# YubiKeys for Azure AD Passwordless

# **User Enablement Guide**

#### Copyright

© 2023 Yubico Inc. All rights reserved.

#### Trademarks

Yubico and YubiKey are registered trademarks of Yubico Inc. All other trademarks are the property of their respective owners.

#### Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

#### **Contact Information**

Yubico Inc 5201 Great America Pkwy #122 Santa Clara, CA 95054 USA yubi.co/contact

#### **Original Document Release Date**

September 22, 2020

#### Version History

Version	Date	Changes
2.2	May 8th, 2023	Edits and Revisions to User Guide
2.1	July 29, 2021	Minor revisions
2.0	March 2, 2021	Updated for general availability
1.0	October 6, 2020	Added YubiKey Lifecycle Management Section
0.5	September 22, 2020	Initial Release

Copyright	2
Trademarks	2
Disclaimer	2
Contact Information	2
Document Release Date	2
Version History	2
Introduction	3
Objectives	3
Before you begin	3
Minimum Requirements	4
Hardware	4
Software	4
YubiKey Bio Series Setup (if applicable)	4
Temporary Access Pass (TAP) for Users	5
Register a YubiKey to your account	7
View your account's security information	7
Add a YubiKey as a security method	9
Sign into a website with a YubiKey	12
Sign into Windows 10 with a YubiKey	15
Single sign-on (SSO) to a website	16
YubiKey Lifecycle Management	17
Change YubiKey PIN	20
Using native Windows 10 tools	20
Using Google Chrome (macOS only)	20
Using YubiKey Manager	21
Reset the YubiKey	21
Using native Windows 10 tools (*Spring 2020 version and up)	21
Using Google Chrome (macOS only)	23
Using YubiKey Manager	24
Removing a YubiKey as a security method	25
References	27

# Introduction

These instructions explain how to enable and use YubiKeys with Azure Multi-Factor Authentication (Azure MFA) as a FIDO2 security key. This document focuses on cloud-based Azure MFA implementations.

# **Objectives**

- User-driven self-enrollment of a YubiKey for Azure AD authentication.
- Sign into a website using a previously enrolled YubiKey.
- Sign into a Windows 10 device using an enrolled YubiKey.
- Single sign-on to a web site, Office 365, using a YubiKey.

### Before you begin

- Ensure that the YubiKey supports Azure AD Passwordless. All YubiKeys that support FIDO2 will work for Azure AD Passwordless. If you are unsure please see this site, Identifying your YubiKey, for help.
- Use a browser that supports Azure AD Passwordless. Work with your IT support team to determine which browser is best for your organization. Edge or Chrome are recommended.
- There is a limit of ten security keys per user. If your account already has ten security keys one will have to be removed to register a new YubiKey.
- The Windows 10 device must already be joined to your company's Azure AD tenant. (Note: The first time you sign-in with a YubiKey, you must have internet connectivity. For subsequent sign-in events, cached sign-in should work and authenticate without internet connectivity)

### **Minimum Requirements**

### Hardware

- At least one and preferably two of any of these YubiKeys
  - YubiKey 5 Series
  - YubiKey Bio series
  - or YubiKey Security Key

### Software

- Azure Hybrid Environments.
  - Windows 10 2004+.
- Azure Only Environments.
  - Windows 10 1903.
- Browser that supports Azure AD Passwordless.

• Latest browser support for WebAuthn can be found here: <u>Browser support of</u> <u>FIDO2 passwordless authentication - Microsoft Entra</u>

# YubiKey Bio Series Setup (if applicable)

To use the YubiKey Bio series, it is required to set up the YubiKey Bio with a PIN and enrolled fingerprints prior to registering the YubiKey Bio with the Azure AD account.

- 1. Set YubiKey Bio PIN (new YubiKey Bio device)
  - a. From Windows, **Start Menu > Settings > Accounts > Sign-in Options**.
  - b. Click Security Key. Once expanded, click Manage.



c. Under Security Key PIN: click Add



d. When prompted, enter and confirm new PIN, then click **OK**:

Windows He	Windows Hello setup X				
Set up	Set up a security key PIN				
	•••••				
•	•••••		0		
	<b>.</b>				
	OK	Cancel			

e. The FIDO2 PIN has now been set on the YubiKey Bio.

#### 2. Add a Fingerprint to the YubiKey Bio

- a. From Windows, navigate to "Sign-in Options" from the Start Menu.
- b. Click **Security Key.** Once expanded, click **Manage.** If prompted, touch the capacitive gold ring on the YubiKey Bio.



c. Under Security Key Fingerprint, click Set Up.



- d. When prompted, enter the PIN.
- e. Follow the prompts to enroll your fingerprint.



f. Your fingerprint is now enrolled in the YubiKey Bio.

Windows Hello setup	×
All set! Use your fingerprint the next time you want to unlock your device.	
Add another finger	

g. Repeat this process to register an additional fingerprint. *Note: There is a limit of 5 registered fingerprints per YubiKey Bio at the time of this writing.* 

### **Temporary Access Pass (TAP) for Users**

A Temporary Access Pass (TAP) is an authentication method to allow users to authenticate without a password (Passwordless). This limited time passcode is typically used for First login, device setup or credential reset (lost password, etc.). The passcode is created for eligible users by an administrator and should be distributed to the user via a secure method. Once the user receives the passcode follow the steps below.

### Users authenticating using TAP

Open a web browser to https://aka.ms/mysecurityinfo.

⊲ ⊳ C		Д	🕄 https	://aka.ms/my	securityinfo	
G Dashboard	PIV Content	🛄 Yu	bico_Corp	OTP Info	FIDO Info	🔲 Testinç

Enter the UPN of the account you created the Temporary Access Pass for, such as <u>tapuser@contoso.com</u>.

⊲ ▷ C 🛛 🔒 login.m	icrosoftonline.com/common/oauth2/v2.0/authorize? 🖞   🦁	🔺 🔹 🖬 🖬 🛃
G Dashboard 📄 PIV Content 📄 Yubico	_Corp _ OTP Info _ FIDO Info _ Testing _ SE Info	
	Microsoft	
	Sign in	
	yubiuser@bundylabs.onmicrosoft.com	
	Can't access your account?	
	Next	
	INCAL	
	Sign-in options	
		Terms of use Privacy & cookies ····

If the user is included in the Temporary Access Pass policy, they'll see a screen to enter their Temporary Access Pass.

	oftonline.com/common/oauth2/v2.0/autho 🗢 🖞 🕴	🦻 🔺 🗈 🖬 🐶 E
G Dashboard 📄 PIV Content 📄 Yubico_Corp	OTP Info 🚺 FIDO Info 🚺 Testing 🚺 SE Info	
	Microsoft	
	$\leftarrow$ yubiuser@bundylabs.onmicrosoft.com	
	Enter Temporary Access Pass	
	w\$8*dz=@	
	Show Temporary Access Pass	
	Other ways to sign in	
	Sign in	
	Gign in	
		Terms of use Privacy & cookies

Enter the Temporary Access Pass that was displayed in the Azure portal. The user will be directed to the users Authentication methods page to allow for management of credentials.

		ation in SE late	ð   🦁 🖌	<u>×</u> *	6	• VPN	Ð
Wy Sign-Ins ~	Tubico_Corp OTPINTO FIDO INTO I TE	sting SE into			Å	2	$(\mathbf{y})$
, e.ge	① For security reasons, we recommend that you delete any	sign-in methods that you no longer use.					×
A Overview	Socurity info						
𝒫 Security info	These are the methods you use to sign into your ac	count or reset your password.					
Organizations	Default sign-in method: Microsoft Authenticator	- notification Change					
💻 Devices	+ Add sign-in method						
A Privacy	Microsoft Authenticator     Push multi-factor authentication (MFA)	VicsiPhone		Delete			
	Security key	YubiKey 5c - yubiuser		Delete	$\sim$		
	Temporary access pass	Expires 5/9/2023, 10:39:36 AM		Delete			
	Lost device? Sign out everywhere						

#### **Note**: Microsoft TAP Documentation can provide additional information, <u>https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-t</u> <u>emporary-access-pass#use-a-temporary-access-pass</u>.

# **Register a YubiKey to your account**

### View your account's security information

**Note**: There are several ways for a user to access the page to register a security key. Determine which method your organization should use to best fit your needs. The site described below is Microsoft's new page for users to manage their profile, <u>https://myprofile.microsoft.com</u>.

- 1. Open a browser window using a <u>supported browser</u>. Sign out of all other Microsoft accounts and close all other browser windows.
- 2. Navigate to https://aka.ms/mysecurityinfo.
- 3. If you have signed in before you will see an account selection window, select the account you would like to use, or enter the account name to your Microsoft account.



- 4. Enter your password and conduct your multi-factor authentication steps if prompted. You may need to select your account to proceed.
- 5. Select **Security Info** in the left navigation or **Update Info** in the Security Info tile.

$ eal$ My Account $\checkmark$		8	?	8
<ul> <li>Overview</li> <li>Security info</li> <li>Devices</li> <li>Password</li> <li>Organizations</li> <li>Privacy</li> <li>My sign-ins (preview)</li> </ul>	YubiKey         Yubikey@yubicolabs.com	Security info Q Keep your verification methods and security info up to date.		

6. You may have to select your account and authenticate again to proceed to update the security information for your account.

### Add a YubiKey as a security method

1. Select Add method.

Security info				
These are the methods you use to sign into your acc	count or reset your password.			
Default sign-in method: Microsoft Authenticator - r	notification Change			
+ Add method				
Microsoft Authenticator	Pixel 3	Delete		

**Note: Another factor is required prior to registering a YubiKey.** If you do not already have one method registered, you will be required to authenticate using another method, such as the <u>Azure AD Temporary Access Pass</u>, before adding a security key. Follow the steps for adding an alternative method first, then click Add method again.

2. Select **Security key** then click **Add**.

Add a method	
Which method would you like to add?	
Security key	~
Authenticator app	
Phone	
Alternate phone	
Email	
Security key	

3. Select **USB** if you will be plugging in your YubiKey into your device, or **NFC** if you will be using placing your YubiKey on a NFC reader either embedded in your device or plugged into your device. Note that this is just for registration, any method can be used for signing in after registration.

Security key	
Choose the type of security key that you have.	
NFC device	
	Cancel

4. Select Next to start the registration process.

Security key		
Have your key ready.		
When you choose Next, you will be promp key into the USB port. Then, touch the bu security key to finish setting up your device	oted to plug your s tton or the sensor <sup>ce.</sup>	security on your
For more detailed instructions, visit your k	ey manufacturer's	website.
	Back	Next

- 5. If prompted, click **Continue** or **OK** in the browser prompt to acknowledge that a record of you visiting Microsoft.com will be recorded on your YubiKey. This information is only readable by you and Microsoft, no other services will be able to read this information.
- 6. Insert your YubiKey into a USB port or place it on a NFC reader.
- 7. If you are using the **YubiKey Bio series**, you will be prompted to touch your Yubikey Bio as shown below. Use one of your enrolled fingerprints to authenticate via the sensor on the YubiKey Bio.



8. If you are using the YubiKey 5 series or Security Key by Yubico, you will be prompted to enter the PIN code for this YubiKey (i), OR if there is not a PIN code set on the YubiKey, you will be prompted to create one (ii).

This PIN code only applies to this YubiKey and is not transmitted to Microsoft or any other YubiKey.

	Windows Security			
	Making sure it's you			
	Set up your security key to sign in to login.microsoft.com as yubikey@yubicolabs.com.			
	This request comes from Firefox, published by Mozilla Corporation.			
	Please enter your security key PIN.			
	PIN PIN			
	Change PIN			
	OK Cancel			
(i)				

Windows Security	×	
Making sure it's you		
Set up your security key to sign in to login.microsoft.com as yubikey@yubicolabs.com.		
This request comes from Firefox, published by Mozilla Corporation.		
You'll need to create a PIN for this		
security key.		
Confirm PIN		
Confirm PIN OK Cancel	1	

- 9. Tap the flashing sensor on your YubiKey or tap it on the NFC reader to continue.
- 10. If prompted, click **Allow** to send Microsoft the model of the YubiKey used. There is no personally identifiable information sent.
- 11. Type a unique name for this YubiKey then select **Next**. It is recommended to use a name that is meaningful to easily know which YubiKey it is, such as "YubiKey 5C NFC wallet", or "YubiKey 5 nano backup".

Security key		
Name your security key. This will hel YubiKey nano Office Laptop	p distinguish it fron	n other keys.
	Cancel	Next

12. Select **Done** to complete the registration process.

# Sign into a website with a YubiKey

Note: Any site that uses the Azure AD sign in page will work, including Office 365 or a non-microsoft site that has been federated with Azure AD.

This example uses <u>https://portal.office.com</u>.

Your YubiKey must first be registered to your Azure AD account before you can use it to sign into Microsoft services.

- 1. Open a browser window using a supported browser.
- 2. Navigate to <u>http://portal.office.com</u> and select sign in.
- 3. Select your account that has a YubiKey registered to it or select Use another account.

<mark>∎</mark> № Pick	licrosoft an account	
à	yubikey@yubicolabs.com	÷
+	Use another account	

4. Select Sign in with Windows Hello or a security key.



5. If you selected Use another account in the previous step select Sign-in options.

Microsoft		
Sign in		
Email, phone, or Skype	<u>,</u>	
No account? Create one!		
Can't access your account	t?	
Sign-in options		
	Back	Next

- 6. Insert your YubiKey into a USB port or place on a NFC reader.
- 7. Enter your YubiKey PIN code when prompted **or** if using a YubiKey Bio series, touch the biometric sensor with an enrolled fingerprint to unlock the FIDO2 credential.



- 8. Tap the flashing sensor on your YubiKey or tap it on the NFC reader to continue.
- 9. Sign in complete.

# Sign into Windows 10 with a YubiKey

1. Select Sign-in options at the Windows 10 sign in screen.



2. Select the security key icon.



3. Insert your YubiKey into a USB port or place on a NFC reader.



4. Enter the PIN code for this YubiKey then press enter.

**Note** - if using the YubiKey Bio series, you will not be prompted to enter the PIN but instead touch the YubiKey with an enrolled fingerprint.



- 5. Tap the flashing sensor on your YubiKey or tap it on the NFC reader to continue.



6. You are now signed in to Windows using your Azure AD account.

# Single sign-on (SSO) to a website

Note: Any site that uses the Azure AD sign in page will work, including Office 365 or a non-microsoft site that has been federated with Azure AD.

This example uses <a href="https://portal.office.com">https://portal.office.com</a>.

- 1. Open the Edge browser.
- 2. Navigate to <u>https://portal.office.com</u>.
- 3. You are now signed in to Office 365.

## YubiKey Lifecycle Management

This section outlines some additional considerations when managing YubiKeys, to include removal of YubiKeys from a user account, changing the PIN, or resetting the YubiKey. The end user has the option to use the following tools:

- 1) Windows 10 Security Key Settings under Account Settings
- 2) macOS Google Chrome Security Key Settings
  - a) Supported on macOS 10.14 or later
  - b) Recommended version 85 or later
- 3) YubiKey Manager by Yubico
  - a) Supported on Microsoft Windows 10 (*admin privileges required*) or MacOS 10.14 or later
  - b) Recommended version 3.1 or later
  - c) This guide only outlines steps for the GUI. For CLI commands, please see the YubiKey Manager CLI User Manual: <u>https://support.yubico.com/hc/en-us/articles/360016614940</u>

### Change YubiKey PIN

Using native Windows 10 tools

- 1. Login to the Windows 10 machine.
- 2. Navigate to **Settings > Accounts > Sign-in options**.
- 3. Click Security Key. Once expanded, click Manage.

Ö	Security Key Sign in with a physical security key	
	Manage a physical security key that can log you i applications.	into
	Learn more	
		Manage

- 4. When prompted, touch the YubiKey and enter in the PIN.
- 5. Select **Change** to change the PIN on the YubiKey.



6. In the **Change your security key PIN** window, provide the current PIN, the new PIN, and confirm the new PIN again. Click **OK**.



7. The PIN is now changed.

#### Using Google Chrome (macOS only)

- 8. Open Google Chrome.
- 9. Navigate to "chrome://settings/securityKeys" in address bar or use the menu as described below:
  - a. Menu (  $\rightarrow$  )  $\rightarrow$  Settings.
  - b. From the left menu, select "**Privacy and security**." Under the **Privacy and security** menu, click **Security**.



- c. Under Advanced, click Manage security keys.
- 10. Click Create a PIN.
- 11. When prompted, insert the YubiKey and tap it.

Create a PIN		,
To continue, insert and touch your security key		
*		
	Cancel Save	

12. At the **Change a PIN** screen, enter in the current PIN, the new PIN, and confirm the new PIN. Once completed, click **Save**.

Change a PIN	
Enter your current the security key, th	PIN to change it. If you don't know your PIN, you'll need to reset hen create a new PIN.
Current PIN	
	0
Enter your new Pl letters, numbers, a	N. A PIN must be at least four characters long and can contain and other characters.
PIN	Confirm PIN
	Cancel Save

13. If successful, Chrome will indicate the PIN was created.

#### Using YubiKey Manager

1. Launch YubiKey Manager and insert the YubiKey. <u>Note</u>: On Windows 10, YubiKey Manager will need to be run as an administrator.



- 2. Navigate to Applications  $\rightarrow$  FIDO2.
- 3. Click Change PIN.
- 4. At the **Change FIDO2 PIN** screen, enter in the current PIN, the new PIN, and confirm the new PIN. Once completed, click **Change PIN**.

🐠 YubiKey Manager		_		×
	YubiKey 5 NFC (9861239)	Help	<li>Abou</li>	ut
yubico ⊦	lome Applications Inte	rfaces		
Change FI Home / FIDO2 / Change	DO2 PIN			
Current PIN ••	••			
New PIN ••	••			
Confirm new PIN ••	••			
< Back		✓ Chan	ge PIN	

5. YubiKey Manager will display Changed FIDO2 PIN when successful.

### Reset the YubiKey

Using native Windows 10 tools (\*Spring 2020 version and up)

Microsoft Windows allows end users to reset their security key if they have forgotten their PIN or need to delete the previously registered FIDO2 credentials.

# Warning!: If you reset your YubiKey, it will no longer be associated with your user account in Azure AD and will need to be re-registered.

**Note:** Windows 10 versions below Spring 2020 (2004) are not able to reset FIDO2 security keys successfully. Use a different method.

- 1. Navigate to **Settings > Accounts > Sign-in options**.
- 2. Click Security Key. Once expanded, click Manage.



- 3. When prompted, touch the YubiKey and enter in the PIN.
- 4. Select **Reset** to reset the security key.



5. Click **Proceed** to reset the Security Key.



6. When prompted, touch the YubiKey. The YubiKey is now reset.

Touch your security key.	
Learn more	

#### Using Google Chrome (macOS only)

- 1. Open Google Chrome.
- 2. Navigate to "chrome://settings/securityKeys" in address bar or use the menu as described below:
  - a. Menu ( i )  $\rightarrow$  Settings.
  - b. From the left menu, select "Privacy and security." Under the Privacy and security menu, click Security.

Î	Clear browsing data Clear history, cookies, cache, and more	+
٩	Cookies and other site data Third-party cookies are blocked in Incognito mode	•
O.	Security	
v	Safe Browsing (protection from dangerous sites) and other security settings	ŕ

- c. Under Advanced, click Manage security keys.
- 3. Click **Reset your security key**.
- 4. When prompted, remove the YubiKey from the device, reinsert the YubiKey and touch it.

Reset your security key	
To continue, remove your security key from your device, then reinse	rt and touch it
	Cancel

5. Touch the YubiKey again to confirm reset.



6. Chrome will display "Your security key has been reset" when completed.



#### Using YubiKey Manager

1. Launch YubiKey Manager and insert the YubiKey. **Note:** On Windows 10, YubiKey Manager will need to be run as an administrator.



- 2. Navigate to **Applications**  $\rightarrow$  **FIDO2**.
- 3. Select Reset FIDO.
- 4. When prompted to confirm, read the warning and click **Yes**. *Note: This will delete all FIDO2 credentials.*
- 5. Remove and re-insert the YubiKey.
- 6. When prompted, touch the YubiKey.

### Removing a YubiKey as a security method

- 1. From the local machine, open a browser window using a supported browser. Sign out of all other Microsoft accounts and close all other browser windows.
- 2. Navigate to https://aka.ms/mysecurityinfo.
- 3. If you have signed in before you will see an account selection window, select the account you would like to use, or enter the account name to your Microsoft account.



- 4. Enter your password and conduct your multi-factor authentication steps if prompted. You may need to select your account to proceed.
- 5. Select Security Info in the left navigation or Update Info in the Security Info tile.

$ eal$ My Account $\sim$		<b>P</b>	?	8
<ul> <li>Overview</li> <li>Security info</li> <li>Devices</li> <li>Password</li> <li>Organizations</li> <li>Privacy</li> <li>My sign-ins (preview)</li> </ul>	YubiKey         yubikey@yubicolabs.com	Security info Qo Keep your verification methods and security info up to date.		4

- 6. You may have to select your account and authenticate again to proceed to update the security information for your account.
- 7. Identify the Security Key you would like to remove and click **Delete**.

Security These are the me	<b>info</b> thods you use to sign into y	our account or reset your password.		
Default sign-in method: Microsoft Authenticator - notification Change				
+ Add metho	Ł			
Microsoft	Authenticator	Pixel 3	Delete	
Security k	³y	YubiKey	Delete 🗸	

8. When prompted to confirm deletion, click **OK**.

Delete security key			
Are you sure you would like to delete this method?			
	Ok	Cancel	

The YubiKey is now de-registered from the account.

#### RDP?

Call out mobile FIDO limitation

### References

Yubico and partner references that support this document.

• <u>Operating system and web browser support for FIDO2 and U2F</u> for latest platform support for FIDO2. Passwordless requires user verification and resident key support.