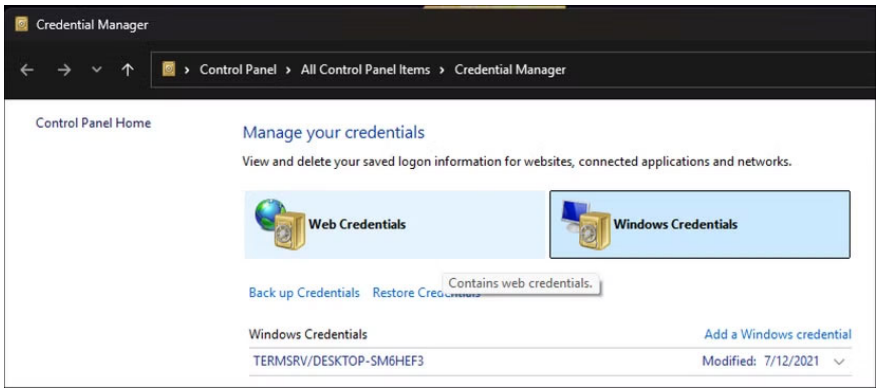
Why can't this built-in Credential Manager feature in Windows replace a password manager?

Windows has a built-in Credential Manager, but it's not what you think it is—and certainly not a replacement for a password manager.

Windows has a built-in Credential Manager, but it's not what you think it is—and certainly not a replacement for a password manager.

What does Windows Credential Manager actually do?

As the name suggests, Credential Manager is a built-in password manager, but it focuses on system-level credentials. It stores usernames and passwords for things like network shares, Remote Desktop connections, and some Windows applications.



It was built to handle logins in Windows environments, especially in work environments. However, it wasn't designed to manage the dozens of personal accounts that most people use today, and Credential Manager's limitations make it unsuitable as a full-fledged password manager.

You can access Credential Manager by typing **Credential Manager** into the Windows search bar and selecting the best match, or by navigating through **Control Panel > User Accounts > Credential Manager** .

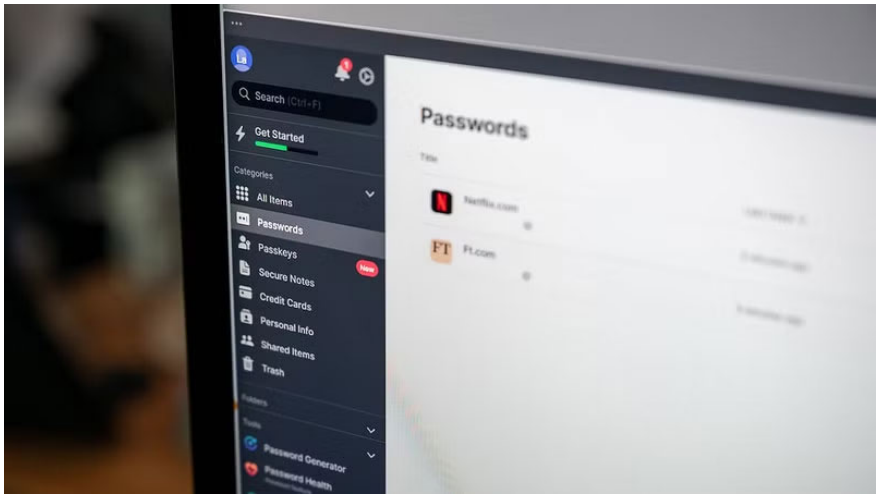
Why can't I use Credential Manager instead of password manager?

While Windows Credential Manager sounds like a suitable replacement for a password manager , there are a number of reasons why it can't be used in the same way.

Poor cross-platform compatibility

Whether you're using a free, open-source password manager like KeePass or a paid service like Bitwarden or 1Password , most options today offer seamless sync across platforms — Windows, macOS, Linux, iOS, Android, and browser extensions.

You can save passwords on your phone while you shop online, and they'll sync to your laptop before you even put your phone down. This instant syncing happens via encrypted cloud services, and it works across every platform imaginable.



Windows Credential Manager, on the other hand, is tightly integrated into Windows and does not provide native support outside of the Windows environment. It does not have an app. You cannot sync or share passwords with anyone else.

Security risks and single points of failure

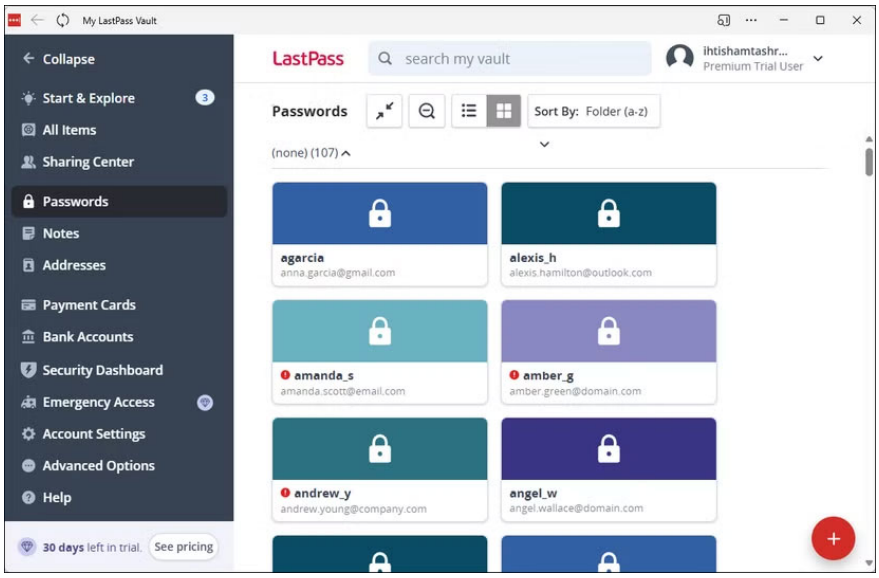
Dedicated password managers operate on the principle of zero knowledge. This means that even if an attacker breaches your company's servers, your passwords are still safe because they are encrypted with a master password, which only you know.

Credential Manager's security model is simple: If you're logged into Windows, you have full access. Click any password, hit **Show** , and it will appear in plain text. One-time authentication is required, but that doesn't offer much protection if someone already knows your login password.

Fewer features than dedicated password managers

A dedicated password manager does more than just securely store and sync your passwords across devices. You can use it to generate strong passwords with a single click, scan the dark web for exposed credentials with automatic alerts when any breaches occur, and even promote security best practices by flagging weak or reused

passwords and prompting you to fix them.

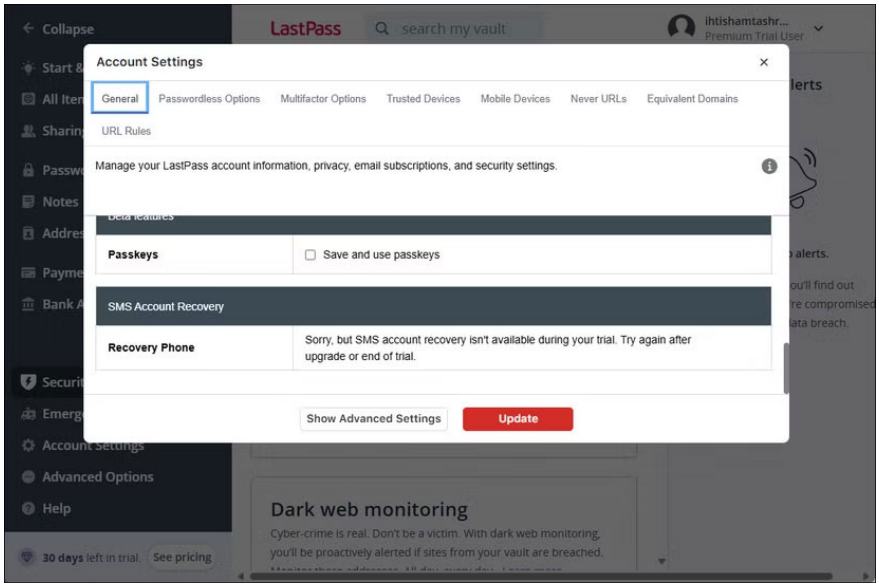


Credential Manager only stores passwords — and that's it. It doesn't offer features like password generation, breach alerts, or security analytics. It won't warn you if you're using weak credentials like password123 for your bank account, and it can't store or generate two-factor authentication codes, either.

Basic recovery options

Redundancy is a core part of most dedicated password managers. If you lose your master password, you can use a recovery code or enlist the help of an emergency contact to regain access.

If your device is stolen, you can revoke access remotely from any browser. All data is automatically backed up to encrypted cloud storage, so even if your master password fails, your passwords are still safe and accessible.



Credential Manager stores passwords locally and associates them with the Windows account on that particular device. If you forget your Windows password or your computer crashes, your saved credentials may be lost.

Browser integration and autofill capabilities are negligible

Any good password manager should work seamlessly with your browser, and autofill is a big part of that equation. It saves time by filling in usernames, passwords, payment information, and other form fields with a single click.

Credential Manager has no native browser support. Even Microsoft Edge , the company's browser, doesn't rely on it and uses its own password system. The only browser that actually works with Credential Manager is Internet Explorer, but it's not supported in the latest version of Windows 11.