Where does Windows store passwords and credentials?

Short answer: In several predictable places — the Windows Credential Manager, browser password stores, VPN client configuration, and on domain controllers the Active Directory database (NTDS). "Predictable" is the key word: automated attacks rely on those locations being the same on every machine.

The main stores

- **Windows Credential Manager** — saved logins for network resources and applications.
- **Browser password stores** — Chrome, Edge, and Firefox each keep saved credentials in known profile paths.
- **VPN client credentials** — usernames, passwords, and key-based authentication material.
- **NTDS (Active Directory)** — on a domain controller, the credential data for the entire domain. The highest-value target on the network.
- **Application-specific stores** — messaging and collaboration tools, file transfer clients, and gaming platforms each maintain their own.

Why predictability is the whole point

Attackers know nothing about your specific environment. Their automation is written against paths that exist everywhere — `C:\Users\[Username]`, standard application data folders, standard drive letters. A script doesn't need to understand your network; it just walks known paths.

That's a weakness in their method. If those exact locations are the ones being watched, the attacker's own reliability requirement becomes the trigger that catches them.

What Cyber Crucible does with that

These stores are the monitored identity-theft entry points. A program reading them has its intent assessed in under 200 milliseconds — and is suspended if that intent is malicious, before any credential is taken.

Revision #3
Created 2026-07-20 19:24:27 UTC by Dennis Underwood
Updated 2026-07-21 19:32:41 UTC by Dennis Underwood