# OS Credential Dumping: DCSync, Sub-technique T1003.006 - Enterprise

Archived: 2026-04-05 15:41:59 UTC

Adversaries may attempt to access credentials and other sensitive information by abusing a Windows Domain Controller's application programming interface (API)[1] [2] [3] [4] to simulate the replication process from a remote domain controller using a technique called DCSync.

Members of the Administrators, Domain Admins, and Enterprise Admin groups or computer accounts on the domain controller are able to run DCSync to pull password data[5] from Active Directory, which may include current and historical hashes of potentially useful accounts such as KRBTGT and Administrators. The hashes can then in turn be used to create a Golden Ticket for use in Pass the Ticket[6] or change an account's password as noted in Account Manipulation.[7]

DCSync functionality has been included in the "lsadump" module in Mimikatz.[8] Lsadump also includes NetSync, which performs DCSync over a legacy replication protocol.[9]

---

Source: https://attack.mitre.org/techniques/T1003/006