

# GitHub - api0cradle/UltimateAppLockerByPassList: The goal of this repository is to document the most common techniques to bypass AppLocker.

By api0cradle

Archived: 2026-04-05 22:32:06 UTC

## Ultimate AppLocker ByPass List

The goal of this repository is to document the most common and known techniques to bypass AppLocker. Since AppLocker can be configured in different ways I maintain a verified list of bypasses (that works against the default AppLocker rules) and a list with possible bypass technique (depending on configuration) or claimed to be a bypass by someone. I also have a list of generic bypass techniques as well as a legacy list of methods to execute through DLLs.

## INDEXED LISTS

- [Generic-AppLockerbypasses.md](#)
- [VerifiedAppLockerBypasses.md](#)
- [UnverifiedAppLockerBypasses.md](#)
- [DLL-Execution.md](#)

## YML

I have also created everything in YML format so it the data can be reused. The YML files can be found under the YML folder.

For details on how I verified and how to create the default rules you can check my blog:

<https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/>

## BLOCK RULES

The rules can be found in the AppLocker-BlockPolicies folder.

Please contribute and do point out errors or resources I have forgotten.

## Other tools

Remember to check out my Powershell module called PowerAL: <https://github.com/api0cradle/PowerAL>. This can help you identify weaknesses

Source: <https://github.com/api0cradle/UltimateAppLockerByPassList>