

WDAC / App Control for Business

Ochrana pred spustením neschváleného kódu. Nasadenie politik pomocou nástroja App Control Policy Wizard.

OBSAH

KAPITOLA PRVÁ - APP CONTROL FOR BUSINESS

KAPITOLA DRUHÁ - APP CONTROL POLICY WIZARD

1 Inštalácia

KAPITOLA TRETIA - VYTVORENIE ZÁKLADNEJ POLITIKY

1 Formát

2 Šablóny

3 Kľúčové možnosti politiky

4 Typy pravidiel

KAPITOLA ŠTVRTÁ - NASADENIE

1 Windows 11 22H2+ a Windows Server 2025

2 Windows Server 2016 až 2022

3 Microsoft Intune

KAPITOLA PIATA - REŽIM AUDITU

KAPITOLA ŠIESTA - DOPLNKOVÉ POLITIKY

KAPITOLA SIEDMA - ODPORÚČANIA A RIEŠENIE ČASTÝCH PROBLÉMOV

1 Voľba úrovne pravidiel podľa administratívnej záťaže

2 Pravidlá typu cesta

3 Pokrytie knižníc a skriptov

4 Podpísané systémové nástroje

5 Cesta k obnove

KAPITOLA ÔSMA - POSTUP NASADENIA

KAPITOLA DEVIATA - ZDROJE

Úvod

Antivírusové riešenia pracujú na princípe blacklistingu — povolia spustiť všetko, čo neobsahuje známu škodlivú signatúru. Nová alebo upravená vzorka preto kontrolou prejde. Application whitelisting tento princíp obracia: spustí sa výhradne to, čo je explicitne povolené.

App Control for Business (do roku 2024 označovaný ako Windows Defender Application Control, WDAC) je implementácia popísaného princípu zabudovaná priamo v systéme Windows. Tento dokument popisuje jej nasadenie pomocou oficiálneho nástroja App Control Policy Wizard.

Verzie softvéru

Nástroj: pri príprave návodu sme použili verziu App Control Policy Wizard 2.8.0.0

Platnosť: Windows 10 (1903+), Windows 11, Windows Server 2016 a novšie



Dokument predpokladá praktickú skúsenosť so správou Active Directory a Windows Servera.

01

KAPITOLA PRVÁ

App Control for Business

App Control for Business je nástroj, ktorý vynucuje integritu kódu na úrovni jadra operačného systému. Pri každom pokuse o načítanie súboru systém overí, či súbor vyhovuje aktívnej politike. Ak nie, načítanie zamietne. Kontrola sa vzťahuje na súbory .exe a .dll, ovládače v režime jadra, skripty (PowerShell, VBScript, JScript), inštalátory MSI, balíčkové aplikácie MSIX a registráciu COM objektov.

Rozhodovanie prebieha v jadre, nie v používateľskom režime. Vynútenú politiku preto nedokáže obísť ani používateľ s lokálnymi administrátorskými oprávneniami. Funkcia je súčasťou systému vo všetkých edíciách a nevyžaduje samostatnú licenciu.



VZŤAH K APPLOCKER

Microsoft odporúča App Control for Business ako primárny nástroj riadenia spúšťaných aplikácií. AppLocker sa má používať už len ako doplnok, napríklad pre pravidlá viazané na jednotlivých používateľov.

Nasadenie je administratívne najmenej náročné v prostrediach s jednotnou softvérovou výbavou, teda tam, kde skupiny staníc zdieľajú rovnaký referenčný obraz. Na staniciach s často sa meniacou softvérovou výbavou (typicky vývojárske) je potrebná premyslenejšia stratégia pravidiel, spravidla postavená na dôveryhodných inštalátoroch (managed installer).

02

KAPITOLA DRUHÁ

App Control Policy Wizard

Nástroj s grafickým rozhraním App Control Policy Wizard obaľuje rutiny modulu ConfigCI. Výstupná politika je identická s tou, ktorú by vytvorili príkazy PowerShellu. Ponúka tri režimy: Policy Creator (tvorba základných a doplnkových politík), Policy Editor (úprava existujúcich politík) a konverzia záznamov denníka udalostí na pravidlá) a Policy Merger (zlúčenie dvoch politík).

Zdrojový kód: <https://github.com/MicrosoftDocs/WDAC-Toolkit>
Stiahnutie: <https://webapp-wdac-wizard.azurewebsites.net/>
Licencia: MIT

1 Inštalácia

Nástroj sa distribuuje ako balík MSIX. Bežná inštalácia:

```
winget install --id Microsoft.AppControlPolicyWizard --exact
```

Na serverových edíciách a v izolovaných prostrediach nemusí byť dostupný komponent App Installer. Systém potom neponúkne pre súbor .msix žiadnu akciu. Balík sa v takom prípade inštaluje priamo:

```
$msix = Get-ChildItem "$env:USERPROFILE\Downloads\*.msix"  
Add-AppxPackage -Path $msix.FullName  
  
# overenie a spustenie  
Get-AppxPackage *WDAC* | Select-Object Name, Version  
explorer.exe shell:AppsFolder\Microsoft.WDAC.WDACWizard_8wekyb3d8bbwe!WDACWizard
```



UMIESTNENIE

Nástroj patrí na administrátorskú pracovnú stanicu, nie na doménový radič. Ideálne na stanicu s reprezentatívnou softvérovou výbavou organizácie.

03

KAPITOLA TRETIA

Vytvorenie základnej politiky

1 Formát

Zvoľte Multiple Policy Format — umožňuje súbežnú platnosť viacerých politík a použitie doplnkových politík.



VÝNIMKA

Nasadenie cez skupinové politiky podporuje výhradne Single Policy Format. Ak plánujete distribúciu cez GPO, formát treba zvoliť už pri vytváraní. Microsoft však GPO ako spôsob nasadenia pre Windows 10 1903 a novšie neodporúča.

2 Šablóny

Šablóna určuje východiskový okruh dôvery. Zoradené od najprísnejšej po najvoľnejšiu:

Šablóna	Okruh dôvery
Default Windows Mode	Komponenty OS, Microsoft Store, Microsoft 365, OneDrive, Teams, ovládače podpísané WHQL. Bez doplnkových pravidiel zablokuje väčšinu administrátorských nástrojov.
Allow Microsoft Mode	Predchádzajúce a navyše všetok softvér podpísaný spoločnosťou Microsoft. Vhodný východiskový bod pre bežné nasadenie.
Signed and Reputable Mode	Predchádzajúce a navyše podpísané súbory s dobrou reputáciou podľa Intelligent Security Graph.

3 Kľúčové možnosti politiky

Možnosť	Význam
Audit Mode	Politika nič neblokuje, iba zaznamenáva. Vždy začnite s touto možnosťou.
Allow Supplemental Policies	Bez nej nie je možné politiku neskôr rozšíriť doplnkovou politikou. Odporúča sa zapnúť.
Advanced Boot Options Menu	Umožní odstránenie politiky pred spustením systému. Ponechať ako záchrannú cestu.
Unsigned System Integrity Policy	Umožní nasadiť politiku bez kryptografického podpisu.
User Mode Code Integrity	Rozšíri kontrolu na aplikácie v používateľskom režime. Bez nej sa kontrolujú len ovládače.

4 Typy pravidiel

Typ	Charakteristika
Publisher	Dôveruje podpisovateľovi. Prežije aktualizáciu aplikácie. Odporúčaná predvoľba.
File Attributes	Podpis v kombinácii s názvom produktu alebo verziou. Užšie ako Publisher, stále odolné voči aktualizáciám.
File Hash	Každá aktualizácia aplikácie zneplatní pravidlo. Najjednoduchšie použiteľné pre nepodpísané a nemenné súbory.
File Path	Povolí obsah adresára. Vyžaduje kontrolu oprávnení — pozri kapitolu 8.2.
Packaged App / COM Object	Pravidlá pre aplikácie MSIX a pre registráciu objektov COM.
Folder Scan	Hromadné vytvorenie pravidiel pre všetky súbory v adresári.

Výstupom sprievodcu sú dva súbory: .xml (čitateľná podoba určená na verziovanie a ďalšie úpravy) a .cip (binárna podoba, ktorá sa nasadzuje). Názov súboru .cip je názov politiky GUID a nesmie sa meniť — systém ho podľa neho identifikuje.

**POZNÁMKA**

Na zariadeniach bez pripojenia na internet môže nástroj zobraziť hlásenie „Wizard Integrity Issue“. Ide o očakávané správanie. Pokračujte voľbou No.

04

KAPITOLA ŠTVRTÁ

Nasadenie

1 Windows 11 22H2+ a Windows Server 2025

Systémy s dostupným nástrojom CiTool umožňujú načítanie politiky bez reštartu:

```
CiTool --update-policy "C:\Cesta\{GUID}.cip"  
CiTool --list-policies  
CiTool --remove-policy <ID>
```

2 Windows Server 2016 až 2022

CiTool na týchto systémoch nie je k dispozícii. Politika sa nasadzuje skopírovaním súboru .cip do adresára aktívnych politik; systém načíta všetky prítomné súbory pri štarte.

```
$dest = "$env:SystemRoot\System32\CodeIntegrity\CiPolicies\Active"  
New-Item -Path $dest -ItemType Directory -Force | Out-Null  
Copy-Item "C:\Cesta\{GUID}.cip" -Destination $dest -Force  
  
Restart-Computer -Force
```

Každá politika je reprezentovaná samostatným súborom, ktorý sa pridáva do adresára. Tento nenahrádza predchádzajúce. Po nasadení doplnkovej politiky musí teda zložka obsahovať dva súbory, po pridaní blokovacieho zoznamu tri — vždy s odlišnými GUID.

3 Microsoft Intune

Odporúčaný spôsob pre spravované zariadenia — Endpoint Security, profil App Control for Business. Umožňuje využiť zabudované šablóny alebo nahrať vlastný súbor XML.

05

KAPITOLA PIATA

Režim auditu

Politika v režime auditu nič neblokuje, iba zaznamenáva, čo by zablokovala. Toto úvodné obdobie je najdôležitejšou fázou nasadenia. Vytvorí inventár reálne používaných aplikácií bez rizika výpadku.

ID	Význam
3076	Súbor by bol zablokováný. Hlavná udalosť režimu auditu.
3077	Súbor bol zablokováný vynútenou politikou.
3089	Informácie o podpise, viazané na udalosť 3076 alebo 3077.
3099	Politika bola úspešne načítaná. Zapisuje sa pri štarte systému.
3090 / 3091 / 3092	Povolenie, audit alebo blokovanie na základe reputácie (ISG) alebo dôveryhodného inštalátora.

Denník: Applications and Services Logs → Microsoft → Windows → CodeIntegrity → Operational. Skripty a inštalátory MSI sa zapisujú do AppLocker → MSI and Script.

Zoznam súborov, ktoré by boli zablokované, spolu s politikou, ktorá ich označila, získate nasledovne:

```
Get-WinEvent -FilterHashtable @{
  LogName = 'Microsoft-Windows-CodeIntegrity/Operational'
  Id = 3076
} | ForEach-Object {
  $x = [xml]$_ | .ToXml()
  [PSCustomObject]@{
    File = ($x.Event.EventData.Data |
      Where-Object Name -eq 'File Name').'#text'
    Policy = ($x.Event.EventData.Data |
      Where-Object Name -eq 'PolicyName').'#text'
  }
} | Sort-Object File -Unique | Format-Table -AutoSize
```

Pole PolicyName je pri viacerých súbežne platných politikách zásadné. Bez neho vieme, že súbor bol označený, ale nevieme ktorou politikou.

Pre priebežné sledovanie je praktické vytvoriť si v Prehliadači udalostí vlastné zobrazenie (Custom View) nad denníkom CodeIntegrity/Operational s filtrom na identifikátory 3076, 3077, 3089 a 3099. Samotný text udalosti 3076 uvádza okrem dotknutého súboru aj proces, ktorý sa ho pokúsil načítať. Pri neočakávanom zázname je to údaj, ktorý odliši interaktívne spustenie od služby alebo naplánovanej úlohy.



OBJEM DENNÍKA

Ku každej udalosti 3076 sa zapisuje aj zodpovedajúca udalosť 3089 s informáciami o podpise, takže počet záznamov je približne dvojnásobný. Pri zostavovaní inventára filtrujte len udalosť 3076. Prehliadač udalostí postačuje na preverenie jednotlivého záznamu. Na spracovanie niekoľkotýždňového auditu je vhodnejší PowerShell alebo Advanced Hunting v službe Microsoft Defender for Endpoint, ktorý zároveň umožňuje export do formátu CSV importovateľného priamo do nástroja.

Odporúčaná dĺžka auditu sú štyri týždne, aby sa zachytili aj mesačné a štvrťročné procesy.

06

KAPITOLA ŠIESTA

Doplnkové politiky

Zistené legitímne aplikácie sa nepridávajú do základnej politiky, ale do doplnkovej (supplemental), ktorá základnú rozširuje. Základná politika tak zostáva stabilná a jedna doplnková politika môže pokrývať jednu aplikáciu alebo skupinu staníc.

Postup: Policy Creator → Multiple Policy Format → Supplemental Policy, následne výber základnej politiky vo formáte XML. Nástroj overí, či základná politika doplnkové politiky povoľuje.



OČAKÁVANÉ SPRÁVANIE

Prepínač Audit Mode je pri doplnkovej politike neaktívny. Režim vynútenia je vlastnosťou základnej politiky a doplnková ho dedí.

Doplnková politika okruh dôvery iba rozširuje. Zakazujúce pravidlá do nej nepatria. Ak je potrebné niečo zakázať, použije sa samostatná základná politika, ako popisuje kapitola 8.4.

Pri tvorbe pravidla typu Publisher nástroj ponúkne atribúty podpisovateľa. Ponechajte zaškrtnuté iba Issuing CA a Publisher. Položky File name a Min. version pravidlo zúžia na konkrétny súbor a konkrétnu verziu, čím sa stratí odolnosť voči aktualizáciám. Ak je cieľom užší okruh dôvery, použite namiesto názvu súboru položku Product name.

Ak nástroj v zozname pravidiel zobrazí označenie „Hash Fallback Possible“, nepodarilo sa zostaviť úplný reťazec certifikátov a časť súborov sa môže porovnávať podľa hashu. Takéto pravidlo je potrebné overiť testovaním.

07
KAPITOLA SIEDMA

Odporúčania a riešenie častých problémov

Nasledujúce body nie sú zoznamom chýb, ale rozhodnutí, ktoré je potrebné vedome urobiť pri návrhu politiky. Vo väčšine prípadov ide o voľbu medzi mierou bezpečnosti a administratívnou záťažou.

1 Voľba úrovne pravidiel podľa administratívnej záťaže

Návod CSIRT.SK k [application whitelistingu](#) popisuje postup založený na zozname hashov vytvorenom z referenčnej stanice a zároveň uvádza prechod na pravidlá podľa podpisu výrobcu ako spôsob, ako znížiť záťaž správcov. Rovnaká úvaha platí aj pre App Control, len s väčším počtom dostupných úrovní.

Pravidlá podľa typu hashu poskytujú najvyššiu mieru istoty — povolený je presne ten súbor, ktorý bol overený. Cenou je, že každá aktualizácia aplikácie zmení hash a pravidlo prestane platiť. Rozsah tejto záťaže je v praxi vyšší, než sa očakáva: bežná aplikácia strednej veľkosti obsahuje desiatky spustiteľných komponentov. Napríklad nástroje VMware Tools na serveri predstavujú vyše päťdesiat súborov, teda päťdesiat pravidiel, ktoré zneplatní každá aktualizácia. Jedno pravidlo podľa podpisu výrobcu pokryje všetky a aktualizáciu prežije.

Úroveň	Bezpečnosť	Údržba	Vhodné použitie
Hash	Najvyššia	Vysoká	Nepodpísané a nemenné súbory, vlastné nástroje, jednoúčelové stanice.
File Attributes	Vysoká	Nízka	Kompromis — viaže pravidlo na podpis aj na názov produktu.
Publisher	Dobrá	Nízka	Podpísaný softvér tretích strán v bežnej prevádzke.
File Path	Podmienená	Najnižšia	Len pre adresáre so zabezpečenými oprávneniami — pozri 8.2.



PRAKTICKÉ ODPORÚČANIE

Použite pravidlá podľa podpisu ako základ a hash ponechajte pre nepodpísané súbory, ktoré sa nemenia. Ak je potrebný užší okruh dôvery než „všetko od tohto výrobcu“, zvolte úroveň File Attributes s naviazaním na názov produktu — pravidlo tak zostane odolné voči aktualizáciám, ale nepokryje celé portfólio výrobcu.

2 Pravidlá typu cesta

Pravidlo povolujujúce obsah adresára je administratívne najjednoduchšie, ale platí len do tej miery, do akej je zabezpečený samotný adresár. Ak doň môže zapisovať bežný používateľ, útočník tam umiestni vlastný binárny súbor a politika ho povolí.



RIEŠENIE

Pred vytvorením takéhoto pravidla overte zoznam riadenia prístupu daného adresára a uistite sa, že zápisy majú výhradne správcovia a systém. Pre adresáre v profile používateľa a priečinkov pre dočasné súbory sa pravidlá typu cesta nehodia. App Control ponúka aj nastavenie, ktoré pravidlá typu cesta obmedzí len na adresáre nezapisovateľné bežným používateľom. Pri tomto prístupe však počítajte s možnosťou, že útočník zneužije známu alebo zero-day zraniteľnosť, čím získá potrebné oprávnenia.

3 Pokrytie knižníc a skriptov

App Control kontroluje každý modul, ktorý proces načíta, nielen spustiteľný súbor. Aplikácia sa preto môže po prechode do vynúteného režimu správať chybne aj vtedy, keď jej hlavný súbor politike vyhovuje a zlyhá až jedna z knižníc. V praxi to znamená, že inventár musí zahŕňať aj súbory .dll, nielen .exe.

Riešenie je rovnaké ako v návode CSIRT.SK pre [application whitelistingu](#) — vytvorenie referenčnej stanice („golden image“) so schválenou softvérovou výbavou a odvodenie pravidiel z nej. Pri App Control má tento postup dva doplnky. Prvým je funkcia Folder Scan, ktorá prehľadá zvolený adresár a vytvorí pravidlá pre všetky nájdené súbory naraz. Druhým je samotný režim auditu, ktorý zachytí aj komponenty načítané až za behu a pri statickom prehľadávaní by unikli.

Zároveň overte, že politika pokrýva aj skripty a inštalátory MSI. Škodlivý kód sa dnes bežne spúšťa cez PowerShell, VBScript alebo balíky MSI. Aktívna politika pre používateľský režim mimochodom automaticky prepne PowerShell do režimu Constrained Language Mode, čo je ďalšia vrstva ochrany.

4 Podpísané systémové nástroje

Šablóny povoľujúce softvér podpísaný spoločnosťou Microsoft povoľujú aj nástroje, ktoré je možné zneužiť na spustenie ľubovoľného kódu (napríklad msbuild.exe, mshta.exe alebo wmic.exe). Ide o legitímne súčasti systému, ktoré nemožno jednoducho odstrániť.

Riešením je hybridný model — široké povoľovacie pravidlá doplnené o explicitné zakazujúce pravidlá. Microsoft na tento účel zverejňuje a priebežne aktualizuje dva zoznamy:

Zoznam aplikácií zneužíteľných na obídenie App Control

<https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/design/applications-that-can-bypass-appcontrol>

Zoznam zraniteľných ovládačov

<https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/design/microsoft-recommended-driver-block-rules>

Oba zoznamy sú publikované vo formáte XML. Odporúčaným postupom pre systémy Windows 10 1903 a novšie nie je zlúčenie s existujúcou politikou, ale nasadenie ako samostatnej základnej politiky. Súbežne platné základné politiky sa vyhodnocujú ako prienik — súbor musí vyhovieť každej z nich — takže zakazujúce pravidlá sa uplatnia bez zásahu do funkčnej povoľovacej politiky:

```
# priradenie nového identifikátora politiky
Set-CIPolicyIdInfo -FilePath $xml `
-PolicyName "MS Recommended Block Rules" -ResetPolicyId

# kompilácia; názov súboru musí byť GUID politiky
ConvertFrom-CIPolicy -XmlFilePath $xml -BinaryFilePath $cip

# nasadenie vedľa existujúcich politik
Copy-Item $cip -Destination `
"$env:SystemRoot\System32\CodeIntegrity\CiPolicies\Active"
```

Ak sa napriek tomu zvolí zlúčenie s existujúcou povoľovacou politikou, je nutné zo zoznamu najprv odstrániť dve pravidlá „Allow all“ (ID_ALLOW_A_1 a ID_ALLOW_A_2) aj ich odkazy v sekcii FileRulesRef. Bez toho by zlúčená politika povolila spustenie čohokoľvek.

Zoznam zraniteľných ovládačov je od aktualizácie Windows 11 z roku 2022 predvolene zapnutý a na systémoch s aktívnou integritou pamäte sa vynucuje automaticky. Na starších systémoch a na

serverových edíciách ho treba doplniť ručne.



ROZSAH PRAVIDIEL

Zoznam nie je plochým zoznamom zakázaných súborov. Časť pravidiel je ohraničená verziou a blokuje len známe zraniteľné zostavenia — napríklad cscript.exe do verzie 5.812.10240.0 alebo bginfo.exe do verzie 4.22. Novšie zostavenia týchto súborov pravidlu nevyhovujú a zablokovanie nebudú. Reálny dopad zoznamu je preto spravidla menší, než sa pri čítaní súpisu názvov očakáva.



PRED NASADENÍM

Microsoft odporúča overiť zoznam blokových ovládačov najprv v režime auditu. Zablockovanie ovládača bez testovania môže spôsobiť nefunkčnosť zariadenia alebo pád systému. Pri zozname aplikácií platí, že na Windows Server 2016 môže časť pravidiel určených pre novšie systémy spôsobiť nefunkčnosť aplikácií.

5 Cesta k obnove

Pred prechodom do vynúteného režimu pripravte postup pre prípad, že politika zablokuje kritickú aplikáciu alebo znemožní prihlásenie. Ponechajte zapnutú možnosť Advanced Boot Options Menu, ktorá umožní odstránenie politiky pred spustením systému, a majte pripravenú náhradnú povoliujúcu politiku. Na zariadeniach spravovaných cez Intune slúži ako záchranná cesta aj nasadenie upravenej politiky, na lokálnych systémoch odstránenie súboru .cip z adresára aktívnych politik a reštart.

08

KAPITOLA ÔSMA

Postup nasadenia

1. Vytvorte základnú politiku zo šablóny Allow Microsoft Mode v režime auditu so zapnutou možnosťou Allow Supplemental Policies.
2. Nasad'te odporúčané blokovacie zoznamy Microsoftu ako samostatnú základnú politiku (pozri 8.4), rovnako v režime auditu.
3. Nasad'te na pilotnú skupinu zariadení reprezentujúcu reálne používanie.
4. Štyri týždne zbierajte udalosti s identifikátorom 3076.
5. Vytvorte doplnkovú politiku s pravidlami typu Publisher pre zistené legitímne aplikácie.
6. Opakujte audit, kým počet neočakávaných udalostí neklesne na nulu.
7. Vypnite režim auditu a nasad'te vynútenú politiku na pilotnú skupinu.
8. Po overení stability rozšírte nasadenie na celú organizáciu.
9. Zaved'te proces schvaľovania a pridávania nových aplikácií do politiky.

09

KAPITOLA DEVIATA

Zdroje

Zdrojový kód a dokumentácia nástroja

<https://github.com/MicrosoftDocs/WDAC-Toolkit>

Stiahnutie nástroja

<https://webapp-wdac-wizard.azurewebsites.net/>

CSIRT.SK – Návod na application whitelisting

https://csirt.sk/wp-content/uploads/2026/06/Navod_Application_whitelisting.pdf

Aplikácie zneužiteľné na obídenie App Control

<https://learn.microsoft.com/en-us/windows/security/application-security/.../applications-that-can-bypass-appcontrol>

Odporúčaný zoznam zraniteľných ovládačov

<https://learn.microsoft.com/en-us/windows/security/application-security/.../microsoft-recommended-driver-block-rules>

App Control for Business Wizard – Microsoft Learn

<https://learn.microsoft.com/en-us/windows/security/application-security/.../appcontrol-wizard>

Konfigurácia App Control politík na Windows Server

<https://learn.microsoft.com/en-us/windows-server/security/osconfig/osconfig-how-to-configure-app-control-for-business>

Identifikátory udalostí App Control

<https://learn.microsoft.com/en-us/windows/security/application-security/.../querying-application-control-events-centrally-using-advanced-hunting>