

## Compare Windows Password manager to Google password manager

Here's a clear **side-by-side comparison of Windows Password Manager vs. Google Password Manager**, covering features, security, ecosystem support, and limitations.

### Core Purpose & Positioning

#### Windows Password Manager

- Built into **Windows 11 and Microsoft ecosystem** (specifically via Microsoft Edge's password/passwordless support like passkeys). TECHCOMMUNIT...
- Focus shifting from traditional passwords toward **passkeys and Windows Hello-protected credentials**. The Verge
- Works across devices where you're signed into **Microsoft Edge/Microsoft Account**, and syncs securely. TECHCOMMUNIT...

#### Google Password Manager

- Built into **Google Account / Chrome browser / Android / cross-platform wherever you sign in with your Google Account**. Several.com
- Focus is on **password storage and autofill**, with some modern security features like optional on-device encryption. Gizchina

### Key Feature Comparison

#### Password Storage & Access

Feature	Windows Password Manager	Google Password Manager
Save & autofill passwords	Yes (via Edge, and expanding) <small>TECHCOMMUNIT...</small>	Yes (Chrome + Android) <small>Several.com</small>
Sync across devices	Yes (Microsoft Account, Edge) <small>TECHCOMMUNIT...</small>	Yes (Google Account) <small>Several.com</small>

Feature	Windows Password Manager	Google Password Manager
Browser support	Edge (native) and other browsers via syncing features increasingly	Chrome (native), limited other browsers <a href="#">Several.com</a>
Passkey support	Native passkey support and passwordless login with Windows Hello <a href="#">TechRadar</a>	Supported via Chrome with future upgrades being added <a href="#">Tom's Guide</a>

👉 **Windows** is embracing the newer **passkey standard**, reducing reliance on passwords over time, while **Google** still centers around traditional password storage with passkey transition tools being tested. [TechRadar](#) +1

## 🔒 Security

### Windows

- Passkey operations are protected by **Windows Hello** (PIN, biometrics). [TECHCOMMUNIT...](#)
- Synced credentials are encrypted with cloud protections and a **Microsoft Password Manager PIN**. [TECHCOMMUNIT...](#)
- Password-less future focus reduces risk of reused or phished passwords. [The Verge](#)

### Google

- Passwords and credentials are encrypted in Google account storage; **optional end-to-end encryption** if enabled. [Several.com](#)
- Supports breach alerts and strong password generation. [Several.com](#)
- Does **not use zero-knowledge encryption by default**, meaning Google holds key access unless on-device encryption is manually activated. [Android Police](#)

💡 **Security nuance:** Google's system is convenient and secure for most typical users, but **advanced attackers or privacy-focused users may prefer services with zero-knowledge models** (not fully inherent in Google's system). [Acer Corner](#)

## 📱 Authentication & Integration

### Windows

- Deep integration with **Windows Hello** (biometric/PIN) for unlocking stored credentials. TECHCOMMUNIT...
- Works well especially if you use Edge and Windows ecosystems.

## Google

- Works across **Chrome and Android devices**, and increasingly integrates biometric unlock on desktops. Thurrott.c...
- Tightly linked to your **Google Account login** and 2FA status.

## Ecosystem & Compatibility

Aspect	Windows Password Manager	Google Password Manager
Best experience on	Windows + Edge	Chrome + Android + cross-devices
Works on other browsers	Partial or via sync	Mainly Chrome, less seamless on others <small>Several.com</small>
Mobile support	Via Microsoft Edge and some OS integrations	Android + iOS (Chrome/Google app) <small>Several.com</small>
Business/enterprise use	Better integrated with Microsoft 365 tools	Less centralized business control features <small>Cyber Ass...</small>

## Limitations & Notes

### Windows Password Manager

- Still evolving; Microsoft is pushing **passkeys (password-less)** and reducing reliance on traditional passwords. The Verge
- Some legacy password-manager features may be less full-featured than dedicated third-party solutions.

### Google Password Manager

- **Encryption not enabled by default**, and browsers can store data that's tied to your Google account (so if that account is compromised, credentials are exposed).

Android Police

- Limited advanced password-management features (no secure document storage, fine-grained sharing, or business compliance tools). Android Police
- Doesn't support zero-knowledge out-of-the-box like dedicated managers.

Acer Corner

---

☰ ChatGPT ▾  Free offer ×



---

### Choose Windows Password Manager if:

- You're deeply integrated into the **Microsoft/Windows ecosystem**.
- You value passkeys and biometric, password-less sign-in.
- You want Edge-centric autofill and sync.

### Choose Google Password Manager if:

- You use **Chrome and Google services across devices**.
- You want a simple, no-extra-app password store that syncs automatically.
- You're fine with basic password security and optional encryption settings.

---

### Extra Tip

Neither built-in system quite matches **full-featured dedicated password managers** (like 1Password or Bitwarden) in terms of **security auditing, zero-knowledge encryption, sharing, and organization tools** — but both are strong **free options for everyday users**. wired.com

---

If you'd like, I can also compare these with dedicated third-party managers like Bitwarden or 1Password for a broader perspective.

       Sources

