What is Credential Manager?

Windows Credential Manager is the built-in vault that stores credentials users save: web logins, network share passwords, and Remote Desktop credentials. It keeps them in Web and Windows vaults, protected by DPAPI. An attacker running as the user (or with their DPAPI master key) can read the saved credentials back as cleartext, collecting passwords to shares, sites, and remote systems. It is a quick, high-value harvest once a user is compromised.

HOW IT WORKS

01 The abuse and payload

In a compromised user's session, the attacker reads the vault:

- List saved credentials: `cmdkey /list` and `vaultcmd /listcreds:"Windows Credentials" /all`.
- Decrypt them with a DPAPI-aware credential tool (`vault::cred`, `dpapi::cred`) to recover cleartext share, RDP, and web passwords.
- Saved RDP and share credentials often point straight at other hosts, fueling lateral movement.

Documented techniques shown for defenders.

> SAVED MEANS RECOVERABLE
>
> *Anything a user saved in Credential Manager can be recovered as cleartext from their context. Saved RDP and share passwords are a direct map to the next hop.*

HOW TO DEFEND

- Discourage saving credentials for privileged shares and remote connections via policy.
- Limit local admin and enable [Credential Guard](/learn/active-directory/what-is-credential-gu to make user-context theft harder.
- Use just-in-time access rather than long-lived saved credentials to sensitive systems.
- Keep privileged accounts off ordinary workstations so their credentials are never saved there.
- Detect bulk vault/credential reads.

SOURCES

[1] MITRE ATT&CK: Credentials from Password Stores (T1555)

[2] Microsoft: Credential Manager API

[3] MITRE ATT&CK: Credential Access (TA0006)

Find the exposed credentials before an attacker does.

securelayer7.net/learn/credential-access/what-is-windows-credential-manager

Open online