

# .. /Odbccconf.exe

Execute (DLL)

Used in Windows for managing ODBC connections

## Paths:

C:\Windows\System32\odbcconf.exe  
C:\Windows\SysWOW64\odbcconf.exe

## Resources:

- <https://gist.github.com/NickTyrer/6ef02ce3fd623483137b45f65017352b>
- <https://github.com/woanware/application-restriction-bypasses>
- <https://www.hexacorn.com/blog/2020/08/23/odbcconf-lolbin-trifecta/>

## Acknowledgements:

- Casey Smith (@subtee)
- Adam (@Hexacorn)

## Detections:

- Sigma: [https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process\\_creation/proc\\_creation\\_win\\_odbcconf\\_response\\_file.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_odbcconf_response_file.yml)
- Sigma: [https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process\\_creation/proc\\_creation\\_win\\_odbcconf\\_response\\_file\\_susp.yml](https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_odbcconf_response_file_susp.yml)
- Elastic: [https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense\\_evasion\\_unusual\\_process\\_network\\_connection.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml)
- Elastic: [https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense\\_evasion\\_network\\_connection\\_from\\_windows\\_binary.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml)

## Execute

. ExecuteDllRegisterServer from DLL specified.

```
odbcconf /a {REGSVR c:\test\test.dll}
```

<b>Use case:</b>	Execute dll file using technique that can evade defensive counter measures
<b>Privileges required:</b>	User
<b>Operating systems:</b>	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
<b>ATT&amp;CK® technique:</b>	T1218.008
<b>Tags:</b>	Execute: DLL

. Install a driver and load the DLL. Requires administrator privileges.

```
odbcconf INSTALLDRIVER "lolbas-project|Driver=c:\test\test.dll|APILevel=2"  
odbcconf configsysdsn "lolbas-project" "DSN=lolbas-project"
```

**Use case:** Execute dll file using technique that can evade defensive counter measures  
**Privileges required:** User  
**Operating systems:** Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11  
**ATT&CK® technique:** T1218.008  
**Tags:** Execute: DLL

. Load DLL specified in target .RSP file. See the Code Sample section for an example .RSP file.

```
odbcconf -f file.rsp
```

**Use case:** Execute dll file using technique that can evade defensive counter measures  
**Privileges required:** Administrator  
**Operating systems:** Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11  
**ATT&CK® technique:** T1218.008