

Passkeys

Passkeys are alternatives to passwords and use [public-key cryptography](#). Passkeys were developed by the Fast Identity Online (FIDO) Alliance.

Passkeys differ from passwords because the identifying information is stored on your device (or in a password manager) and passes between your device and the website without you having to enter a username or password. Passkeys can be stored on your phone, your computer, or a security key. Passkey prompts can be biometric scans or on-screen prompts.

What makes passkeys more secure than passwords is that they **ONLY** interact with the registered site.

In a phishing attack, you are directed to a fake website that looks like a real site, and you manually enter your username and password (thus giving that information to the hacker). With a passkey, your device will only talk to the “correct” website. This means you cannot accidentally give away your login credentials.

Additionally, each domain and account has a unique passkey, so even if a passkey *could* be stolen, the credentials would be useless on other sites.

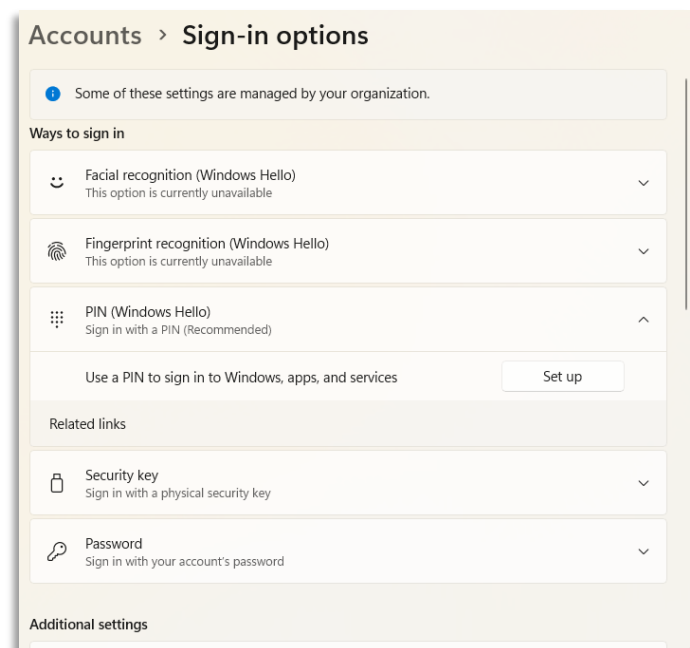
Windows 11

Windows Hello

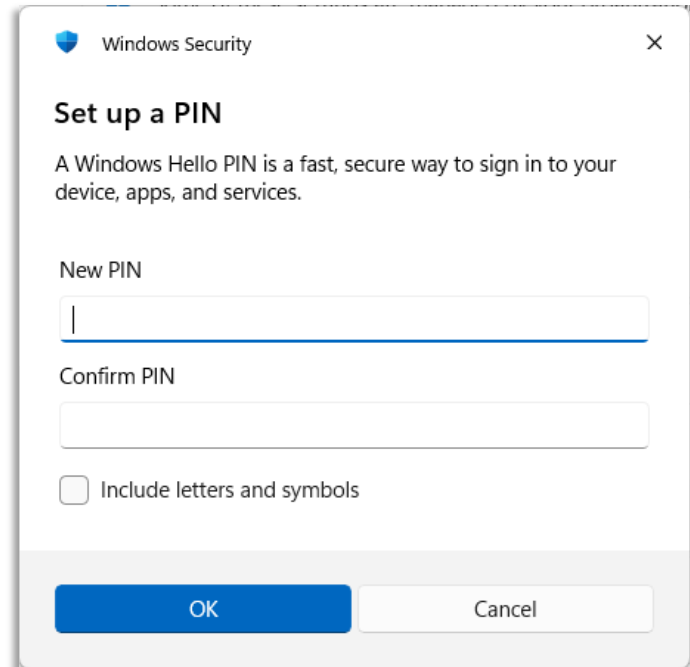
Windows Hello is a security option that allows you to use biometrics or a PIN for logins and is required to use Passkeys.

Setting Up Windows Hello

1. Open Windows Settings, go to **Accounts** and then **Sign-in Options**.
2. Select **PIN**. If you do not already have a PIN, click **Set Up**.



3. Create a PIN. By default it will be numbers only, however you can choose to include letters and symbols.
4. Reenter your PIN.
5. Click **OK**.

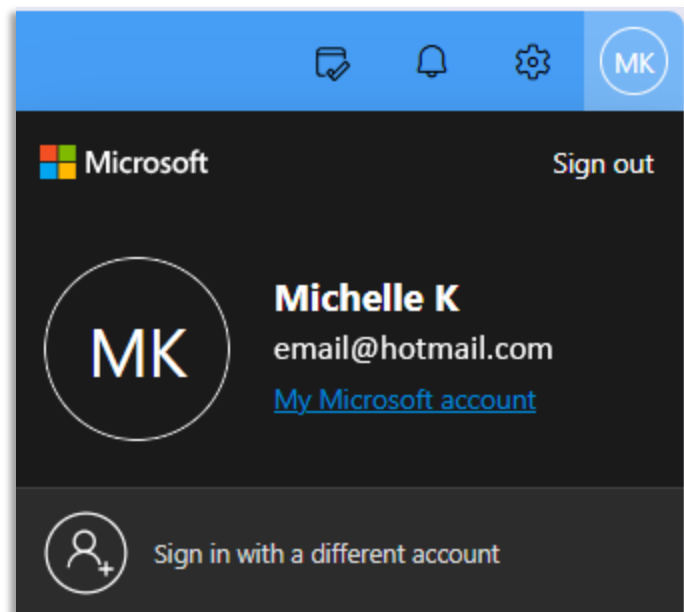


Creating Passkeys

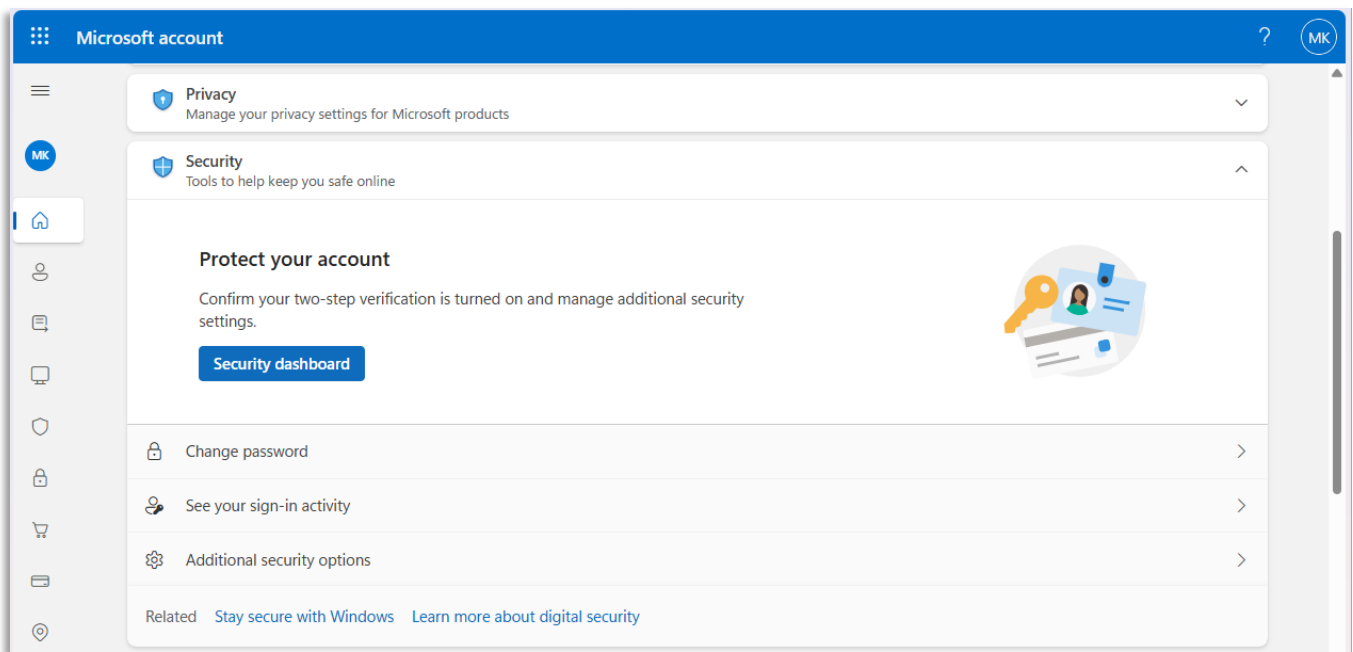
Once you have Windows Hello set up, you can create passkeys for [any account that allows it](#).

Adding a Passkey to a Microsoft Email Account

1. Login to your [Microsoft email](#).
2. In the top right corner of the window, click your initials.
3. From the drop down menu select **My Microsoft account**.

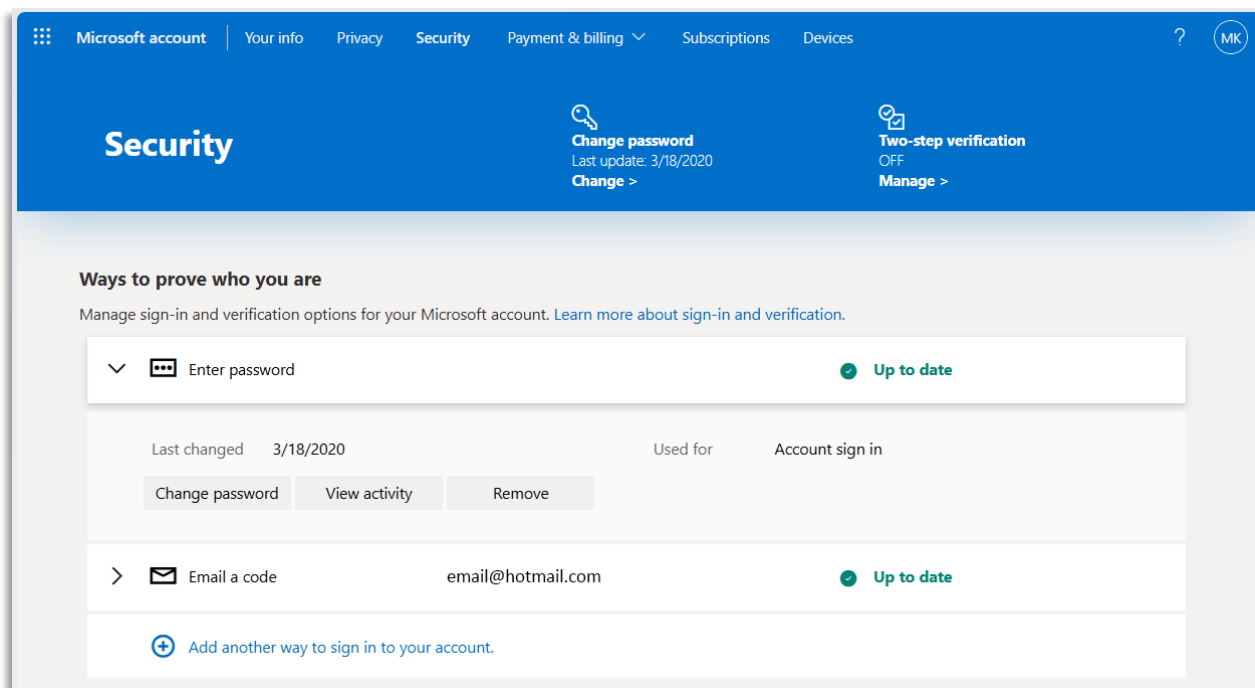


4. Scroll until you find **Security**.

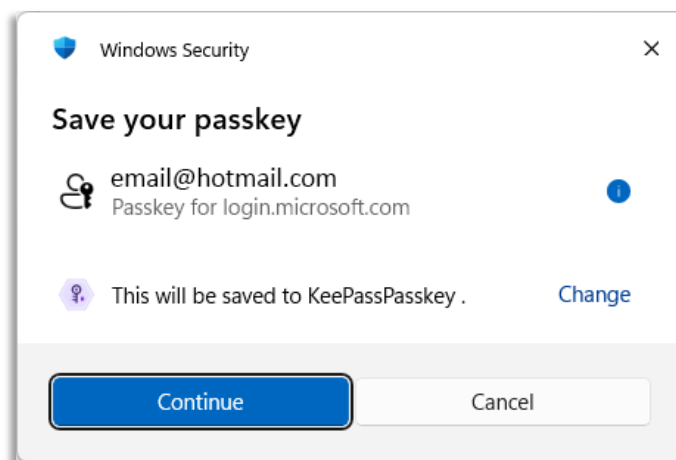


5. **Click** Security dashboard.

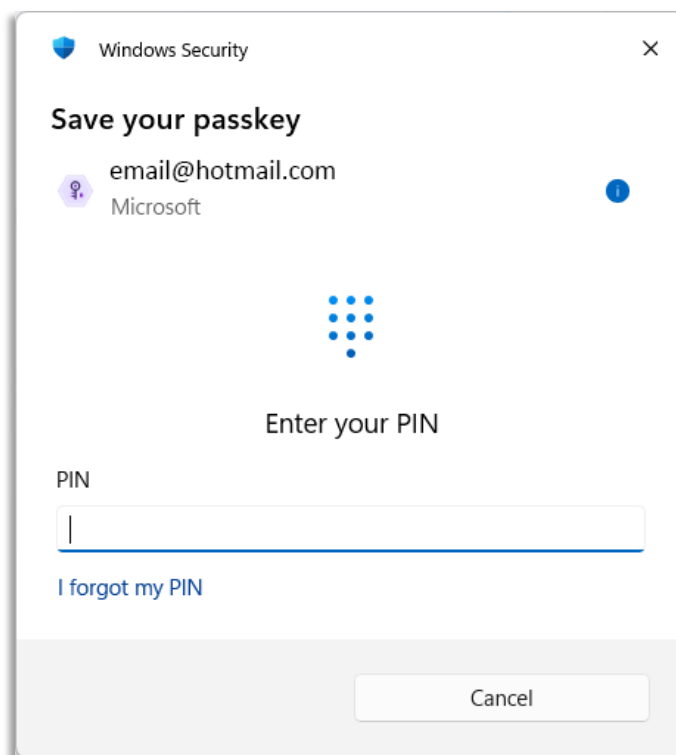
6. Look for **Ways to prove who you are** and click **Add another way to sign in to your account**.



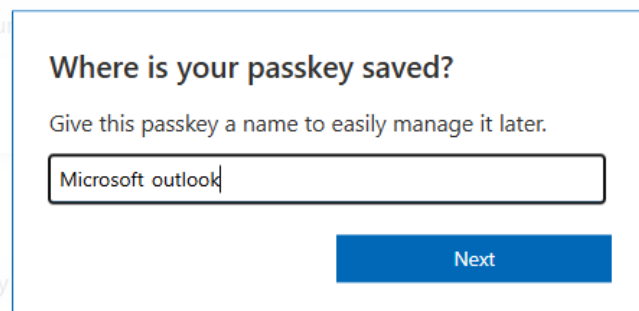
7. In the dialog box that opens, click **Face, fingerprint, PIN, or security key**.
8. You are prompted to save your passkey.
Click **Continue**.



9. Enter your PIN.

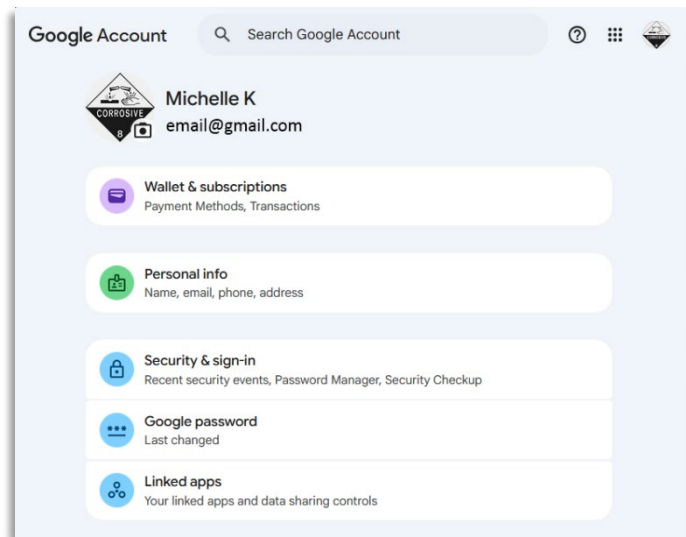


10. Create a name for your passkey,
11. Click **Next**.

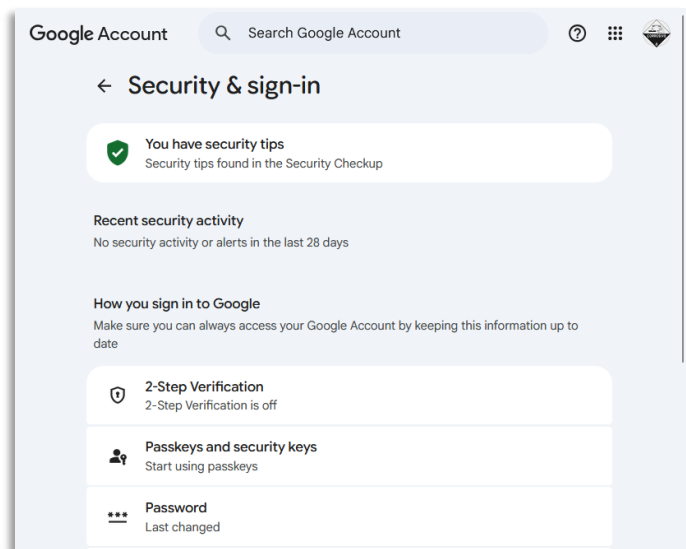


Adding a Passkey to a Gmail Account

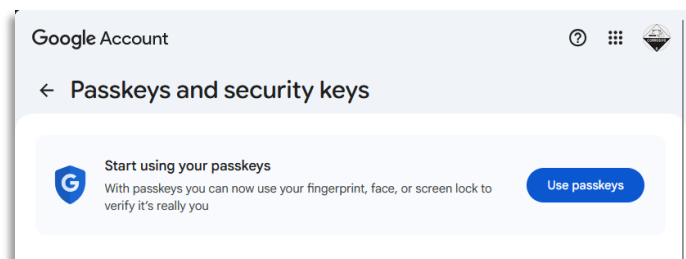
1. Login to your [gmail account](#).
2. Open your account settings. In the top right corner of the window, click your avatar and select **Manage your Google account**.
3. Click **Security and sign in**.



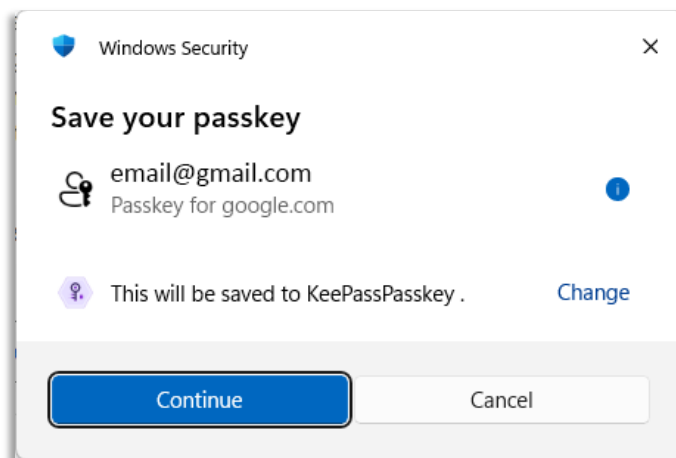
4. In the How you sign in to Google section, click **Passkeys and security keys**.



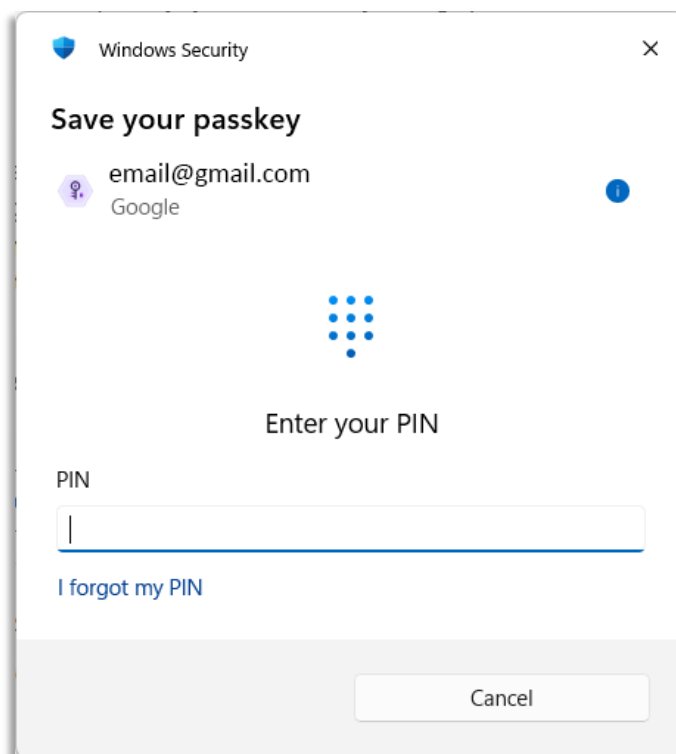
5. Verify your credentials.
6. Click **Use passkeys**.



7. Click **Continue**.

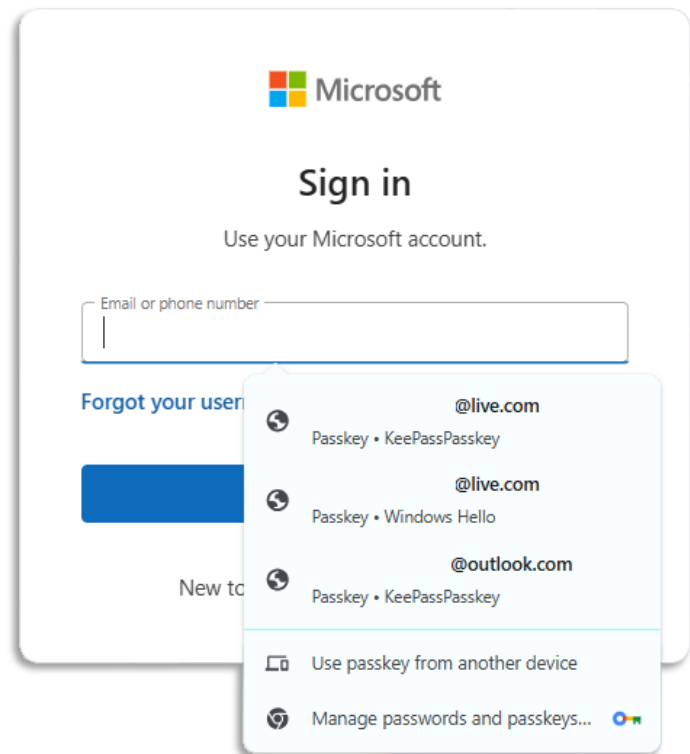


8. Enter your PIN to confirm the creation of the passkey.

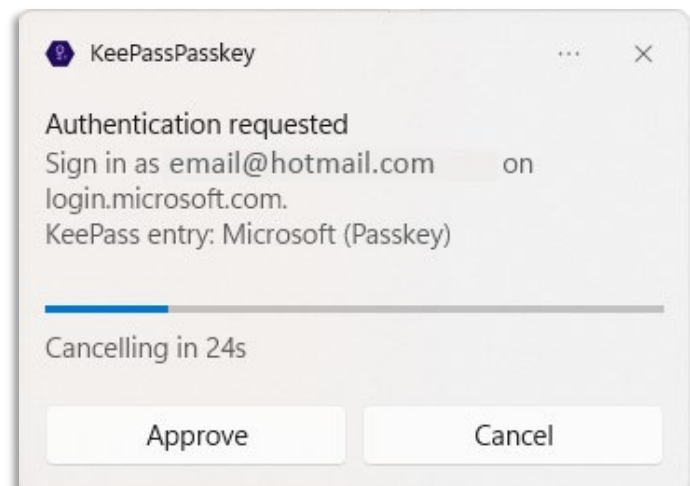


Using Passkeys

1. Go to the website you want to log into.
2. Click where you would enter your username, and then select the correct account.



3. If prompted, enter your PIN.
4. A window appears in the lower right corner of your window. Click **Approve**.



Resources

[Passkeys.directory](#)

[Microsoft email](#)

[Google email](#)

[Fast Identity Online \(FIDO\) Alliance](#)

[Passkeys: Passwordless logins for beginners](#) (Freedom of the Press Foundation 2023)

[Still Using Passwords? It's Time to Upgrade to Passkeys Now](#) (PC Mag 2026)