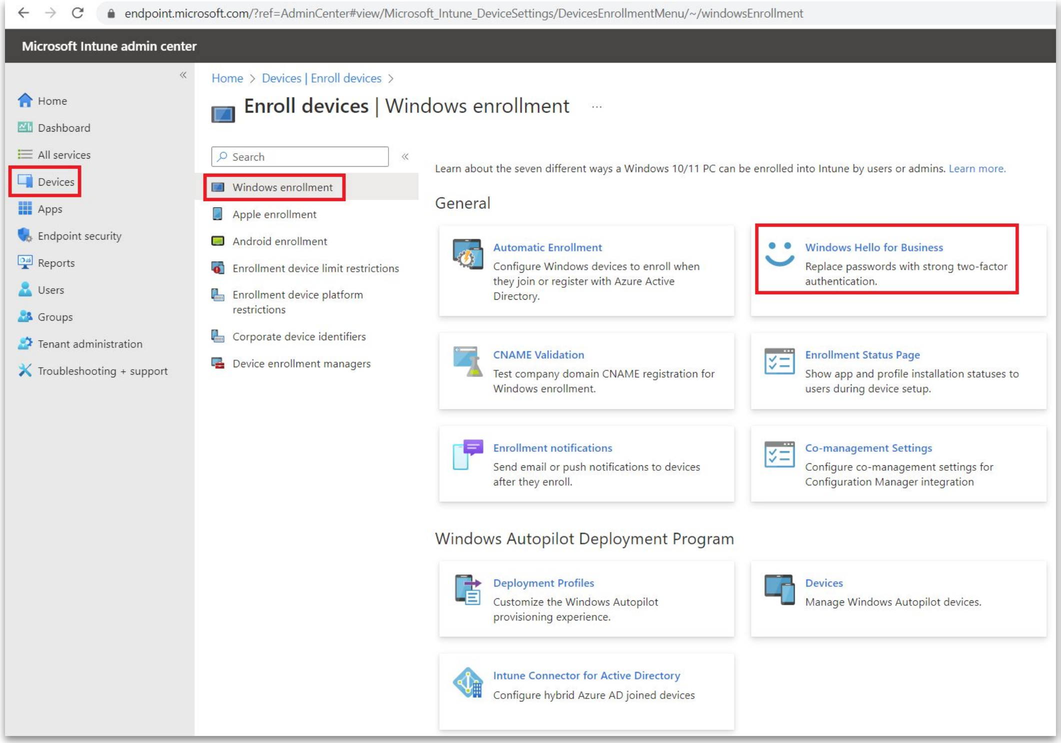
- On-premises AD domain-joined only devices
- Windows Server logon
- Signing in or unlocking a Windows 10/11 device with a security key containing multiple Entra ID accounts. This scenario utilizes the last [AAD] account added to the security key. WebAuthN (in-browser logon) allows users to choose the account they wish to use
- VDI scenarios using a security key may not work for certain systems*
- S/MIME using a security key
- "Run as" using a security key
- If you haven't used your security key to sign in to your device while online, you can't use it to sign in or unlock offline

***Note:** For details on VDI solutions, check support with the vendor.

Enabling Security Key Sign-in on Windows

- Methods for both Hybrid and Entra ID-only joined devices
  - Endpoint Manager (Microsoft Intune)
  - Provisioning package
- Method only for Hybrid AAD joined devices
  - Group Policy

Endpoint Manager (Microsoft Intune)



endpoint.microsoft.com/?ref=AdminCenter#view/Microsoft_Intune_DeviceSettings/DevicesEnrollmentMenu/~/windowsEnrollment

Microsoft Intune admin center

Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Home > Devices | Enroll devices >

Enroll devices | Windows enrollment

Search
Windows enrollment
Apple enrollment
Android enrollment
Enrollment device limit restrictions
Enrollment device platform restrictions
Corporate device identifiers
Device enrollment managers

Learn about the seven different ways a Windows 10/11 PC can be enrolled into Intune by users or admins. Learn more.

General

Automatic Enrollment – Configure Windows devices to enroll when they join or register with Azure Active Directory.

Windows Hello for Business – Replace passwords with strong two-factor authentication.

CNAME Validation – Test company domain CNAME registration for Windows enrollment.

Enrollment Status Page – Show app and profile installation statuses to users during device setup.

Enrollment notifications – Send email or push notifications to devices after they enroll.

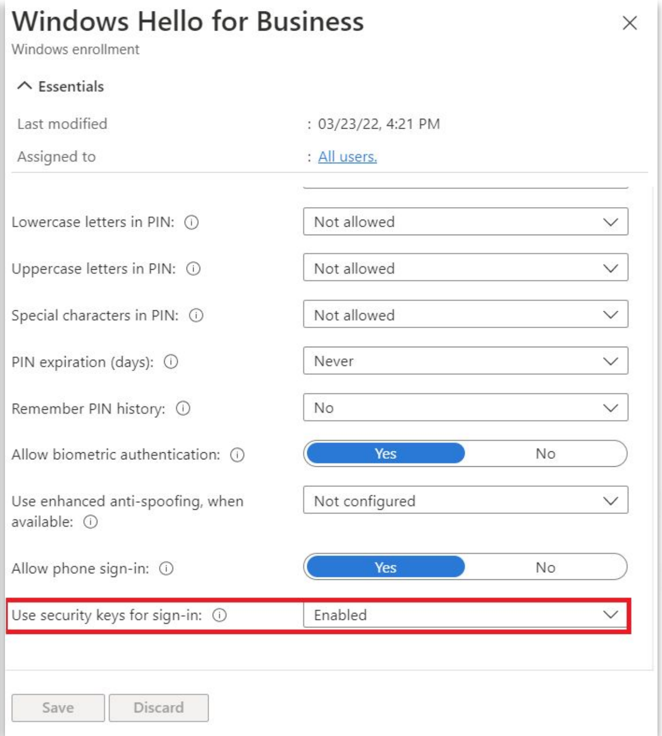
Co-management Settings – Configure co-management settings for Configuration Manager integration

Windows Autopilot Deployment Program

Deployment Profiles – Customize the Windows Autopilot provisioning experience.

Devices – Manage Windows Autopilot devices.

Intune Connector for Active Directory – Configure hybrid Azure AD joined devices



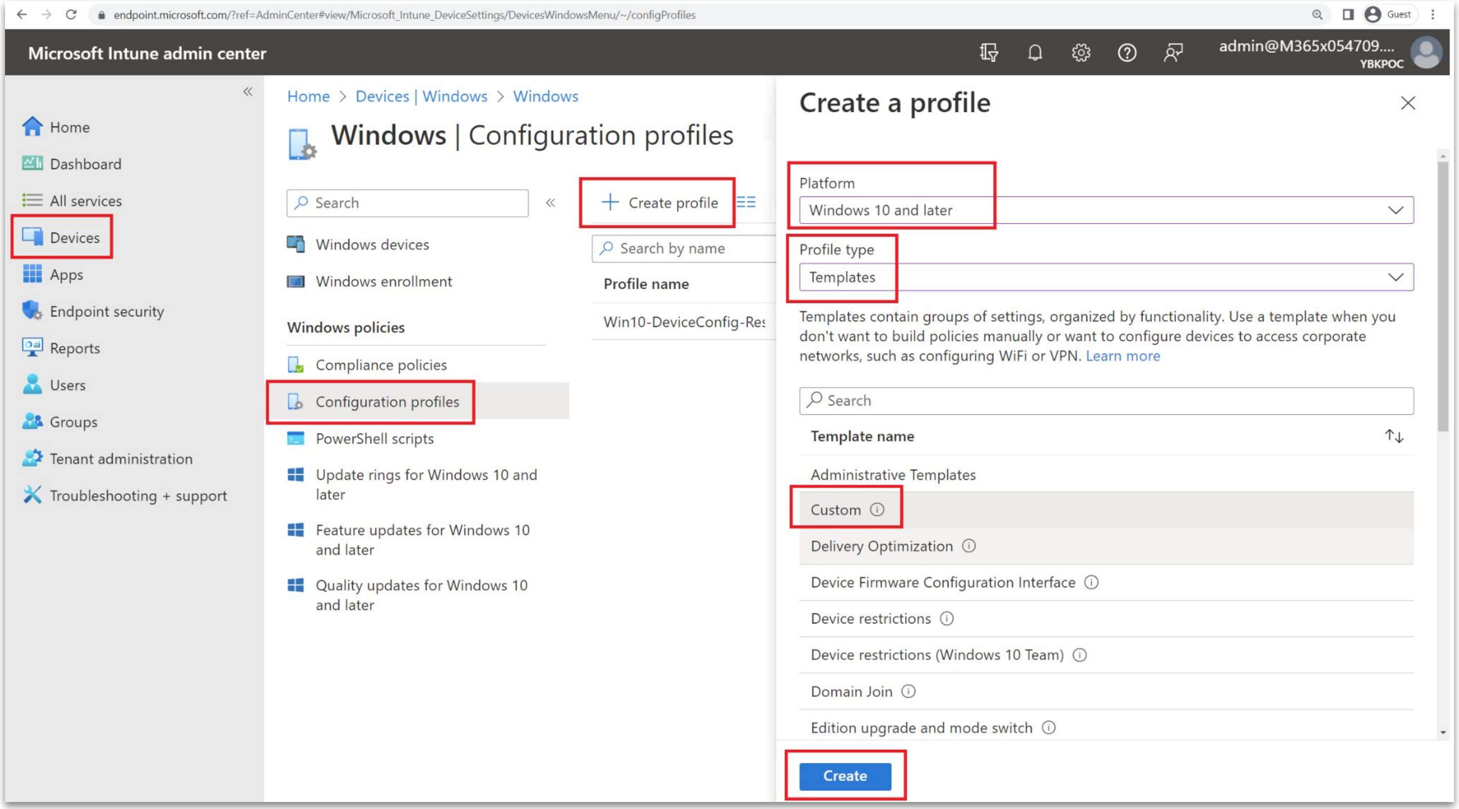
Windows Hello for Business

Windows enrollment

Essentials

Last modified	: 03/23/22, 4:21 PM
Assigned to	: All users.
Lowercase letters in PIN:	Not allowed
Uppercase letters in PIN:	Not allowed
Special characters in PIN:	Not allowed
PIN expiration (days):	Never
Remember PIN history:	No
Allow biometric authentication:	[✓ Yes] No
Use enhanced anti-spoofing, when available:	Not configured
Allow phone sign-in:	[✓ Yes] No
Use security keys for sign-in:	Enabled

Endpoint Manager (Microsoft Intune)



endpoint.microsoft.com/?ref=AdminCenter#view/Microsoft_Intune_DeviceSettings/DevicesWindowsMenu/~/configProfiles

Microsoft Intune admin center

admin@M365x054709....
YBKPOC

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Devices | Windows > Windows

Windows | Configuration profiles

Search

- Windows devices
- Windows enrollment

Windows policies

- Compliance policies
- Configuration profiles
- PowerShell scripts
- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later
- Quality updates for Windows 10 and later

+ Create profile

Search by name

Profile name
Win10-DeviceConfig-Res

Create a profile

Platform: Windows 10 and later

Profile type: Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

Search

Template name
Administrative Templates
Custom ⓘ
Delivery Optimization ⓘ
Device Firmware Configuration Interface ⓘ
Device restrictions ⓘ
Device restrictions (Windows 10 Team) ⓘ
Domain Join ⓘ
Edition upgrade and mode switch ⓘ

Create

Endpoint Manager (Microsoft Intune)

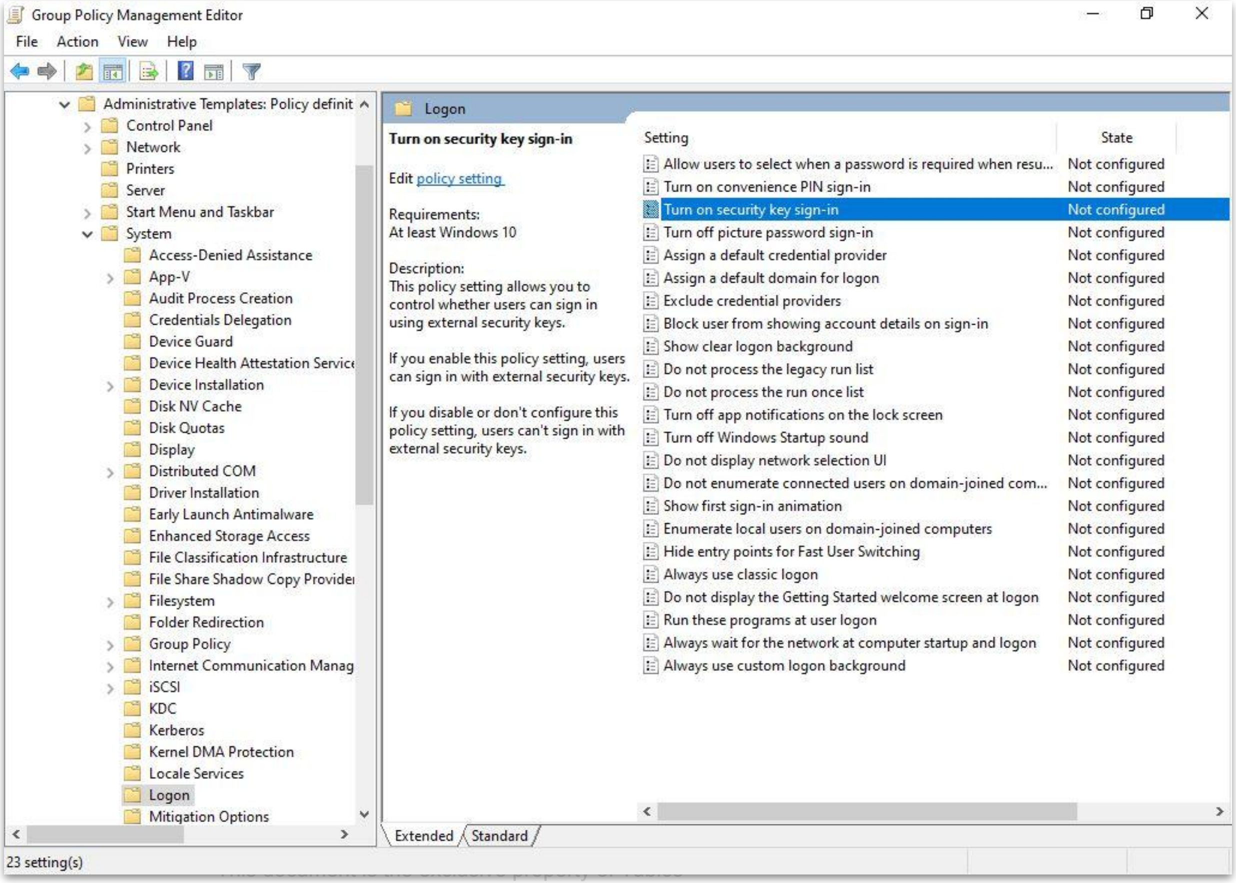
1. **Configure the new profile with the following settings:**
   - Platform: **Windows 10 and later**
   - Profile type: **Templates** > **Custom**
   - Name: **Security Keys for Windows Sign-In**
   - Description: **Enables FIDO Security Keys to be used during Windows Sign In**
2. **Click Next > Add and in Add Row, add the following Custom OMA-URI Settings:**
   - Name: **Turn on FIDO Security Keys for Windows Sign-In**
   - OMA-URI: **./Device/Vendor/MSFT/PassportForWork/SecurityKey/UseSecurityKeyForSignin**
   - Data Type: **Integer**
   - Value: **1**
3. **The remainder of the policy settings include assigning to specific users, devices, or groups:**
   - Go to **Devices** > **Windows** > **Configuration profiles** > Name of profile.
   - Click **Edit** next to **Assignments**, click **Add groups** under Included groups, use the pop-out UI to locate and select the desired group, then click **Review + save**.

Provisioning Package

- Lets you quickly and efficiently configure a device without having to install a new image.
- Can be applied:
  - During initial setup (from a USB drive)
  - After initial setup through Windows settings or by simply double-clicking a provisioning package
- .PPKG files created by the Windows Configuration Designer, which is available as an app in the Microsoft Store
- It's best suited for small- to medium-sized businesses with deployments that range from tens to a few hundred computers
- **Instructions:**
  - Provisioning packages for Windows
  - Enable FIDO2 security key logon with a provisioning package
  - Apply a provisioning package

Group Policy Object (GPO) - Hybrid Only

Computer Configuration > Administrative Templates > System > Logon > Turn on security key sign-in



Turn on security key sign-in

Edit policy setting

Requirements:
At least Windows 10

Description:
This policy setting allows you to control whether users can sign in using external security keys.

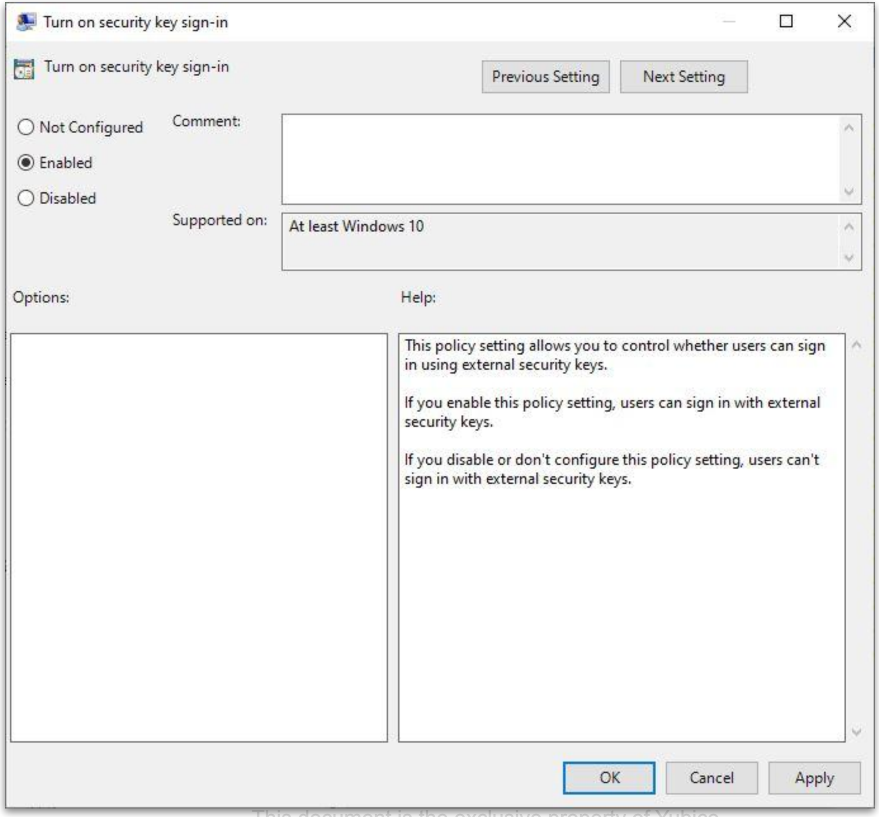
If you enable this policy setting, users can sign in with external security keys.

If you disable or don't configure this policy setting, users can't sign in with external security keys.

Setting	State
Allow users to select when a password is required when resu...	Not configured
Turn on convenience PIN sign-in	Not configured
Turn on security key sign-in	Not configured
Turn off picture password sign-in	Not configured
Assign a default credential provider	Not configured
Assign a default domain for logon	Not configured
Exclude credential providers	Not configured
Block user from showing account details on sign-in	Not configured
Show clear logon background	Not configured
Do not process the legacy run list	Not configured
Do not process the run once list	Not configured
Turn off app notifications on the lock screen	Not configured
Turn off Windows Startup sound	Not configured
Do not display network selection UI	Not configured
Do not enumerate connected users on domain-joined com...	Not configured
Show first sign-in animation	Not configured
Enumerate local users on domain-joined computers	Not configured
Hide entry points for Fast User Switching	Not configured
Always use classic logon	Not configured
Do not display the Getting Started welcome screen at logon	Not configured
Run these programs at user logon	Not configured
Always wait for the network at computer startup and logon	Not configured
Always use custom logon background	Not configured

Group Policy Object (GPO) - Hybrid Only

Select "Enabled" Radio Button



Turn on security key sign-in

○ Not Configured

● Enabled

○ Disabled

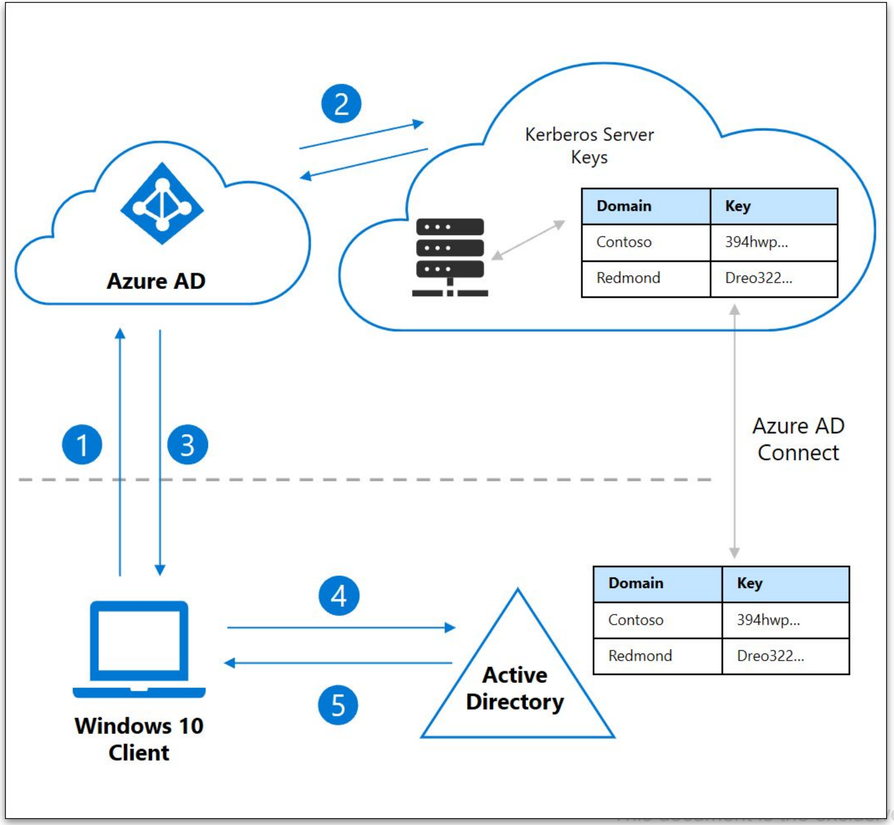
Supported on: At least Windows 10

This policy setting allows you to control whether users can sign in using external security keys.

If you enable this policy setting, users can sign in with external security keys.

If you disable or don't configure this policy setting, users can't sign in with external security keys.

Enable SSO to On-prem Resources - Hybrid Only



Domain	Key
Contoso	394hwp...
Redmond	Dreo322...

Domain	Key
Contoso	394hwp...
Redmond	Dreo322...

1. A user signs in to a Windows 10 device with an FIDO2 security key and authenticates to Entra ID.
2. Entra ID checks the directory for a Kerberos Server key that matches the user's on-premises AD domain.

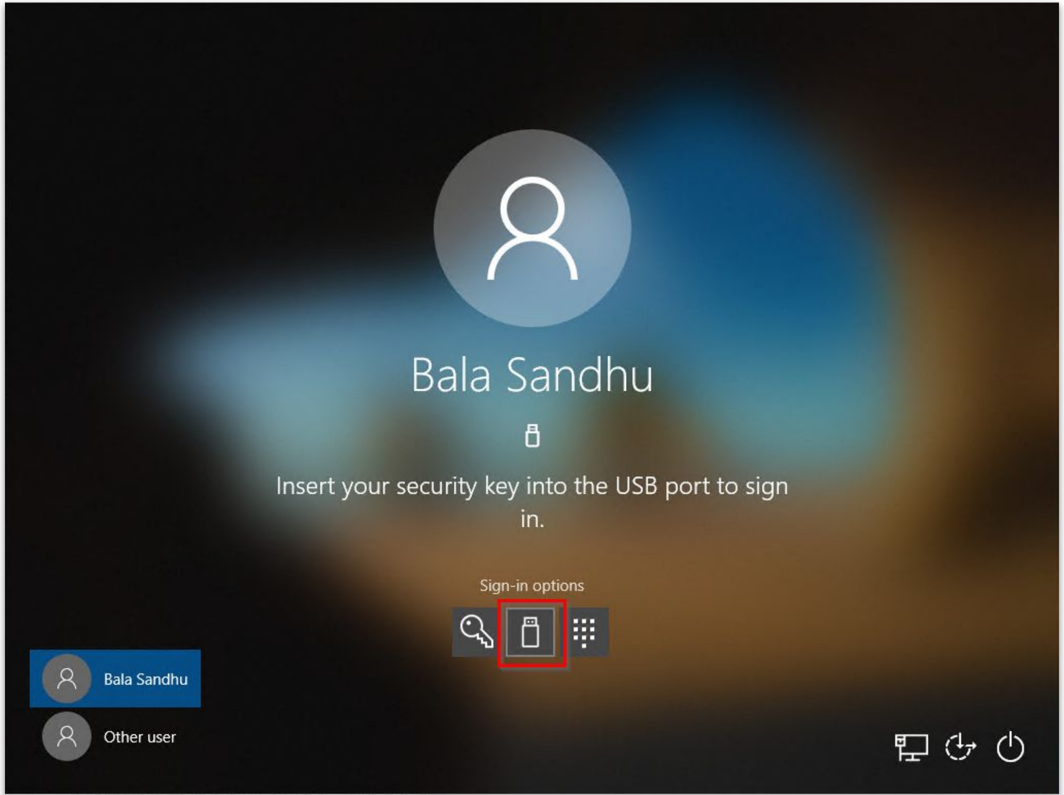
   Entra ID generates a partial Kerberos TGT for the user's on-premises AD domain. The TGT includes the user's SID only, and no authorization data.
3. The partial TGT is returned to the client along with the user's Entra ID Primary Refresh Token (PRT).
4. The client machine contacts an on-premises Domain Controller and trades the partial TGT for a fully formed TGT.
5. The client machine now has an Entra ID PRT and a full AD TGT and can access both cloud and on-premises resources.

Enable SSO to On-prem Resources - Hybrid Only

- **Instructions:**
    - Install the Entra ID Kerberos PowerShell module
    - Create a Kerberos Server object
    - View and verify the Entra ID Kerberos Server
- **Operational best practice:**
    - Rotate the Entra ID Kerberos Server key

Note: For multiple Active Directory domains or forests, one Kerberos Server object is required for each domain in each forest.

YubiKey FIDO2 Windows Authentication



Bala Sandhu

Insert your security key into the USB port to sign in.

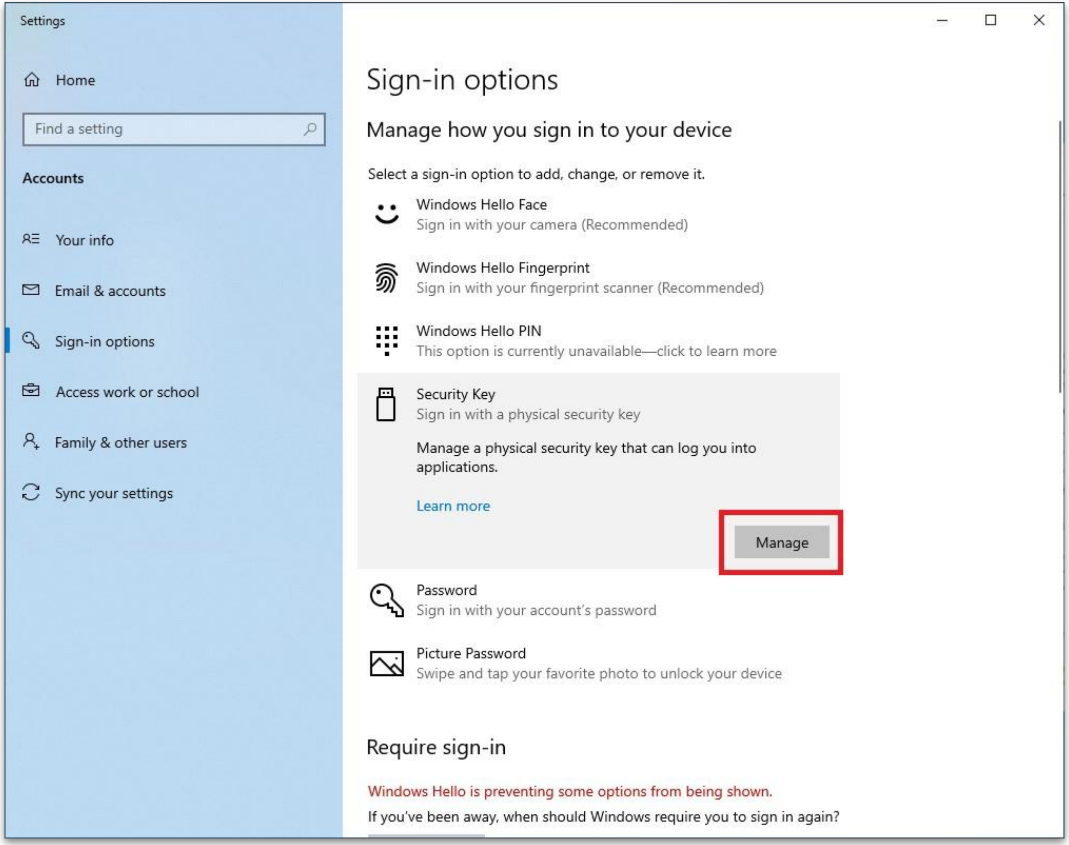
More on FIDO2 PINs

- FIDO2 PINs can be changed
  - In Windows under **Settings > Accounts > Sign-in options > Security Key > Manage > Change**
  - In non-Windows OSes in Google Chrome via **chrome://settings/securityKeys**
  - On any OS using the Yubico Authenticator by navigating to **Passkeys** > **Request access** (to elevate privilege) > **Change PIN**
  - If a user enters their FIDO2 PIN incorrectly 8 times consecutively, the function will lock and need to be reset
  - Every 3 incorrect attempts, the YubiKey will need to be power cycled (reinserted) in order to continue making attempts

Resetting the FIDO2 Function

- The FIDO2 function can be reset
  - In Windows under **Settings > Accounts > Sign-in options > Security Key > Manage > Reset**
  - In non-Windows OSes in Google Chrome via **chrome://settings/securityKeys**
  - On any OS using **Yubico Authenticator** by navigating to **Home > Factory reset > FIDO2 > Request access** (to elevate privilege) **> Reset**
- Precautions
  - Resetting FIDO2 will invalidate all registrations done with services via both FIDO U2F or FIDO2
  - The FIDO2 authentication method (registration) must be manually removed from the user in Entra ID
  - Prior to performing a reset, it is recommended to follow the instructions from our article **Understanding YubiKey PINs** under *Prior to performing a FIDO2 reset*

Managing FIDO2 - Windows Settings



Settings

Home

Find a setting

Accounts

Your info

Email & accounts

Sign-in options

Access work or school

Family & other users

Sync your settings

Sign-in options

Manage how you sign in to your device

Select a sign-in option to add, change, or remove it.

Windows Hello Face
Sign in with your camera (Recommended)

Windows Hello Fingerprint
Sign in with your fingerprint scanner (Recommended)

Windows Hello PIN
This option is currently unavailable—click to learn more

Security Key
Sign in with a physical security key

Manage a physical security key that can log you into applications.

Learn more

Manage

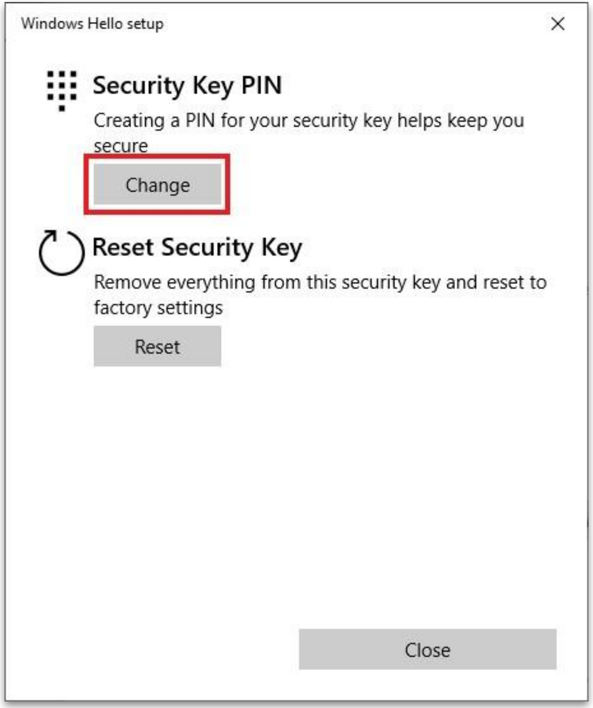
Password
Sign in with your account's password

Picture Password
Swipe and tap your favorite photo to unlock your device

Require sign-in

Windows Hello is preventing some options from being shown.

If you've been away, when should Windows require you to sign in again?



Windows Hello setup

Security Key PIN

Creating a PIN for your security key helps keep you secure

Change

Reset Security Key

Remove everything from this security key and reset to factory settings

Reset

Close

FIDO2 with RDP

FIDO2 Authentication to RDP Sessions

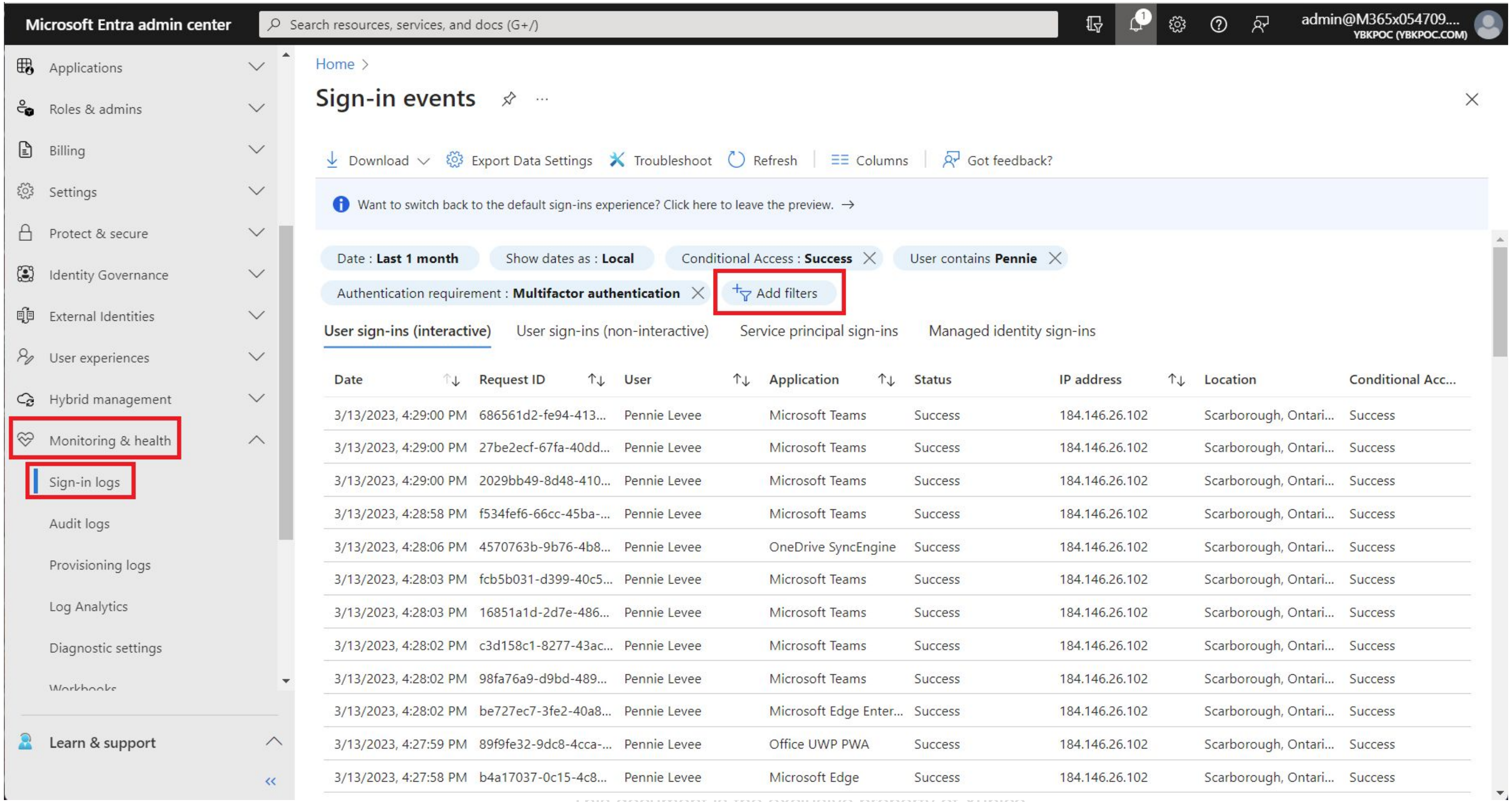
- **Requirements:**
  - The latest supported Windows 10/11 version with the latest updates
  - The remote host is either Windows 10/11 or Windows Server 2022/2025 with the latest updates
  - The remote host must be natively Entra ID or Entra ID hybrid-joined
  - The remote host must be accessible over NETBIOS name or FQDN (not IP address)
- **Instructions:**
  - The complete guide to RDP with Security Keys

Entra ID Sign-in Logs and Reporting

Entra ID Sign-in Logs

- **Provide detailed information about user sign-in activity**
  - User information
  - Date and time
  - Client application, user-agent
  - Authentication details (method, success/failure)
  - Device information
  - Location
  - Target resource
  - Conditional Access Policy applied

Entra ID Sign-in Logs



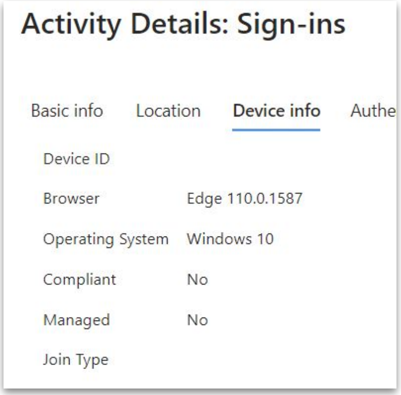
Sign-in events

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : **Last 1 month** | Show dates as : **Local** | Conditional Access : **Success** | User contains **Pennie** | Authentication requirement : **Multifactor authentication**

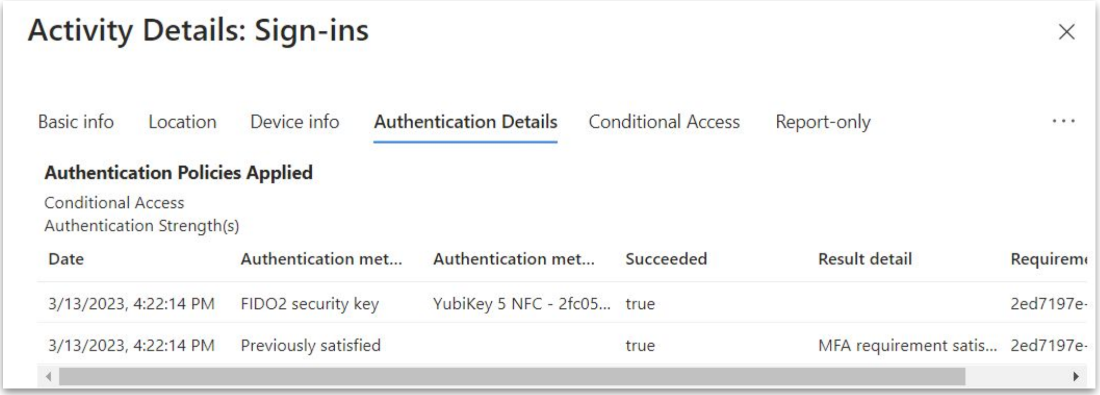
Date	Request ID	User	Application	Status	IP address	Location	Conditional Acc...
3/13/2023, 4:29:00 PM	686561d2-fe94-413...	Pennie Levee	Microsoft Teams	Success	184.146.26.102	Scarborough, Ontari...	Success
3/13/2023, 4:29:00 PM	27be2ecf-67fa-40dd...	Pennie Levee	Microsoft Teams	Success	184.146.26.102	Scarborough, Ontari...	Success
3/13/2023, 4:29:00 PM	2029bb49-8d48-410...	Pennie Levee	Microsoft Teams	Success	184.146.26.102	Scarborough, Ontari...	Success
3/13/2023, 4:28:58 PM	f534fef6-66cc-45ba-...	Pennie Levee	Microsoft Teams	Success	184.146.26.102	Scarborough, Ontari...	Success
3/13/2023, 4:28:06 PM	4570763b-9b76-4b8...	Pennie Levee	OneDrive SyncEngine	Success	184.146.26.102	Scarborough, Ontari...	Success
3/13/2023, 4:28:03 PM	fcb5b031-d399-40c5...	Pennie Levee	Microsoft Teams	Success	184.146.26.102	Scarborough, Ontari...	Success
3/13/2023, 4:28:03 PM	16851a1d-2d7e-486...	Pennie Levee	Microsoft Teams	Success	184.146.26.102	Scarborough, Ontari...	Success
3/13/2023, 4:28:02 PM	c3d158c1-8277-43ac...	Pennie Levee	Microsoft Teams	Success	184.146.26.102	Scarborough, Ontari...	Success
3/13/2023, 4:28:02 PM	98fa76a9-d9bd-489...	Pennie Levee	Microsoft Teams	Success	184.146.26.102	Scarborough, Ontari...	Success
3/13/2023, 4:28:02 PM	be727ec7-3fe2-40a8...	Pennie Levee	Microsoft Edge Enter...	Success	184.146.26.102	Scarborough, Ontari...	Success
3/13/2023, 4:27:59 PM	89f9fe32-9dc8-4cca-...	Pennie Levee	Office UWP PWA	Success	184.146.26.102	Scarborough, Ontari...	Success
3/13/2023, 4:27:58 PM	b4a17037-0c15-4c8...	Pennie Levee	Microsoft Edge	Success	184.146.26.102	Scarborough, Ontari...	Success

Entra ID Sign-in Logs



Activity Details: Sign-ins

Device ID	
Browser	Edge 110.0.1587
Operating System	Windows 10
Compliant	No
Managed	No
Join Type	

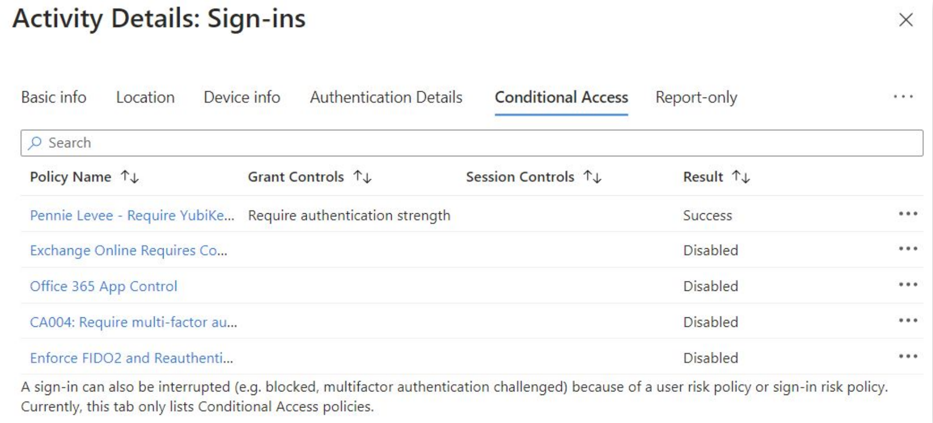


Activity Details: Sign-ins

Authentication Policies Applied

Conditional Access
Authentication Strength(s)

Date	Authentication met...	Authentication met...	Succeeded	Result detail	Requireme
3/13/2023, 4:22:14 PM	FIDO2 security key	YubiKey 5 NFC - 2fc05...	true		2ed7197e-
3/13/2023, 4:22:14 PM	Previously satisfied		true	MFA requirement satis...	2ed7197e-



Activity Details: Sign-ins

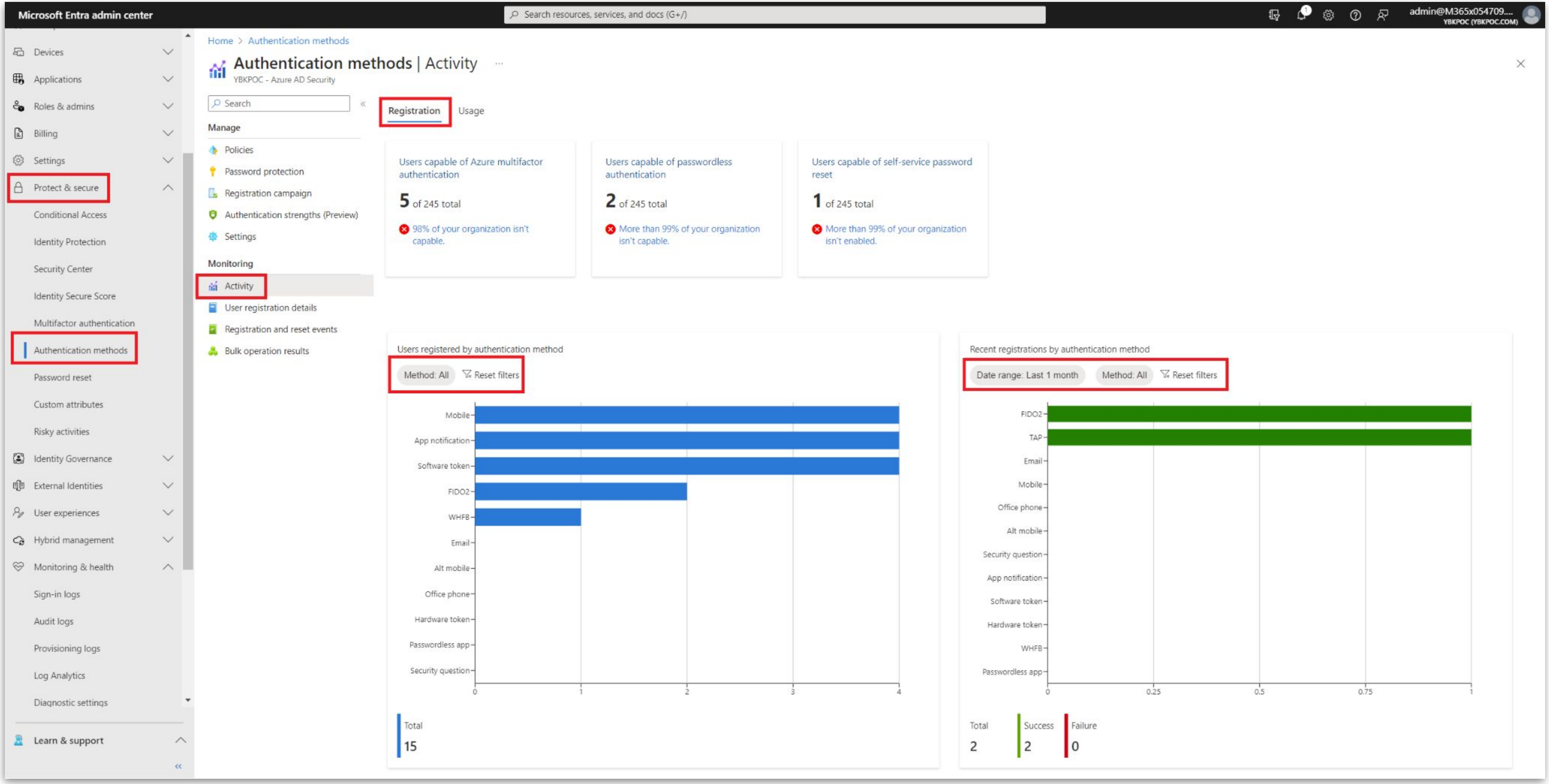
Policy Name ↑↓	Grant Controls ↑↓	Session Controls ↑↓	Result ↑↓
Pennie Levee - Require YubiKe...	Require authentication strength		Success
Exchange Online Requires Co...			Disabled
Office 365 App Control			Disabled
CA004: Require multi-factor au...			Disabled
Enforce FIDO2 and Reauthenti...			Disabled

A sign-in can also be interrupted (e.g. blocked, multifactor authentication challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.

Entra ID Reporting

- **Entra ID provides an activity dashboard that enables admins to:**
  - Monitor authentication method registrations
  - Monitor authentication method usage
- **Helps with tracking the progress of MFA device registration and the adoption of passwordless authentication methods**

Entra ID Reporting



Authentication methods | Activity

YBKPOC - Azure AD Security

Users capable of Azure multifactor authentication

5 of 245 total

98% of your organization isn't capable.

Users capable of passwordless authentication

2 of 245 total

More than 99% of your organization isn't capable.

Users capable of self-service password reset

1 of 245 total

More than 99% of your organization isn't enabled.

Users registered by authentication method

Method: All | Reset filters

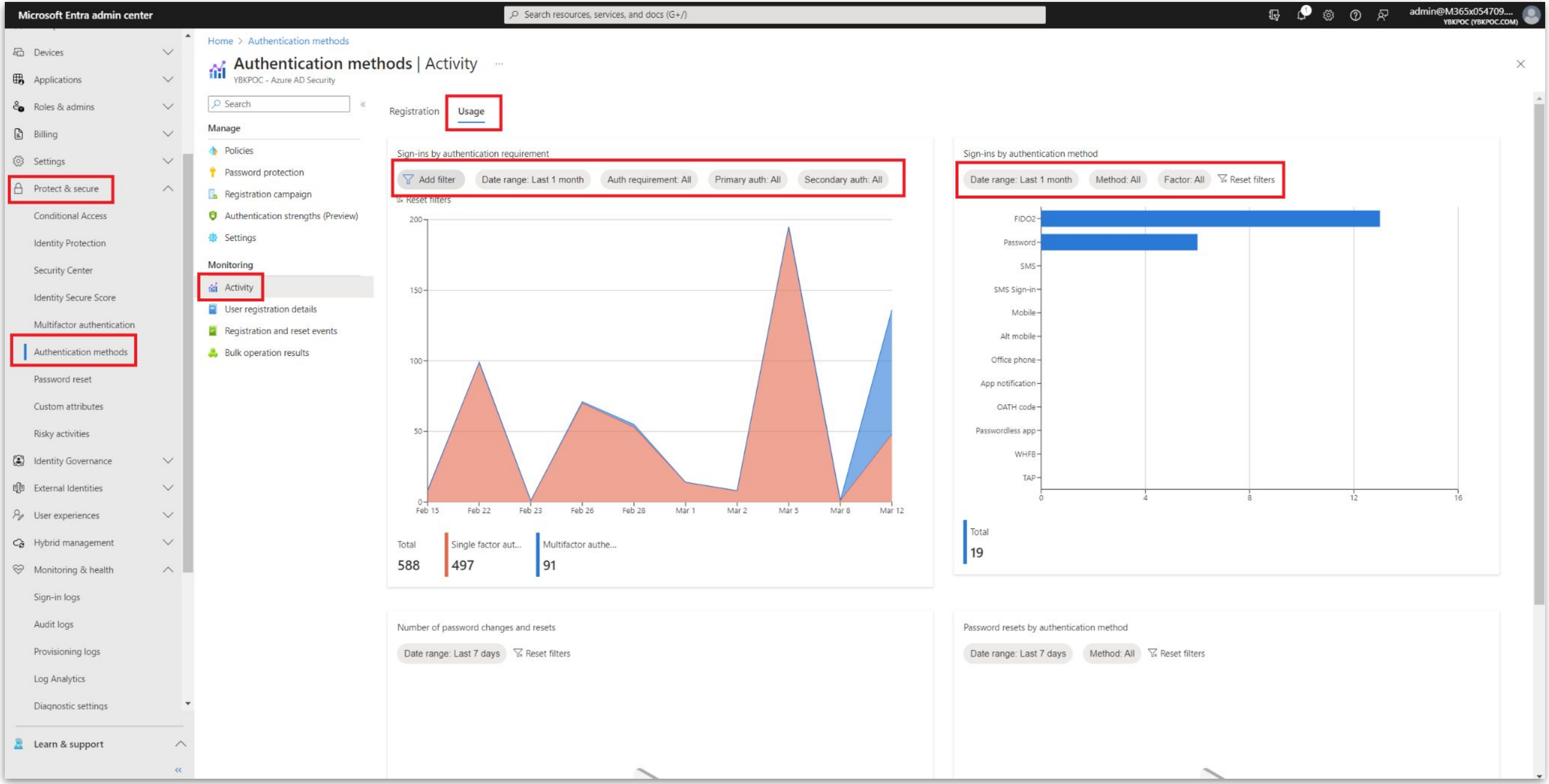
Total 15

Recent registrations by authentication method

Date range: Last 1 month | Method: All | Reset filters

Total	Success	Failure
2	2	0

Entra ID Reporting



Authentication methods | Activity

YBKPOC - Azure AD Security

Sign-ins by authentication requirement

Date range: Last 1 month · Auth requirement: All · Primary auth: All · Secondary auth: All

Total 588 · Single factor aut... 497 · Multifactor authe... 91

Sign-ins by authentication method

Date range: Last 1 month · Method: All · Factor: All

Total 19

Number of password changes and resets

Date range: Last 7 days

Password resets by authentication method

Date range: Last 7 days · Method: All

What’s Next?

Deployment Best Practices Workshop

Planning for the operational aspects of a YubiKey deployment

The workshop will cover…

- Project readiness & planning
- Distributing YubiKeys
- Preparing and training end users
- YubiKey lifecycle management
- Successful user communications
- Customer deployment stories
- Available resources and materials

YubiKey Deployment Office Hours

Join us for open sessions to answer your questions, troubleshoot, provide consultation and discuss YubiKeys

Tuesdays at 1 PM	Fridays at 10 AM
Join Microsoft Teams Meeting	Join Microsoft Teams Meeting
ID: 243436492249	ID: 215605564804
Passcode: mQ6KU3ZC	Passcode: wi6CL3Ln

Professional Services Hours

Features

On-demand consulting

Provides technical and operational guidance when you need it

Flexible hours

Not tied to a specific engagement timeline. Hours can be used over 12 month period

Multiple methods of assistance

Can be used to schedule virtual meetings or email with PS engineers and advisors

How to communicate with Professional Services

1. Open a support case online (https://yubi.co/support). This is the preferred contact method for most scenarios as your support case will be logged for future reference
2. Email us at **professional-services@yubico.com**

Professional Services Hours

Features

On-demand consulting

Provides technical and operational guidance when you need it

Flexible hours

Not tied to a specific engagement timeline. Hours can be used over 12 month period

Multiple methods of assistance

Can be used to schedule virtual meetings or email with PS engineers and advisors

How to contact Yubico

1. Open a support case online (https://yubi.co/support). This is the preferred contact method for most scenarios as your support case will be logged for future reference
2. Email us at **professional-services@yubico.com**

Questions and Wrap-Up

Questions