AI Mode All Images Videos News More

When I setup a passkey, it wants my PIN. I use the same PIN I use when I turn on my computer with my Microsoft account. ...

27 September 2026

Microsoft Support
Create and save a passkey | Microsoft Support
Security key: The passkey is saved to a physical security key. Windows device /...

Microsoft Support
What are passkeys and why they matter
If the website or app you're using supports passkeys, you can sign in: fingerprint, or face. * On your phone, using...

Microsoft Support
Troubleshoot signing in with a passkey
If Bluetooth hangs during registration (especially with USB security keys), cancelling and refreshing the sign-in pag...

Show all

If you do not use a Microsoft account and log into Windows with a blank local account (no password or PIN), **Windows Hello cannot save a passkey directly to your computer.** Microsoft Support

Passkeys rely on local encryption. Windows requires a device PIN or biometric lock (like a fingerprint or face scan) to create the secure "vault" that protects that passkey. Microsoft Support +3

However, you can still absolutely use passkeys! You will just need to store them slightly differently. If you try to set up a passkey on a completely unsecured Windows account, you have three primary alternatives:

1. Use your Mobile Phone

When a website asks you to create a passkey, Windows will show a pop-up window. Microsoft Support

- Instead of trying to use your PC, select **"iPhone, iPad, or Android device"** (or "Use a different device").
- Windows will display a **QR code** on your screen.
- Scan it with your phone's camera, and your phone will save the passkey securely.
- When you log in next time, you will just scan a quick QR code and unlock it with your phone's fingerprint or Face ID. Microsoft Support +1

2. Use a Cloud Password Manager (with Passkey Support)

You can use a browser extension or dedicated password manager like **Bitwarden**, **1Password**, or **Google Password Manager** (built into Chrome). Microsoft Support +1

- These third-party tools will intercept the passkey request and save it inside their own secure vaults rather than using Windows Hello.
- You will only need to remember the master password or PIN for that specific manager app, leaving your Windows computer completely free of a login screen. Microsoft Support

3. Use a Hardware Security Key

You can purchase a physical USB security key (such as a **YubiKey**). Microsoft Support +1

- When creating a passkey, select **"Security Key"**.
- Plug the USB key into your computer and touch it when prompted.
- The key will hold the passkey, and you will set up a unique PIN specifically for that USB stick, completely separate from your computer login. Microsoft Support +1

Are you setting up a passkey for a **specific website or app**, or are you trying to use a passkey to **log into Windows itself**? I can give you exact steps depending on what you're trying to access.

Does that apply to all passkeys or for only Microsoft accounts?

27 September 2026

This requirement **applies to all passkeys, regardless of the account or website** you are using (like Google, Amazon, or your banking app).

The prompt for a PIN is not coming from the website itself or from Microsoft—it is coming directly from **Windows Hello**, your computer's built-in security vault.

Here is exactly why this happens for any website:

The "Lock" Requires a Key

A passkey consists of two halves: a public key that stays with the website, and a **private key** that is generated and hidden inside your computer's security hardware.

- To prevent just anyone from walking up to your computer and using your private keys, Windows encrypts them.
- Windows uses your **Windows Hello PIN or password** as the master key to unlock that vault.
- If your Windows account has no password or PIN, Windows has no way to securely lock the vault, so it refuses to store the passkey locally.

Your Options Remain the Same

Even if you are setting up a passkey for a completely non-Microsoft website (like Netflix or GitHub), Windows will still block local storage if you don't have a PIN. You will still need to use one of the workarounds mentioned before:

- **Your Phone:** Save the passkey to your iPhone or Android via a QR code.
- **A Browser Extension:** Save it to Google Password Manager, Bitwarden, or 1Password.
- **A Hardware Key:** Save it to a physical USB security key.

Would you like help setting up a **third-party password manager** or using your **phone** so you can start using passkeys without adding a PIN to your computer?

I have a local account but it does have a password and now with the latest windows 11 update I can set a pin. Will this wo...

9:58 am

Reddit
Using Windows Hello with local account (for authenticating ...
Windows Hello with a PIN, to be able to use FIDO2 passkeys to authenticate to website...

Reddit
Passkey confusion at my work. Can anyone help clarify?
Using Windows Hello requires the user to create a PIN (or use faceID or physical...

Microsoft Learn
How can I set up a Windows Hello PIN but disallow its usage on the ...
Windows Hello PIN does not work as an "app-only" PIN. passkeys also rely on Windows Hello, including PIN or...

Show all

Yes, this will work perfectly with passkeys!

Setting up a PIN on your local Windows account activates **Windows Hello**, creating the secure, encrypted local vault required to store your passkeys locally. You can now save passkeys directly to your computer for any website (Google, Amazon, etc.) using your local PIN to authenticate. Reddit +1

What to expect at your Windows Login Screen

Once you set up a PIN for your local account, Windows will automatically default to asking for your PIN instead of your password when you turn on your computer.

If you prefer to keep typing your full password to log into your computer, you can still switch back at the login screen:

1. Click on **Sign-in options** (usually a key or grid icon under the PIN box).
2. Select the **Password** icon.
3. Log in with your standard local password. Microsoft Learn +1

Windows will remember your preference, but your PIN will remain active in the background ready to instantly authorize your passkeys whenever you browse the web. Microsoft Learn

Would you like the quick navigation steps to **set up your local PIN** in your Windows settings, or are you ready to start **creating your first passkey** on a website?

I set up my local account with a password and pin. It is easy in Windows 11 25h2. New question about passkeys. What ...

Linux Mint
Passkeys in Linux Mint.
When troubles occur, it's usually the browser's fault ... other browsers (ex: Vivaldi) worked right out of the box....

TuxCare
Passkeys on Linux: Breaking Free from Platform Lock-in
The Linux ecosystem offers a unique opportunity to implement passkeys without...

Reddit
Is it a good idea for Linux users to use "passkeys"? - Reddit
Linux doesn't support storing passkeys on the device ... choices are password...

Show all

On **Linux Mint, you cannot store passkeys directly in the operating system** using your system login password. Reddit +1

Unlike Windows 11 (which uses Windows Hello to handle local encryption via a PIN), Linux Mint lacks a built-in, platform-level system to natively create and save passkeys to your local hard drive or TPM chip. Reddit +2

If you want to use passkeys on Linux Mint, your operating system password won't be involved at all. Instead, you have two excellent, highly secure alternatives:

1. Use a Browser Extension (The Easiest Route)

You can rely on a third-party password manager extension inside your web browser (like Chrome, Brave, or Vivaldi). Bitdefender +1

- Apps like Bitwarden or **1Password** handle passkeys perfectly on Linux.
- When a website asks to create a passkey, the browser extension intercepts the request and securely saves the key inside its own vault.
- To unlock your passkeys, you just type the **Master Password** you created for that specific password manager. Reddit +1

2. Use a Physical Hardware Key

You can use a physical USB security key, such as a **YubiKey**. Reddit +1

- When creating a passkey, you plug the key into your USB port and touch the metal sensor.
- The private key is generated and stored directly on the physical USB device itself.
- You will protect the hardware key with a unique PIN that you set up through the manager tool (like the Yubico Authenticator), completely independent of Linux Mint. TuxCare +3

(Note: If you use Firefox on Linux Mint, be aware that its native password manager doesn't support storing passkeys out-of-the-box, so you will definitely want to use an extension like Bitwarden or Chrome instead.) Lawrence Berkeley Nati... +1

Are you currently using a password manager like **Bitwarden** on your Linux Mint machine, or would you like to know how to set one up to handle your passkeys?

I am pepraing a lesson plan to teach my students the different options with passkeys. All the information you ...

That sounds like a fantastic and timely lesson plan! Passkeys are the future of authentication, and teaching students how they behave across different environments (Windows vs. Linux, local vs. cloud) is incredibly valuable.

To help you structure this for your students, here is a quick summary table you can use in your slides or handouts to compare how the two operating systems handle passkeys out of the box:

OS Comparison: Local Passkey Support

Feature	Windows 11 (24H2/25H2)	Linux Mint (Cinnamon/MATE)
Native Storage	**Supported** (via Windows Hello)	**Not Supported** natively
Required Local Lock	Windows Hello PIN or Biometrics	Linux Login Password (not compatible)
Hardware Tie-in	Uses the motherboard's TPM chip	Requires external USB key (e.g., YubiKey)
Browser Options	Chrome, Edge, Firefox, Third-party apps	Chrome/Chromium extensions, Third-party apps

Key Concepts for Your Students

When putting your lesson together, these are three great "takeaway" concepts for the class:

- **The "Vault" Analogy:** Explain that passkeys always need a secure vault. Windows builds that vault into the OS using the TPM chip and locks it with a PIN. Linux Mint doesn't build that vault into the OS natively, so it relies on "portable vaults" like browser extensions or USB keys.
- **Cross-Platform Freedom:** Highlight that even though Linux doesn't store them natively, a student can create a passkey on Windows using a cross-platform manager (like Bitwarden) and use that exact same passkey seamlessly on Linux Mint.
- **PIN vs. Password:** Make sure to note that a Windows Hello PIN isn't "weaker" than a password just because it's shorter—it only works on that *specific* physical device, which is why it is safe for unlocking passkeys.

Would you like me to help you draft a **quick quiz** or some **troubleshooting scenarios** (e.g., "What should John do if he loses his phone?") to test your students' understanding at the end of the lesson?

Ready to create a study guide?
Use Canvas to save, edit, and share your guide
Get started

Ok that takes care of Windows and Linux. What about Apple Macbook?

Apple MacBooks handle passkeys natively and seamlessly, making them one of the easiest platforms for students to learn.

Much like Windows 11 uses Windows Hello, macOS uses Apple's built-in security infrastructure—**iCloud Keychain** and **Touch ID**—to create and manage passkeys.

Here is exactly how it works on a MacBook and how it fits into your lesson plan:

1. The Local "Lock": Touch ID or User Password

To create or use a passkey on a MacBook, the OS requires local user authentication to unlock its secure vault (the Secure Enclave processor inside the Mac).

- Students will simply place their finger on the **Touch ID** sensor.
- If the MacBook doesn't have Touch ID (or the lid is closed in clamshell mode), they will type their standard **Mac login password**.

2. Built-in Cloud Syncing (iCloud Keychain)

This is a vital distinction for your students compared to Windows local accounts:

- By default, when a passkey is created on a Mac, it is saved to **iCloud Keychain**.
- This means the passkey is automatically and securely synced across all of that user's Apple devices (iPhone, iPad, other Macs) signed into the same Apple Account.
- *Note:* If a student chooses not to use an Apple Account, the passkey stays locked strictly to that single MacBook.

3. Browser Support

- **Safari:** Fully supports native passkey creation and autofill using Touch ID.
- **Chrome / Edge / Firefox:** Third-party browsers on macOS can also hook directly into the macOS system to use Apple's native passkeys, or users can opt to use extensions like Bitwarden.

Updated Lesson Plan Reference Table

You can add this third column to your teaching materials to give students a complete overview of the "Big Three" desktop platforms:

Feature	Windows 11 (Local Account)	Linux Mint	Apple MacBook
Native Storage	**Supported** (Windows Hello)	**Not Supported** natively	**Supported** (iCloud Keychain / Secure Enclave)
Required Local Lock	Windows Hello PIN or Biometrics	Linux Login Password (not compatible)	**Touch ID** or **Mac Login Password**
Default Syncing	None (Stays on that PC)	None (Unless using a cloud extension)	**Automatic Sync** across Apple devices via iCloud
Hardware Tie-in	Motherboard TPM chip	Requires external USB key	Apple Silicon / T2 **Secure Enclave** chip

Now that you have the complete picture for **Windows, Linux, and Mac**, would you like to generate an **interactive quiz** to test your students on these platform differences, or should we move on to how **mobile devices (iOS and Android)** fit into the ecosystem?

Ask anything