MITRE | ATT&CK®

ATT&CK v16 has been released! Check out the blog post for more information.

Home > Software > esentutl

# esentutl

esentutl is a command-line tool that provides database utilities for the Windows Extensible Storage Engine.[1]

> **ID:** S0404
>
> ⓘ **Associated Software:** esentutl.exe
>
> ⓘ **Type:** TOOL
>
> ⓘ **Platforms:** Windows
>
> **Contributors:** Edward Millington; Matthew Demaske, Adaptforward
>
> **Version:** 1.3
>
> **Created:** 03 September 2019
>
> **Last Modified:** 28 September 2023

Version Permalink

## Techniques Used

ATT&CK® Navigator Layers ▾

| Domain | ID | Name | Use |
|--------|-----|------|-----|
| Enterprise | T1005 | Data from Local System | esentutl can be used to collect data from local file systems.[2] |
| Enterprise | T1006 | Direct Volume Access | esentutl can use the Volume Shadow Copy service to copy locked files such as ntds.dit [3] |