YubiKeys for Azure AD Passwordless

User Enablement Guide

© Yubico 2023.

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

© Yubico 2023.

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.

© Yubico 2023.

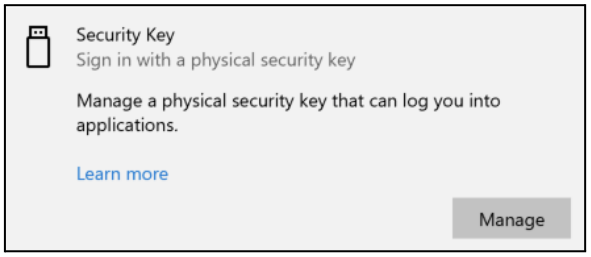
- Latest browser support for WebAuthn can be found here: [Browser support of FIDO2 passwordless authentication - Microsoft Entra]

YubiKey Bio Series Setup (if applicable)

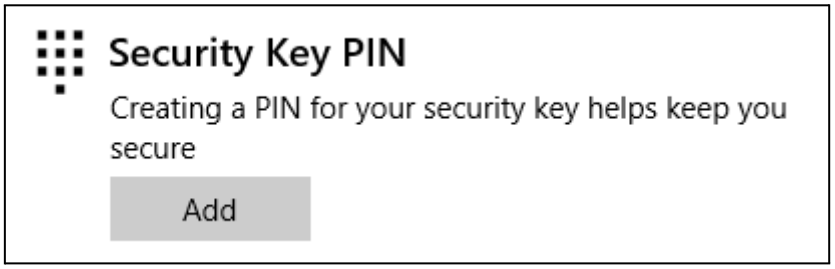
To use the YubiKey Bio series, it is required to set up the YubiKey Bio with a PIN and enrolled fingerprints prior to registering the YubiKey Bio with the Azure AD account.

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.**

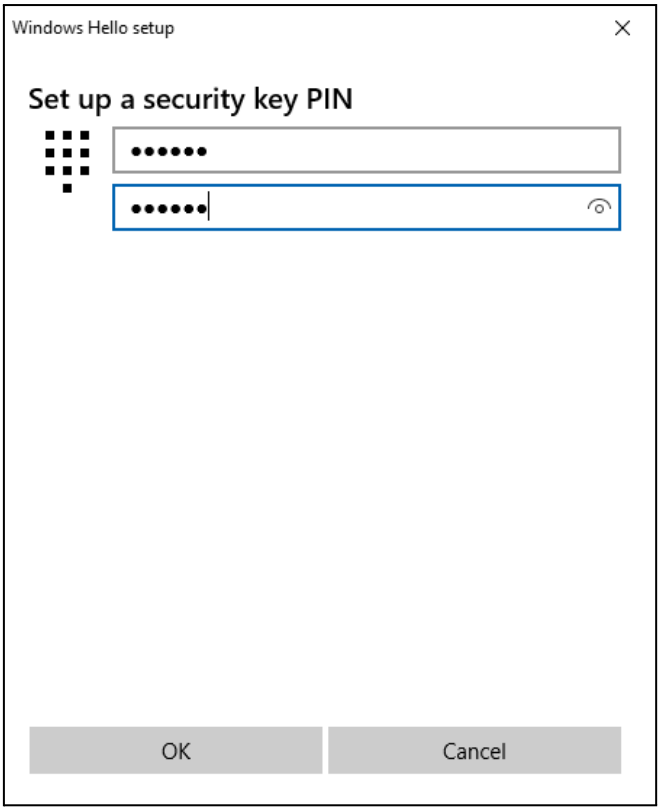


   c. Under **Security Key PIN:** click **Add**



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

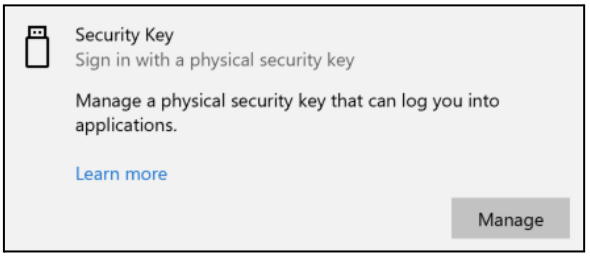
© Yubico 2023.



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

2. Add a Fingerprint to the YubiKey Bio

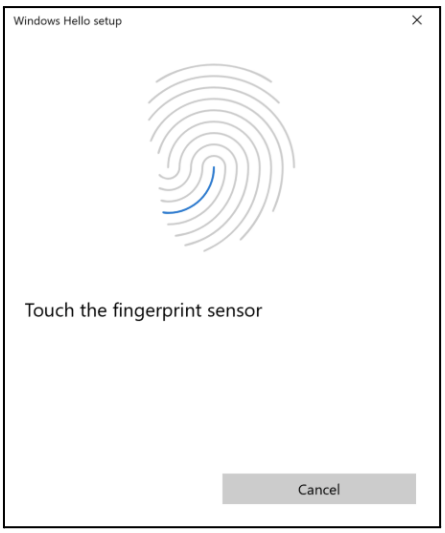
a. From Windows, navigate to "**Sign-in Options**" from the Start Menu.
b. Click **Security Key.** Once expanded, click **Manage.** If prompted, touch the capacitive gold ring on the YubiKey Bio.



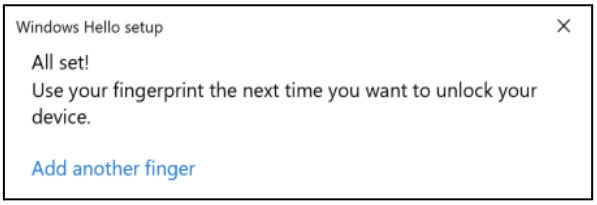
c. Under **Security Key Fingerprint,** click **Set Up**.

© Yubico 2023.

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



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



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.*

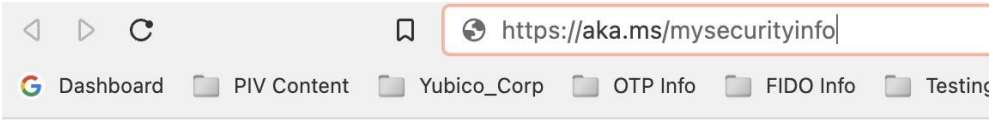
Temporary Access Pass (TAP) for Users

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.

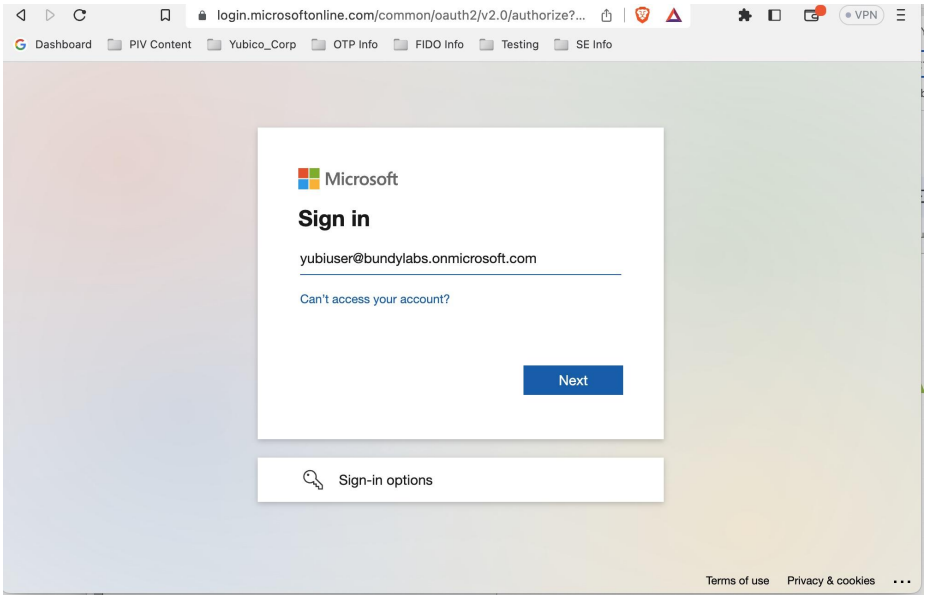
© Yubico 2023.

Users authenticating using TAP

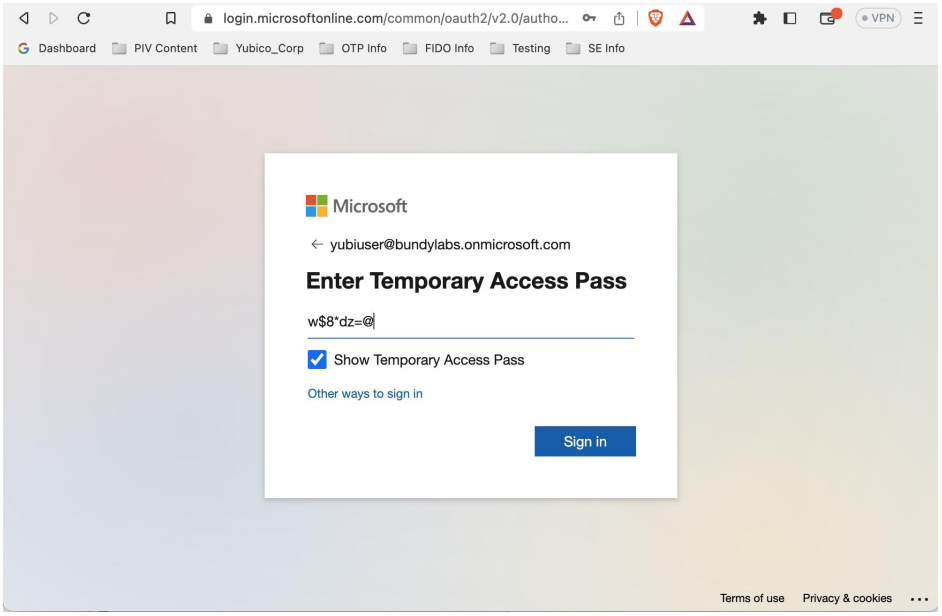
Open a web browser to https://aka.ms/mysecurityinfo.



Enter the UPN of the account you created the Temporary Access Pass for, such as *tapuser@contoso.com*.

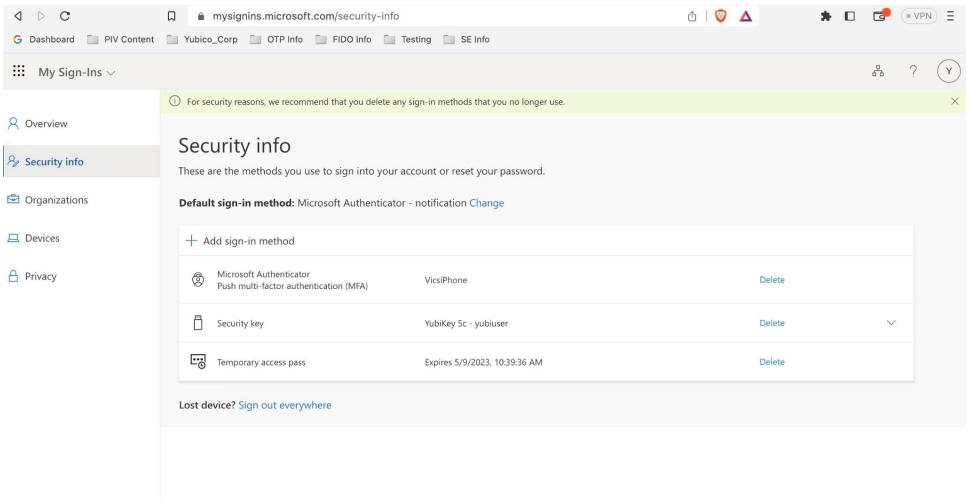


If the user is included in the Temporary Access Pass policy, they'll see a screen to enter their Temporary Access Pass.



© Yubico 2023.

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.



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

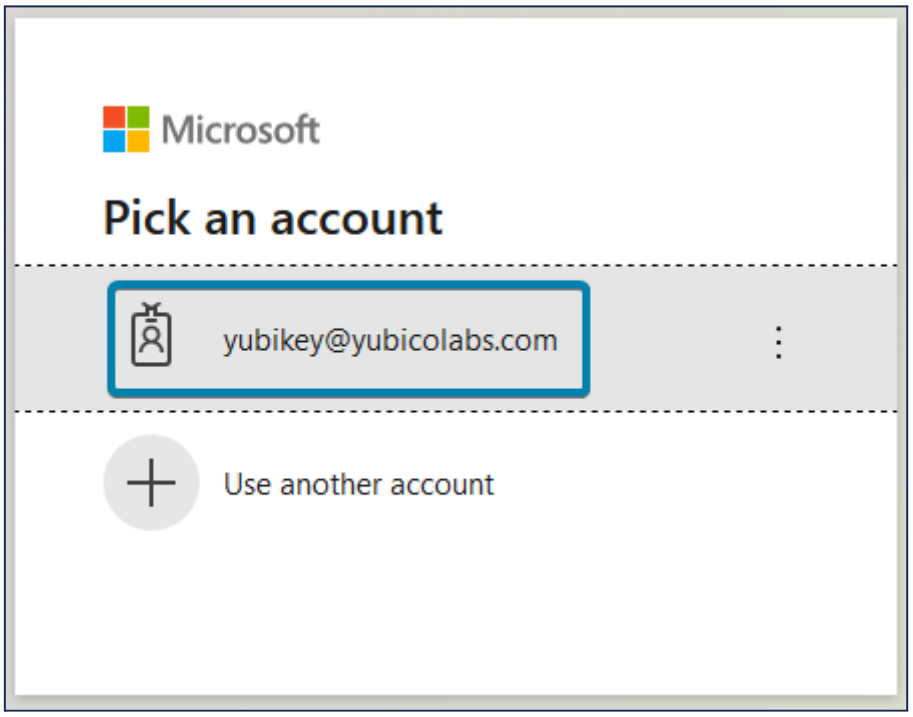
Register a YubiKey to your account

View your account's security information

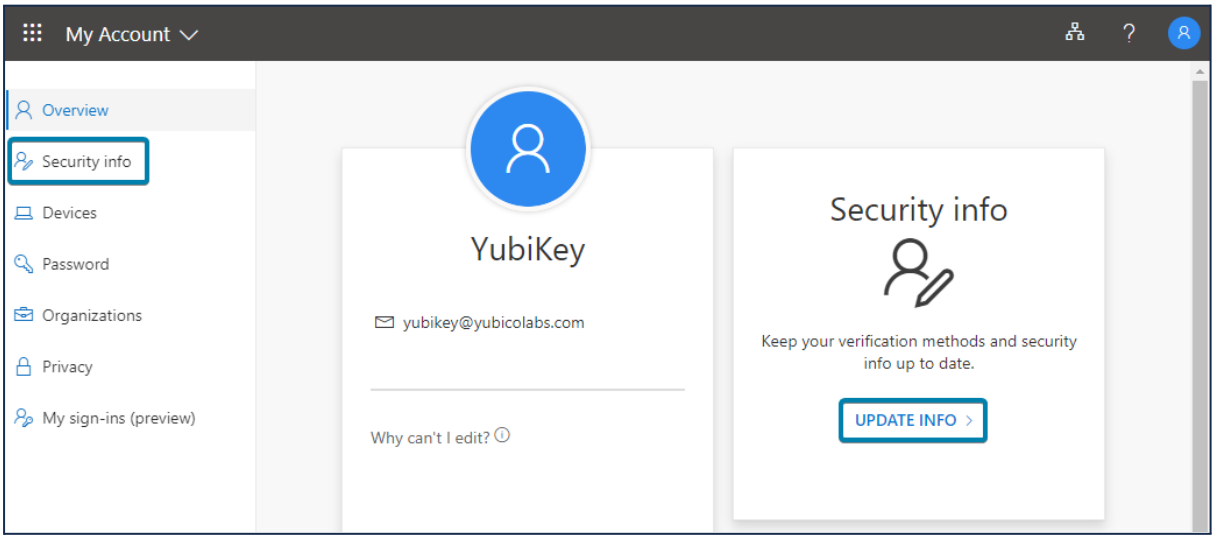
Note: There are several ways for a user to access the page to register a security key. Determine which method your organization should use to best fit your needs. The site described below is Microsoft's new page for users to manage their profile, https://myprofile.microsoft.com.

1. 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.

© Yubico 2023.



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.

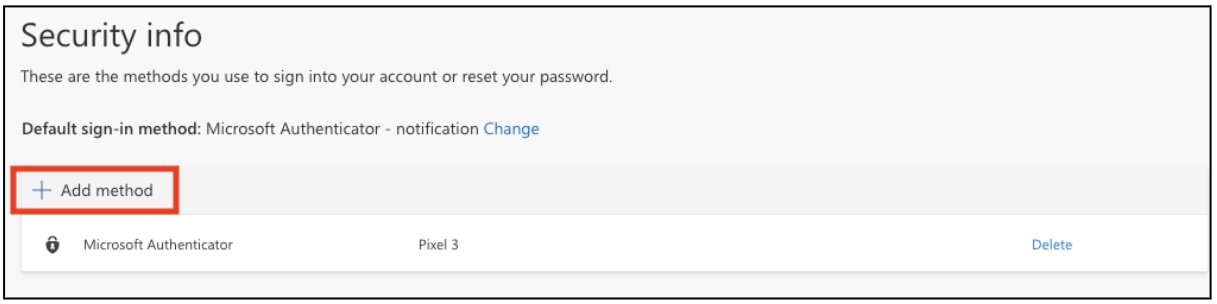


6. You may have to select your account and authenticate again to proceed to update the security information for your account.

Add a YubiKey as a security method

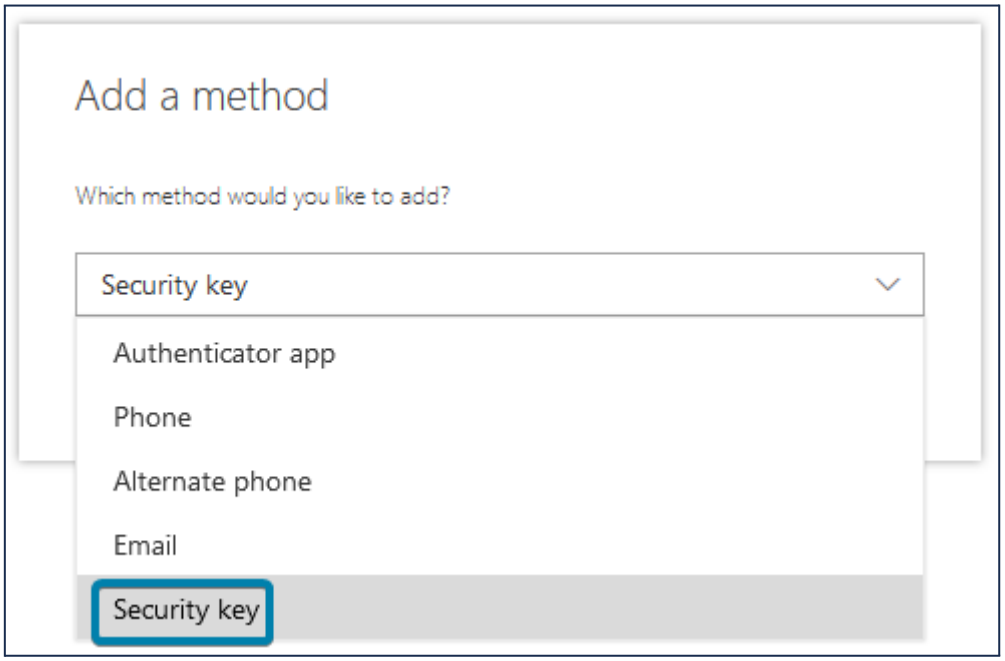
1. Select **Add method**.

© Yubico 2023.



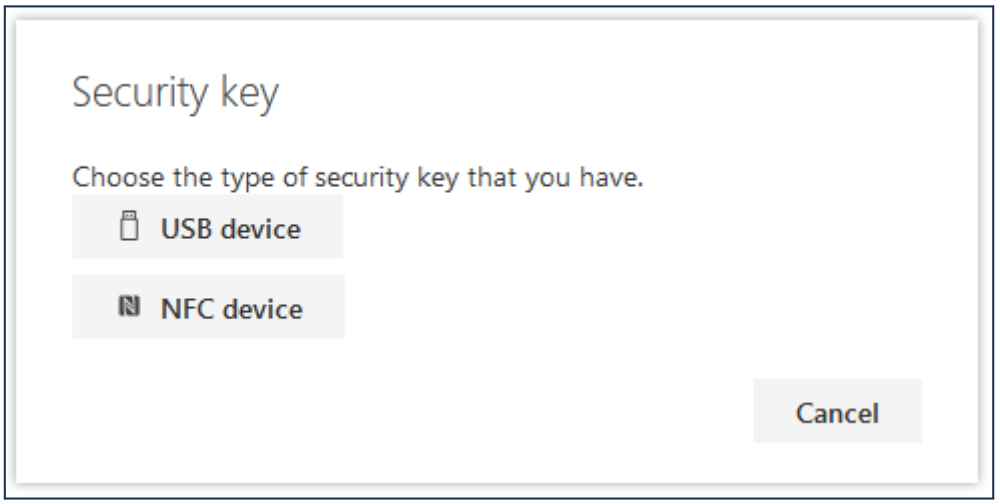
Note: Another factor is required prior to registering a YubiKey. If you do not already have one method registered, you will be required to authenticate using another method, such as the Azure AD Temporary Access Pass, before adding a security key. Follow the steps for adding an alternative method first,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

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

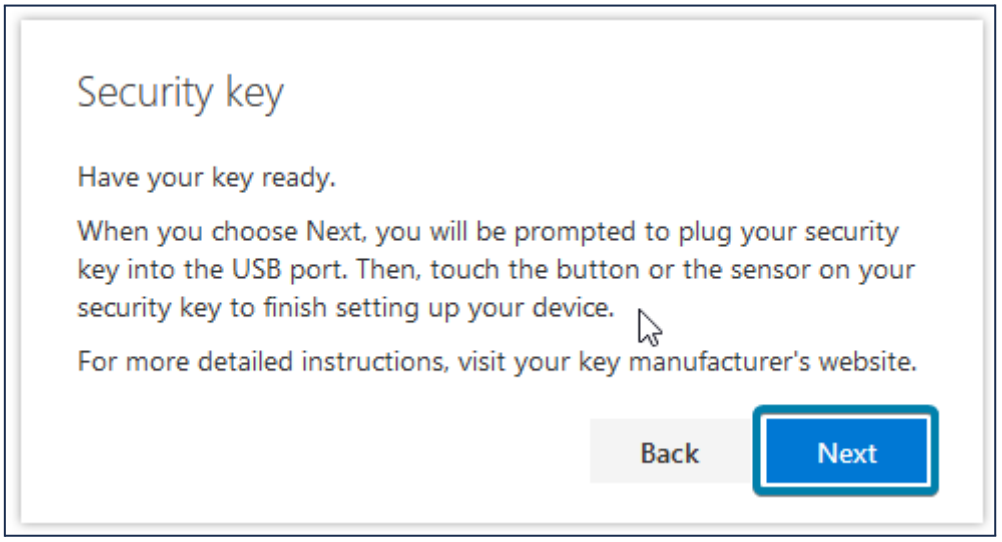


3. Select **USB** if you will be plugging in your YubiKey into your device, or **NFC** if you will be using placing your YubiKey on a NFC reader either embedded in your device or plugged into your device. Note that this is just for registration, any method can be used for signing in after registration.

© Yubico 2023.



4. Select Next to start the registration process.



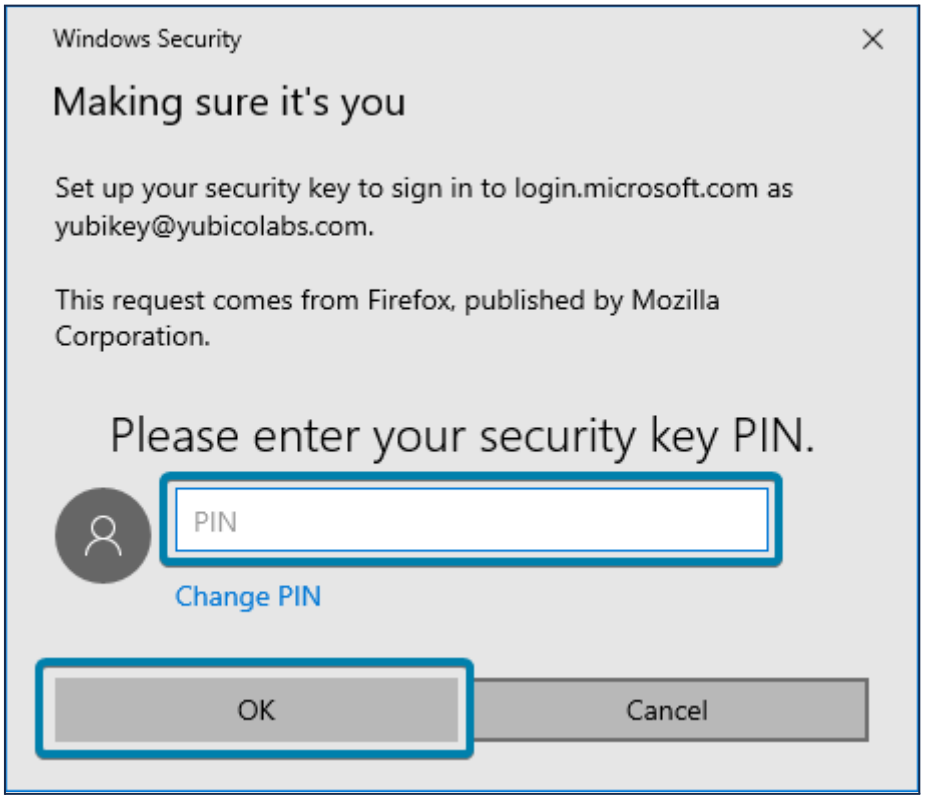
5. If prompted, click **Continue** or **OK** in the browser prompt to acknowledge that a record of you visiting Microsoft.com will be recorded on your YubiKey. This information is only readable by you and Microsoft, no other services will be able to read this information.
6. Insert your YubiKey into 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.

© Yubico 2023.

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).

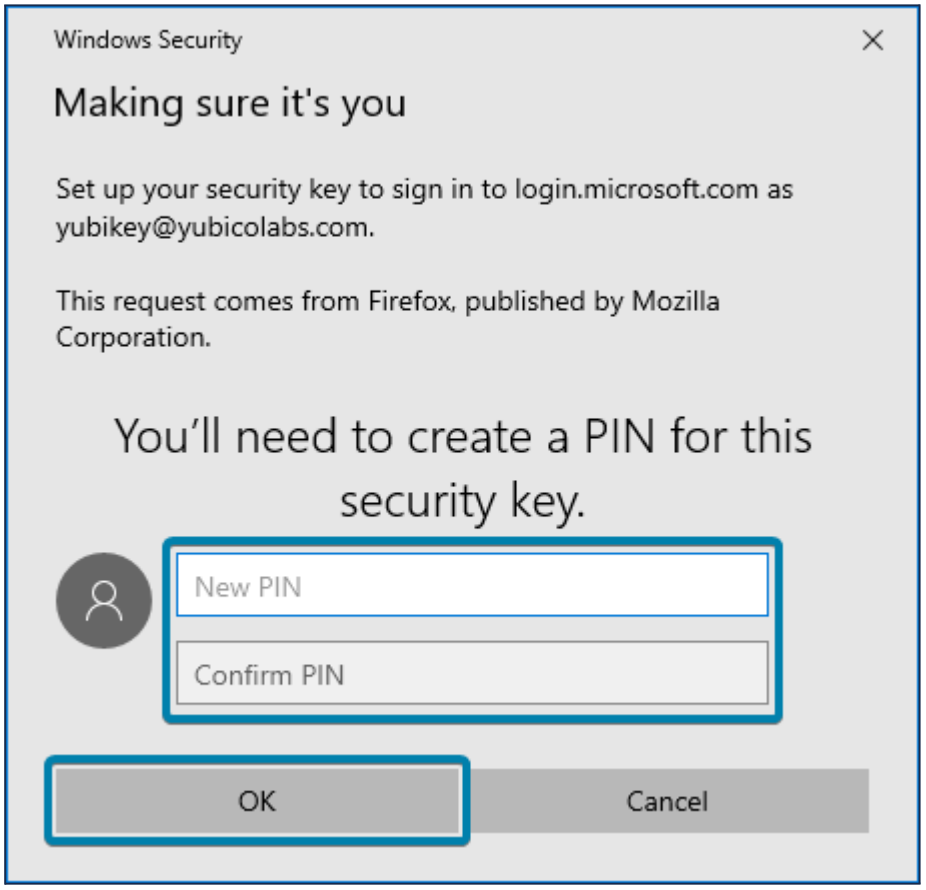
   This PIN code only applies to this YubiKey and is not transmitted to Microsoft or any other YubiKey.

(i)



© Yubico 2023.

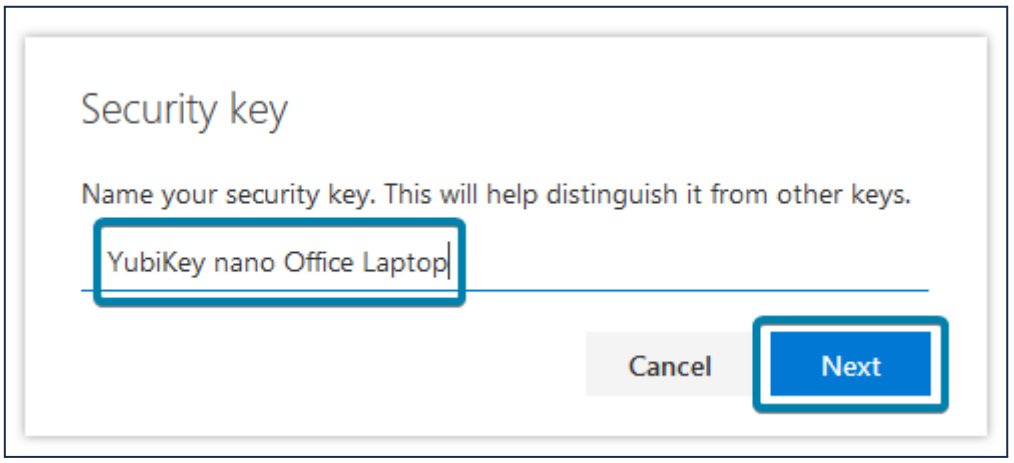
(ii)



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”.



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

© Yubico 2023.

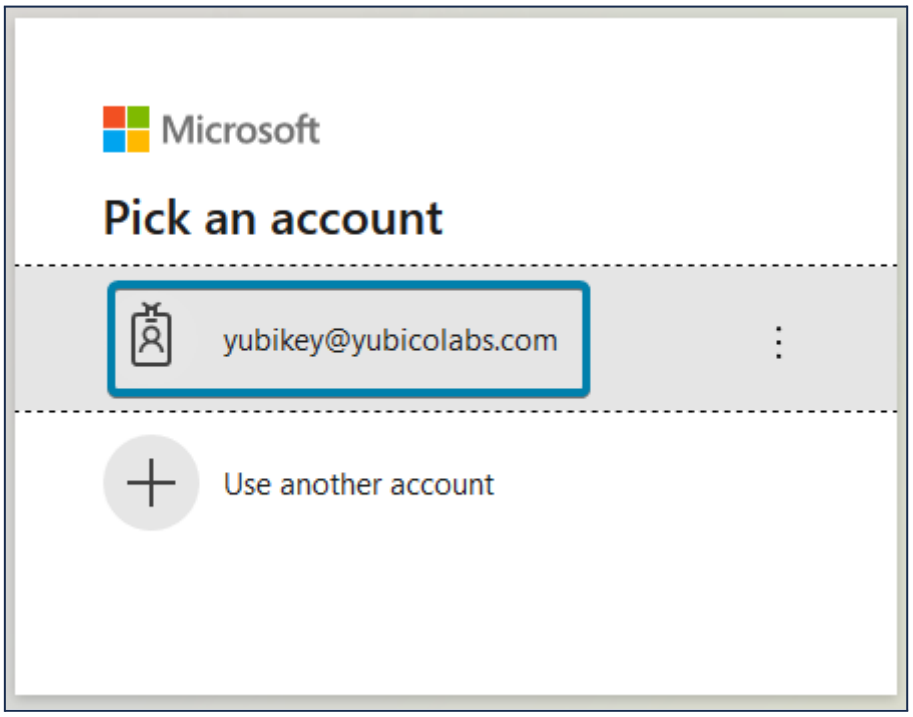
Sign into a website with a YubiKey

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 https://portal.office.com.

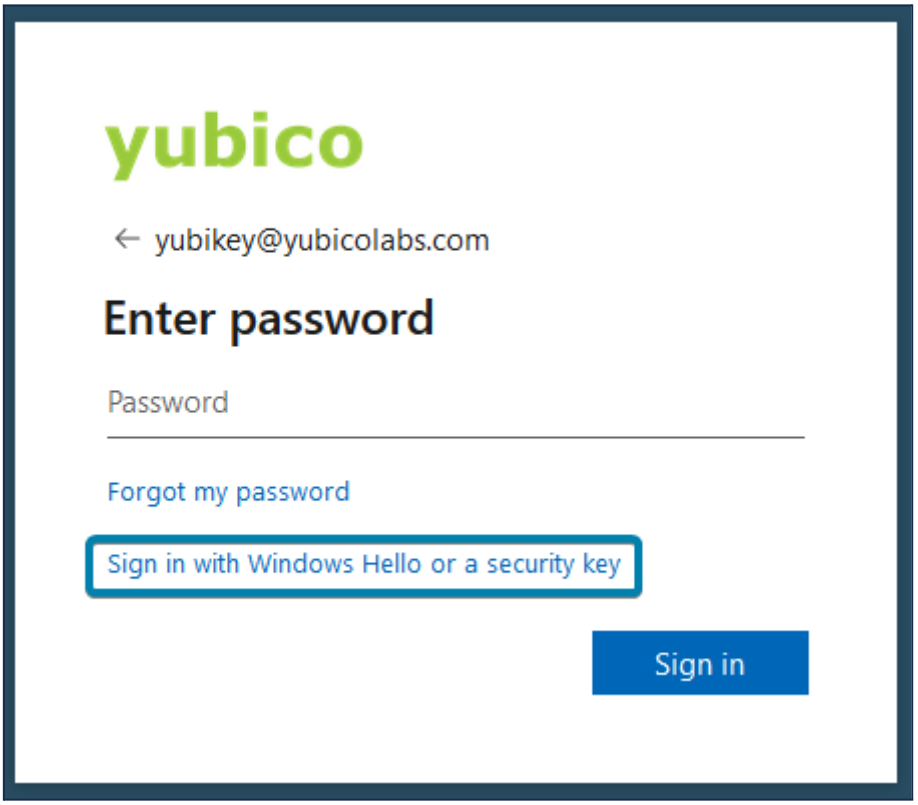
Your YubiKey must first be registered to your Azure AD account before you can use it to sign into Microsoft services.

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

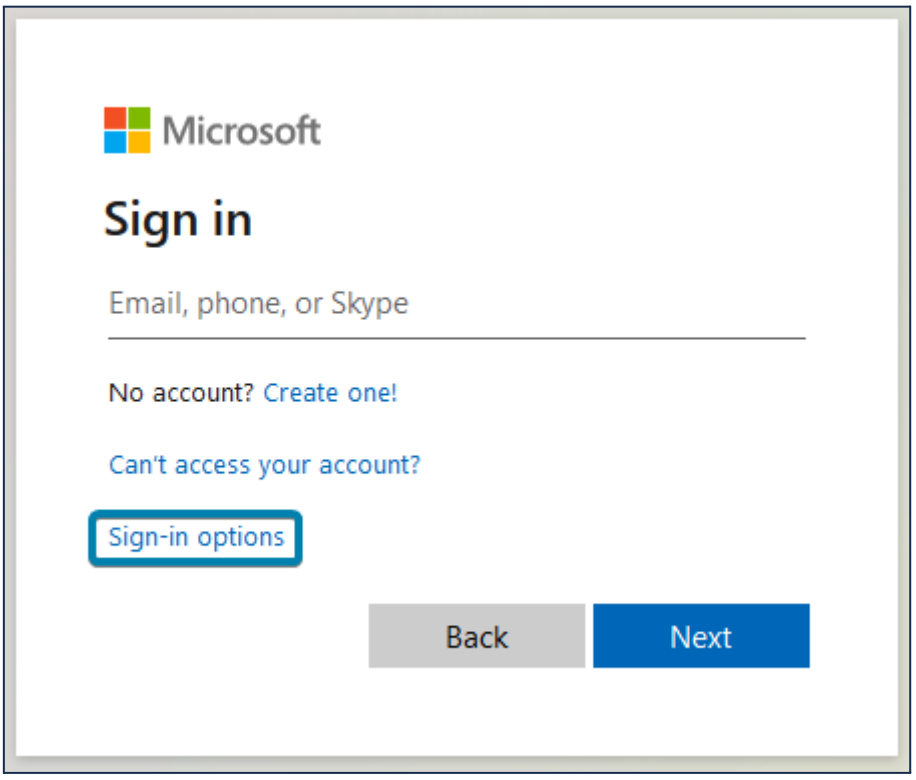


4. Select **Sign in with Windows Hello or a security key.**

© Yubico 2023.

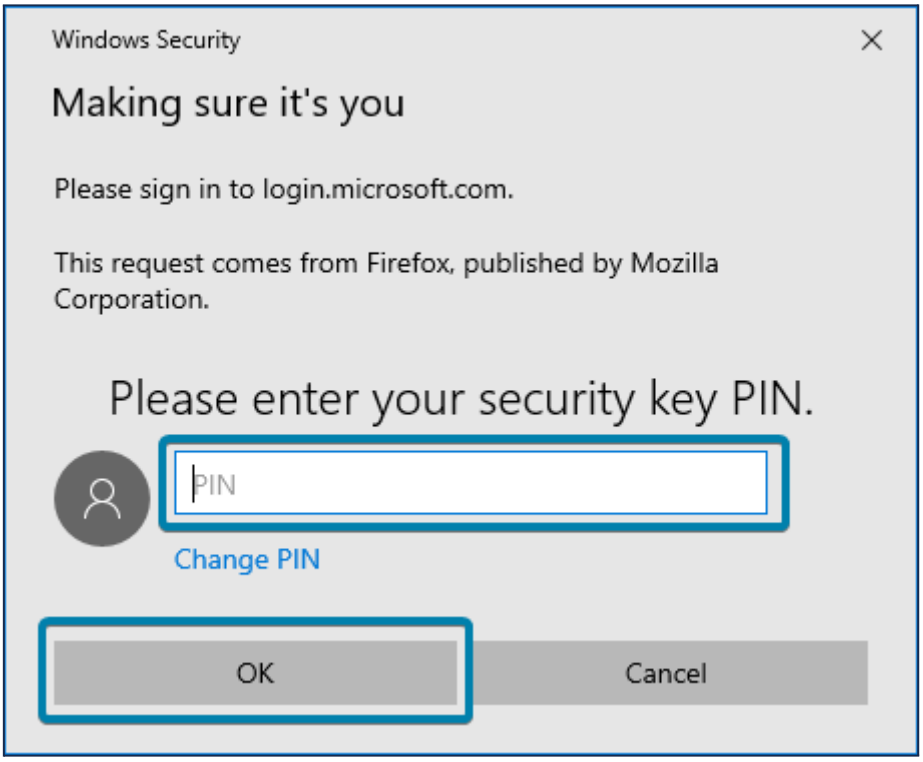


5. If you selected Use another account in the previous step select Sign-in options.



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.

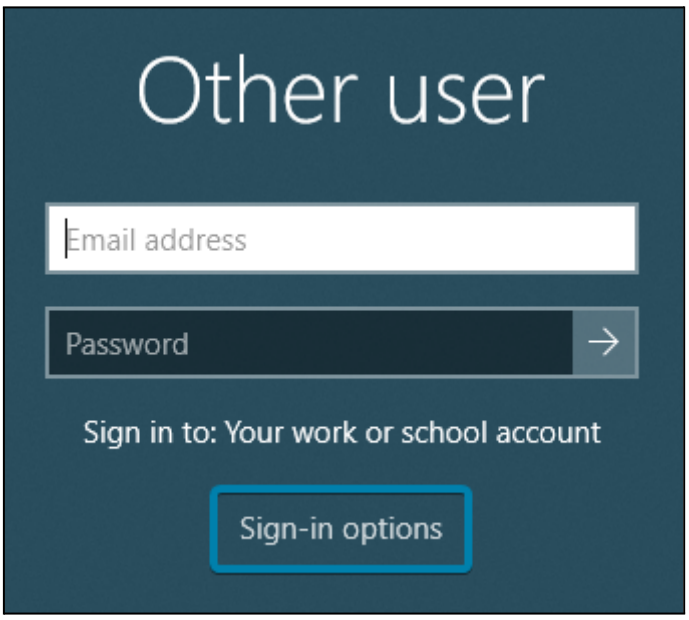
© Yubico 2023.



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

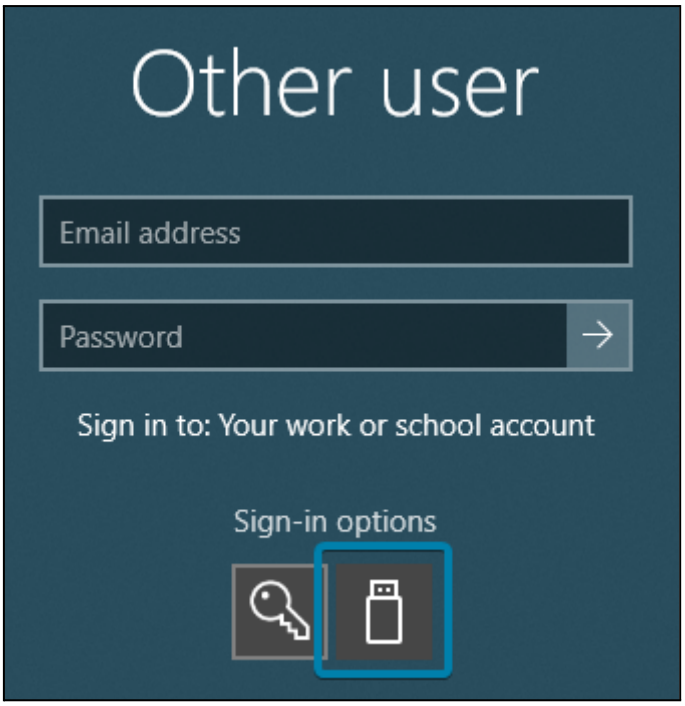
Sign into Windows 10 with a YubiKey

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

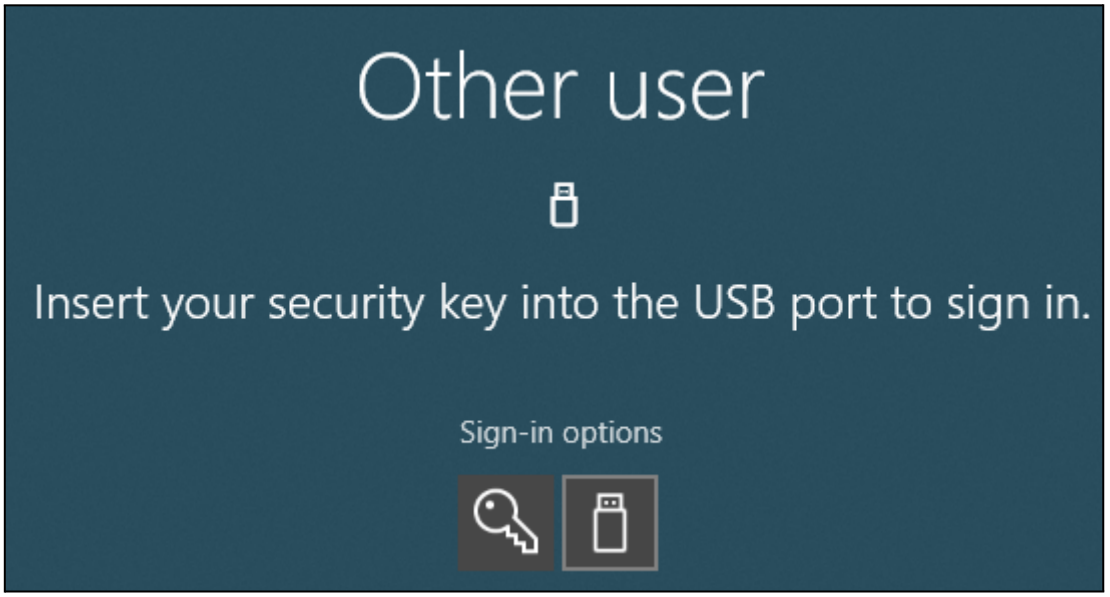


2. Select the security key icon.

© Yubico 2023.



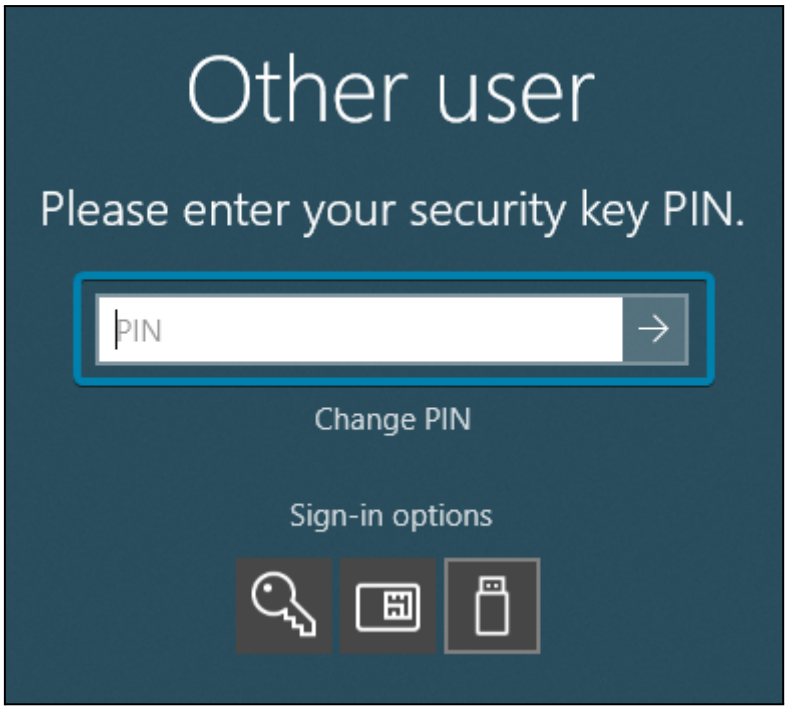
3. Insert your YubiKey into a USB port or place on a NFC reader.



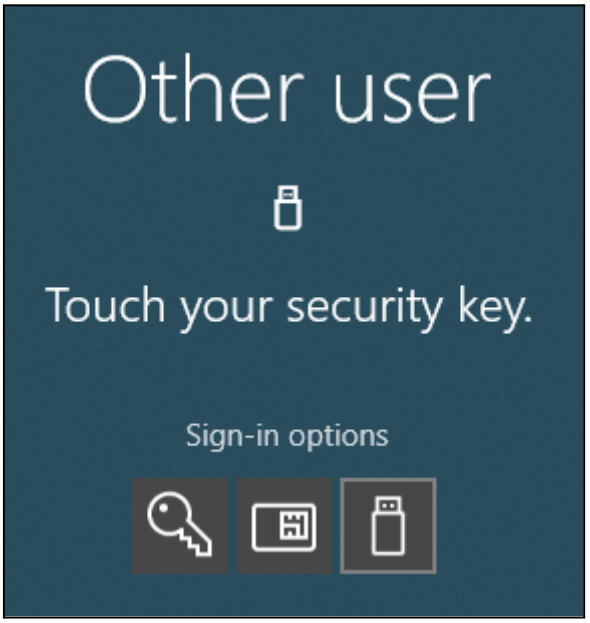
4. Enter the PIN code for this YubiKey then press enter.

   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.

© Yubico 2023.



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.

© Yubico 2023.

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 https://portal.office.com.

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

YubiKey Lifecycle Management

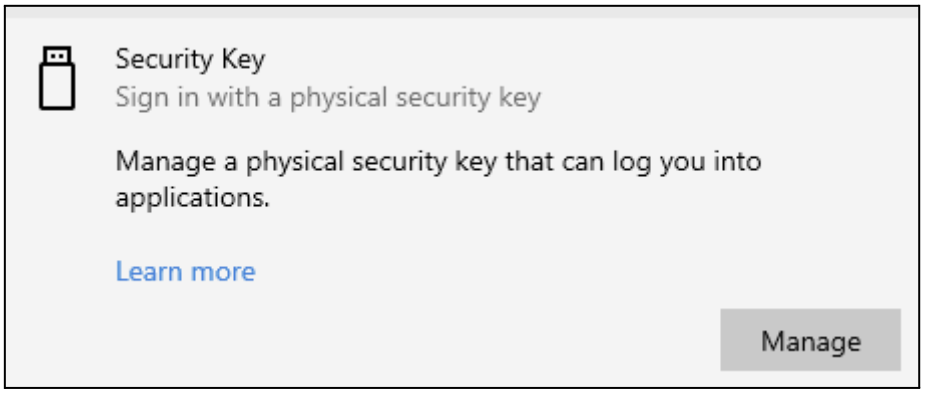
This section outlines some additional considerations when managing YubiKeys, to include removal of YubiKeys from a user account, changing the PIN, or resetting the YubiKey. The end user has the option to use the following tools:

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: https://support.yubico.com/hc/en-us/articles/360016614940

Change YubiKey PIN

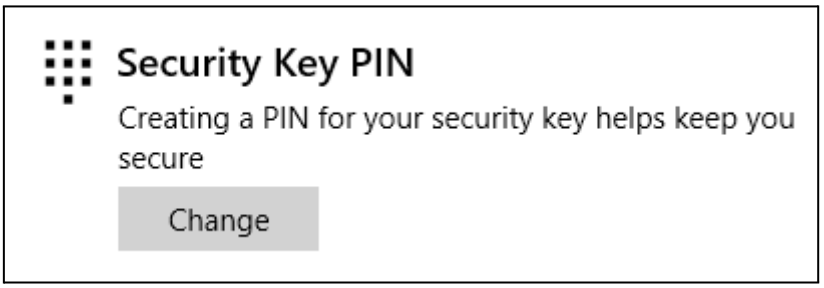
Using native Windows 10 tools

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

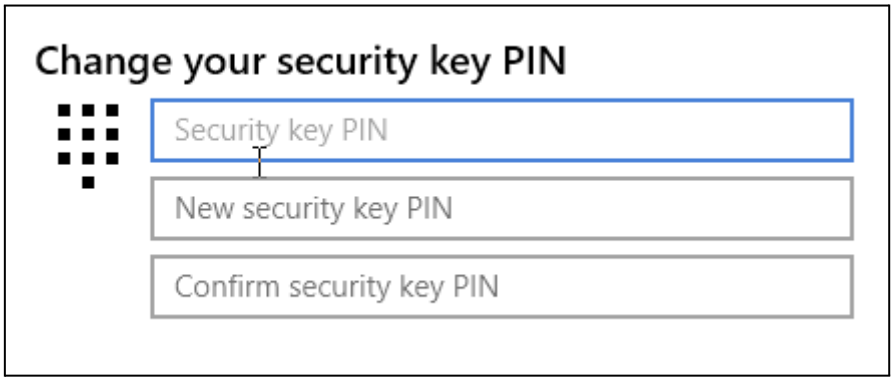


© Yubico 2023.

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



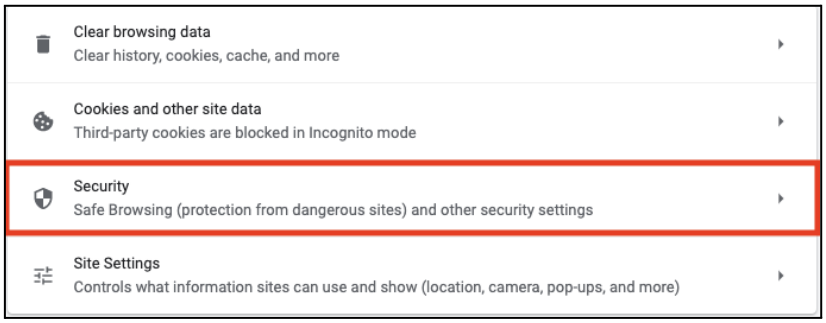
6. In the **Change your security key PIN** window, provide the current PIN, the new PIN, and confirm the new PIN again. Click **OK**.



7. The PIN is now changed.

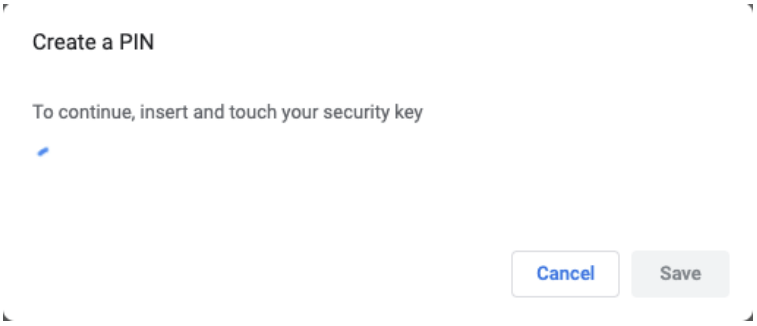
Using Google Chrome (macOS only)

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

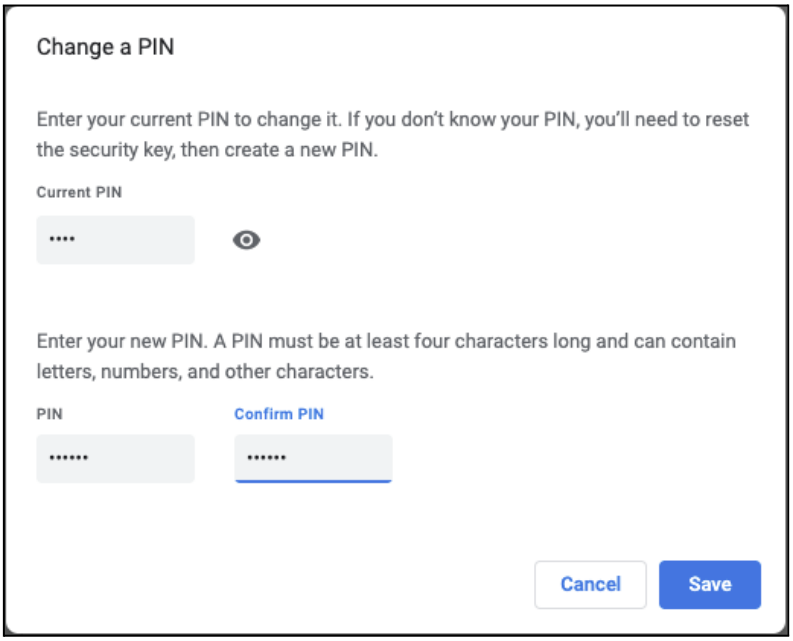


    c. Under **Advanced,** click **Manage security keys**.
10. Click **Create a PIN**.
11. When prompted, insert the YubiKey and tap it.

© Yubico 2023.



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

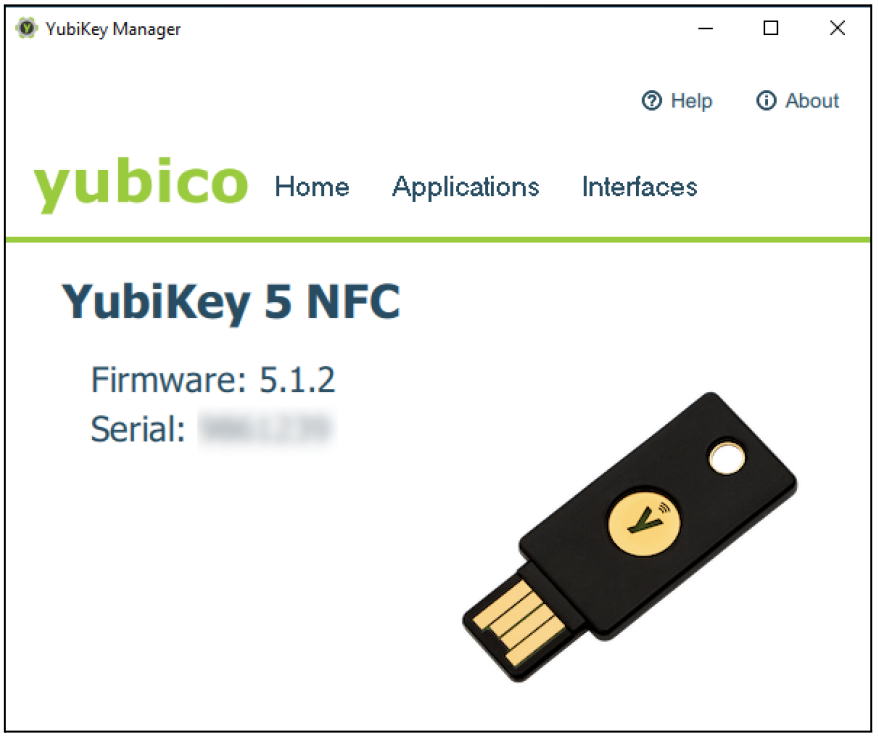


13. If successful, Chrome will indicate the PIN was created.

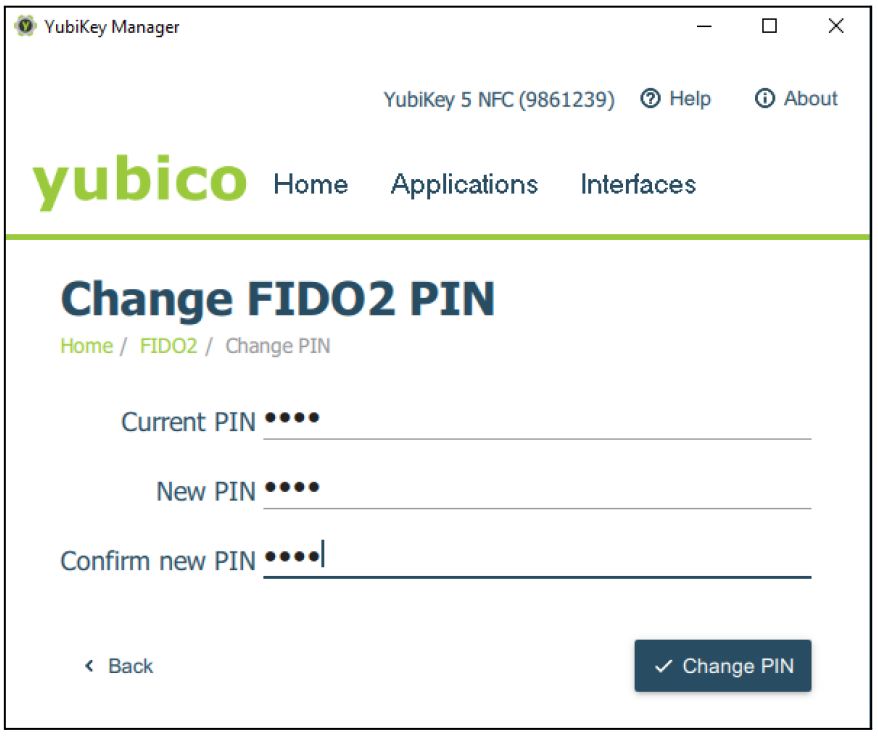
Using YubiKey Manager

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

© Yubico 2023.



2. Navigate to **Applications** → **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**.



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

© Yubico 2023.

Reset the YubiKey

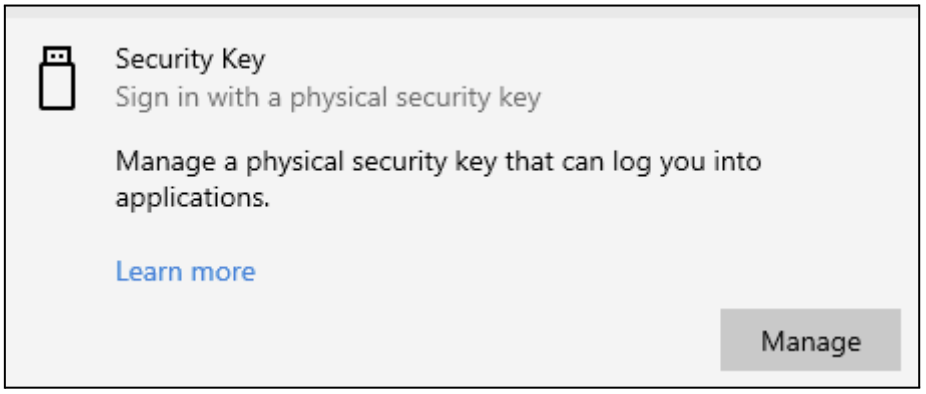
Using native Windows 10 tools (*Spring 2020 version and up)

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.

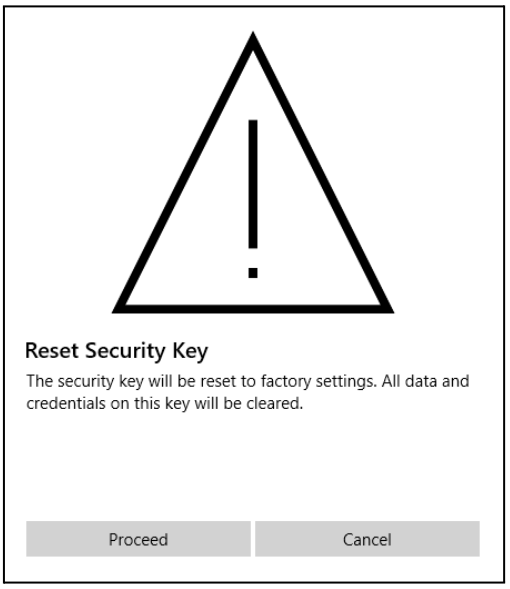
1. Navigate to **Settings > Accounts > Sign-in options**.
2. Click **Security Key**. Once expanded, click **Manage**.



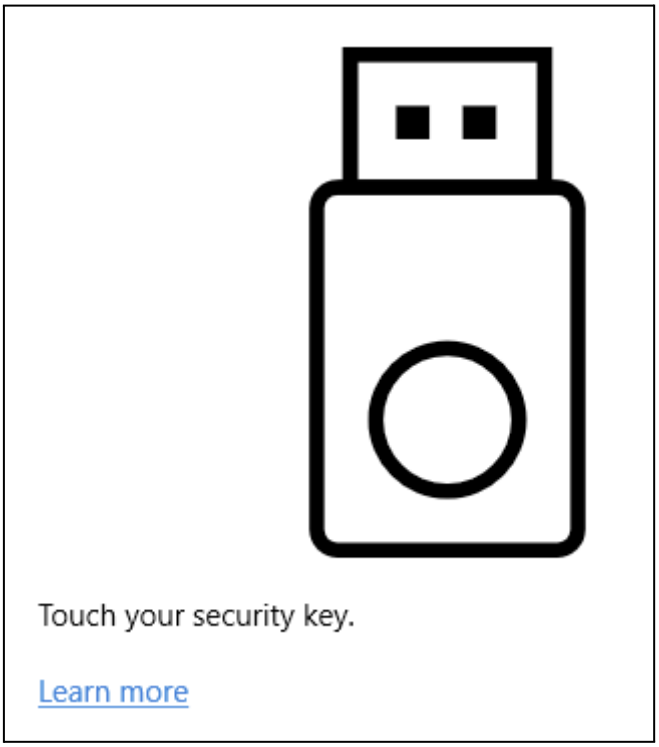
3. When prompted, touch the YubiKey and enter in the PIN.
4. Select **Reset** to reset the security key.

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

© Yubico 2023.



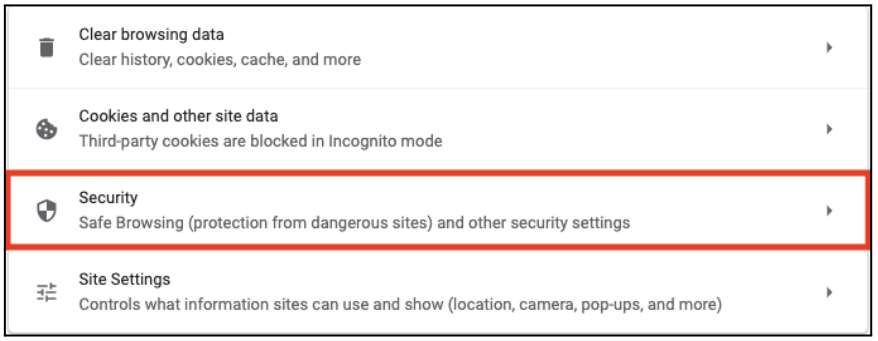
6. When prompted, touch the YubiKey. The YubiKey is now reset.



Using Google Chrome (macOS only)

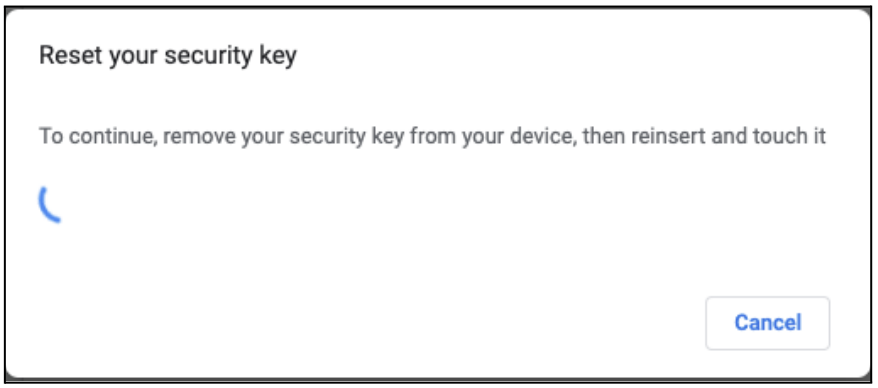
1. Open Google Chrome.
2. Navigate to “chrome://settings/securityKeys” in address bar or use the menu as described below:
    a. **Menu (** ⋮ **)** → **Settings**.
    b. From the left menu, select “**Privacy and security.**” Under the **Privacy and security** menu, click **Security.**

© Yubico 2023.

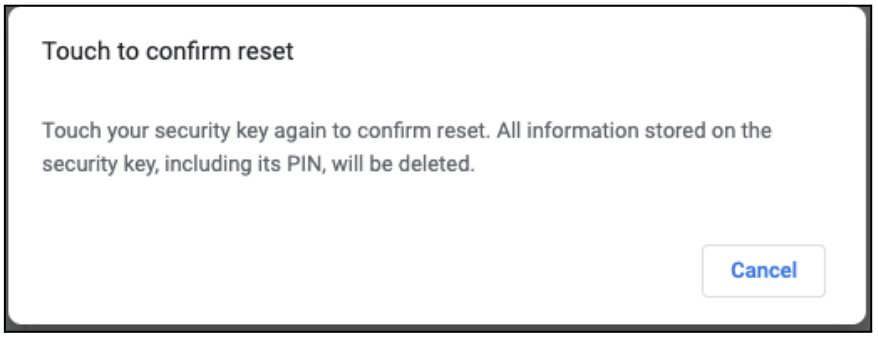


c. Under **Advanced,** click **Manage security keys**.

3. Click **Reset your security key**.
4. When prompted, remove the YubiKey from the device, reinsert the YubiKey and touch it.



5. Touch the YubiKey again to confirm reset.

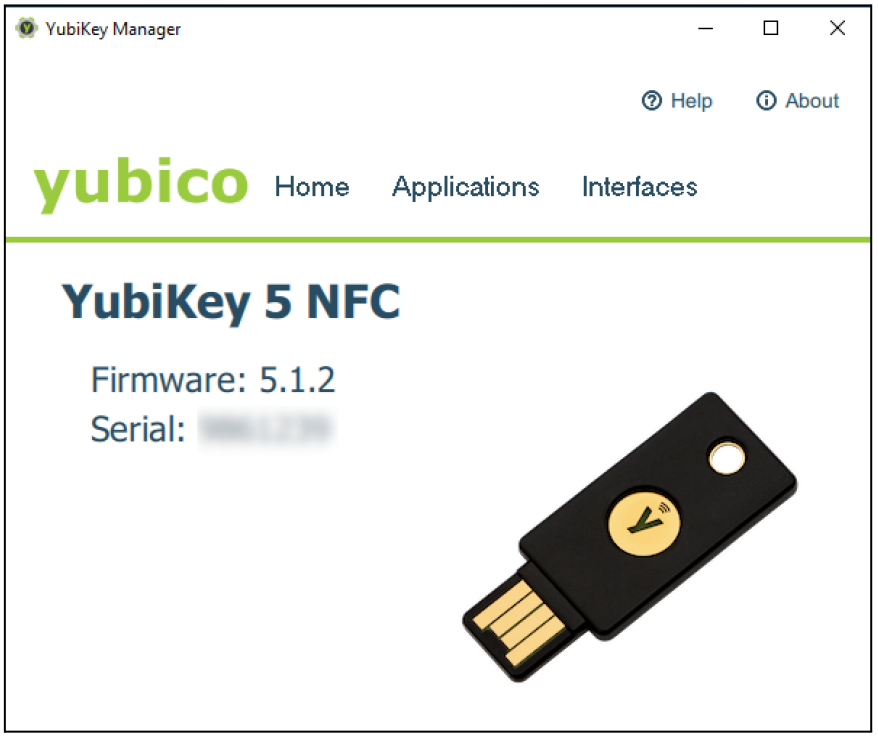


6. Chrome will display “Your security key has been reset” when completed.

© Yubico 2023.

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.

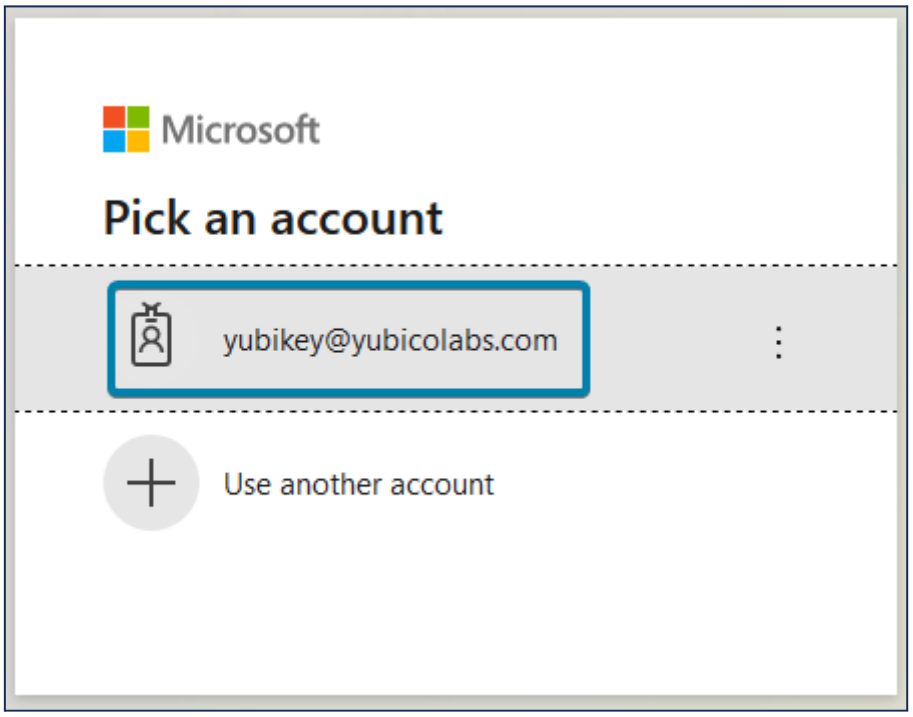


2. Navigate to **Applications** → **FIDO2**.
3. Select **Reset FIDO**.
4. When prompted to confirm, read the warning and click **Yes**. *Note: This will delete all FIDO2 credentials.*
5. Remove and re-insert the YubiKey.
6. When prompted, touch the YubiKey.

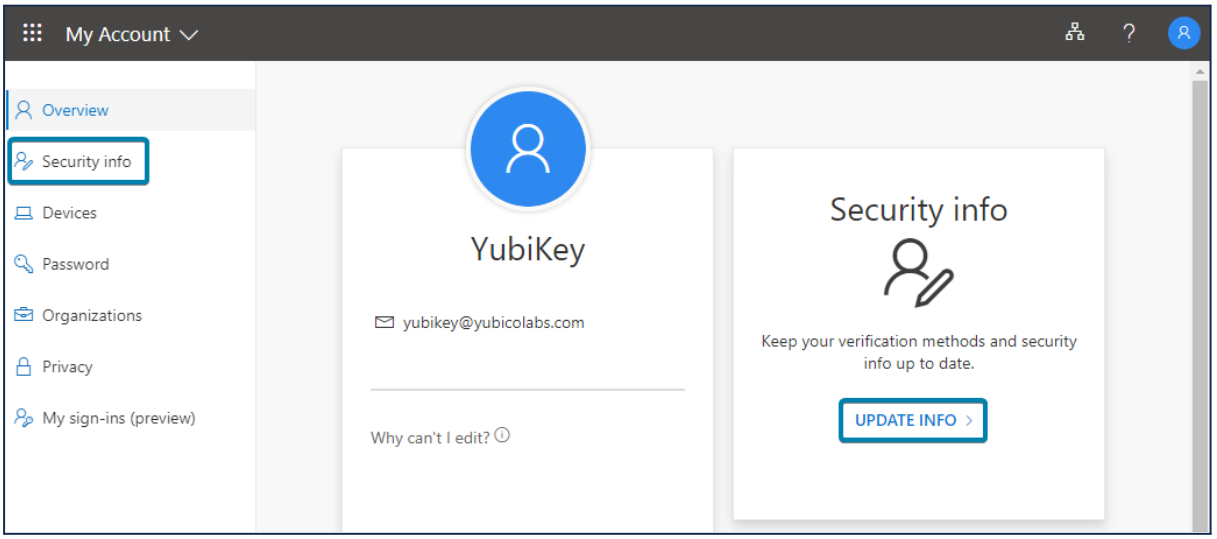
Removing a YubiKey as a security method

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.

© Yubico 2023.

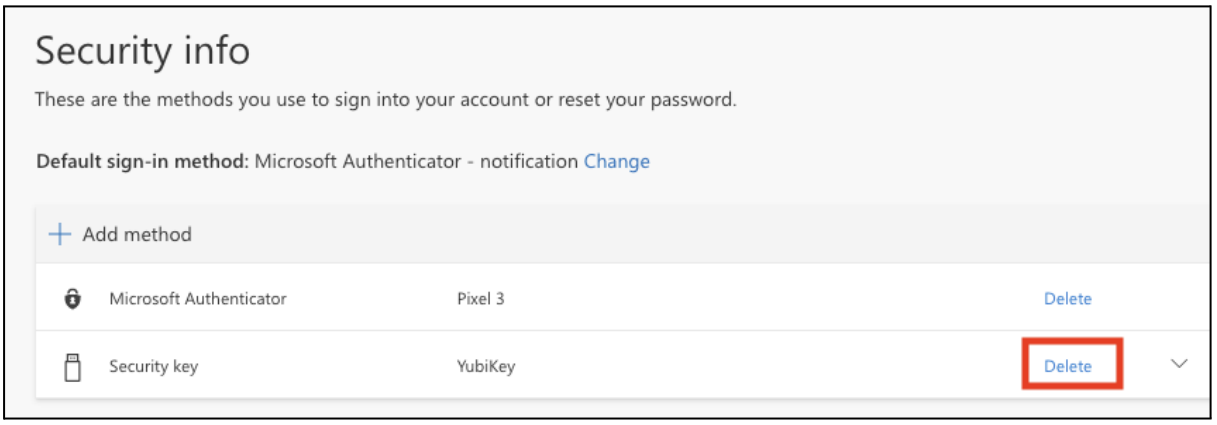


4. Enter your password and conduct your multi-factor authentication steps if prompted. You may need to select your account to proceed.
5. Select **Security Info** in the left navigation or **Update Info** in the Security Info tile.

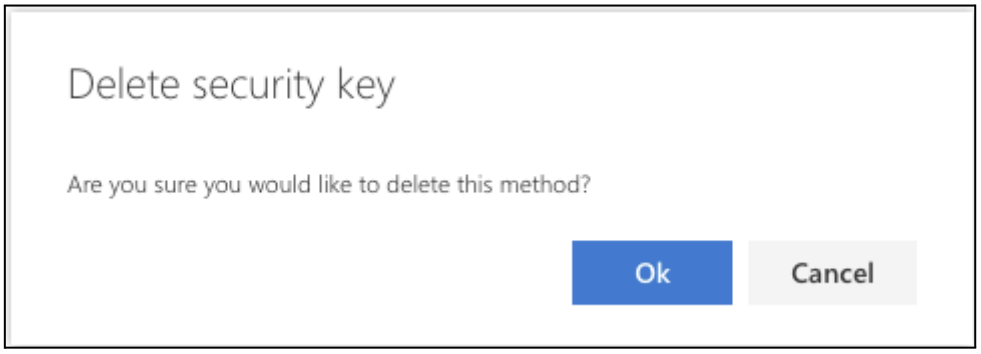


6. You may have to select your account and authenticate again to proceed to update the security information for your account.
7. Identify the Security Key you would like to remove and click **Delete**.

© Yubico 2023.



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



The YubiKey is now de-registered from the account.

RDP?

Call out mobile FIDO limitation

References

Yubico and partner references that support this document.

- Operating system and web browser support for FIDO2 and U2F for latest platform support for FIDO2. Passwordless requires user verification and resident key support.

© Yubico 2023.