

# Credential Dumping Mitigation, Mitigation T1003 - Enterprise

Archived: 2026-04-05 15:07:37 UTC

## Windows

Monitor/harden access to LSASS and SAM table with tools that allow process whitelisting. Limit credential overlap across systems to prevent lateral movement opportunities using [Valid Accounts](#) if passwords and hashes are obtained. Ensure that local administrator accounts have complex, unique passwords across all systems on the network. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.

---

Source: <https://attack.mitre.org/mitigations/T1003>