



AP HOGESCHOOL
ANTWERPEN

AP.BE

Microsoft Defender Application Control (MDAC)

Cybersecurity Intro

Opleiding: **graduaat systeem- en netwerkbeheer**

Academiejaar: **2024-25**

Jelle Van den Broeck

Ernie De Magtige

Inhoud

Microsoft Defender Application Control	1
1 Voorwoord	1
2 Wat is het	2
3 Verschil App Control en Smart App control	3
3.1 App Control	3
3.2 Smart App Control	3
4 Hoe werkt het	4
4.1 WDAC Wizard	5
4.2 Group Policies	6
4.3 AppLocker	7
4.4 Powershell	8
4.5 Microsoft Intune	9
4.6 Adaptive Application Control	10
5 How To Get Started	11
5.1 Voorbereiding	12
5.2 Rules aanmaken	15
5.2.1 publisher	16
5.2.2 Path	16
5.2.3 File hash	16
6 Panopto video	19
7 Logboek	19
8 Afbeeldingen	20
9 Bibliografie	21

Microsoft Defender Application Control

1 Voorwoord

In deze Magnum Opus zal het onderwerp Microsoft Defender Application Control behandeld worden. Zo zal er besproken worden wat het is en wat het doet, maar ook zal er aan bod komen hoe je hiermee kan werken. Op de dag van vandaag is beveiliging een heel belangrijk aspect, hiervoor komt Microsoft zelf al met een goed beveiligingssysteem die je volledig zelf kan instellen naar je eigen perfecties. Ik heb voor dit onderwerp gekozen omdat het mij een heel interessant onderwerp lijkt en ook belangrijk is dat je dit kent als je later een job zoekt in cybersecurity.

2 Wat is het

Microsoft defender application control is een software van Microsoft die tegenwoordig standaard in bepaalde edities van windows zit. Dit zit in de edities van education, enterprise en windows server vanaf versie 2016 en nieuwer. Vanaf windows 11 versie 22H2 bestaat er ook een Smart App Control die vooral bedoeld is voor consumenten en kleine bedrijven. De application control verandert windows naar een plek waar enkel code word uitgevoerd als uw beleid dat voorschrijft. Met deze software kan je het gebruik van apps van gebruikers gaan beperken en niet kunnen uitvoeren en zelfs de code die uitgevoerd word in de kernel. Hiermee kan je een eigen bubbel gaan creëren van applicaties die wel en niet toegestaan zijn. En zo je netwerk van je bedrijf gaan beveiligen op eventuele websites die virussen en dergelijke kunnen bevatten.

Let op. Microsoft Defender Application Control is zeker geen vervanging voor een antivirus software. Voor optimale beveiliging van je netwerk/systeem kan je best nog een antivirus naast de App Control draaien.



Afbeelding 1: Microsoft Defender Application Control

3 Verschil App Control en Smart App control

In dit hoofdstuk ga ik al een kleine toelichting geven wat het verschil is tussen de standaard App Control en Smart App Control. Dit is belangrijk om te weten dat je geen onderwerpen door elkaar haalt omdat ze wel hetzelfde doen maar niet op dezelfde manier werken.

3.1 App Control

Bij de standaard versie van Application control kan je als administrator zelf alles specifiek gaan instellen wat er wel gebruikt mag worden en wat er geblokkeerd moet worden. Het voordeel hieraan is dat je alles zelf kan beslissen, als er bijvoorbeeld apps zijn die niet gekend zijn door Microsoft maar je bedrijf wel nodig heeft kan je dit wel doorlaten. Maar het nadeel is wel dat dit veel werk is om alles in te stellen en een goede documentatie vereist, alsook opvolging voor nieuwe applicaties toe te laten of te blokkeren.

3.2 Smart App Control

Smart App Control gaat zelf beslissen of de applicatie die geopend wilt worden veilig is of niet. Dit gaat te werk door te kijken naar de intelligente cloudbeveiligingsservice van Microsoft en zo kijkt of het een betrouwbare voorspelling kan doen over de veiligheid van de app. Als er daar instaat dat het veilig is laat hij de app door maar als die daar als onbetrouwbaar gemarkeerd is word die tegengehouden.

Als de beveiligingsservice geen betrouwbare voorspelling kan maken, controleert Smart App Control of de applicatie een geldige handtekening heeft. Op basis hiervan gaat Smart App Control beslissen of de app betrouwbaar is of niet.

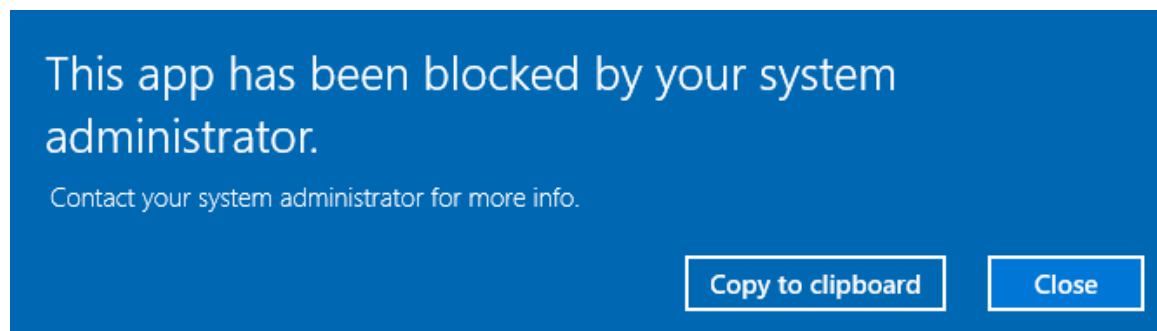
Je kan Smart App Control zelf inschakelen voor je computer maar eerst zal de evaluatiemodus beslissen of je een goede kandidaat bent om dit te gebruiken of niet. Dit word beslist door te kijken hoe vaak App Control in de weg gaat staan en of je je computer gebruikt voor zakelijke of persoonlijke doelen.

4 Hoe werkt het

In tegenstelling tot Smart App Control waar je zelf niets kan instellen en volledig werkt met de data die Microsoft zelf heeft of nagaat op de digitale handtekening van de applicaties, kan je bij de standaard Application Control echt alles naar je eigen wens zetten. Daarom gaan we hier ook vooral de standaard App Control toelichten omdat je hier veel meer zelf mee kan spelen en dus veel dieper kan ingaan qua uitleg.

Je hebt een aantal verschillende manieren hoe dit kan instellen. Zo kan je dit zelf in de instellingen gaan instellen zoals bij Microsoft Intune, maar dit is vrij beperkt in opties. Als je dit voor een netwerk gaat doen kan je het in de GPO's instellen maar je kan ook zelf handmatig doen in powershell. Powershell is de meest aangeraden optie omdat je hier heel nauwkeurig zelf alles kan instellen naar je eigen wens. Maar dit is niet gemakkelijk als je niet veel van Powershell kent. Daarom is het best aangeraden om AppLocker te gebruiken als je een klein netwerk hebt omdat dit het meest gebruiksvriendelijke is maar als je al een groter netwerk moet beheren zal Intune een duidelijker overzicht kunnen geven.

Er zijn verschillende methodes waar App Control mee werkt, zo heb je de optie om via Powershell zelf een beleid te maken op basis van de hash van het bestand maar dit is al vrij ingewikkeld en moet je goed weten hoe dit werkt. Maar je kan ook op basis van de naam van het bestand zoals met AppLocker.



Afbeelding 2: foutmelding

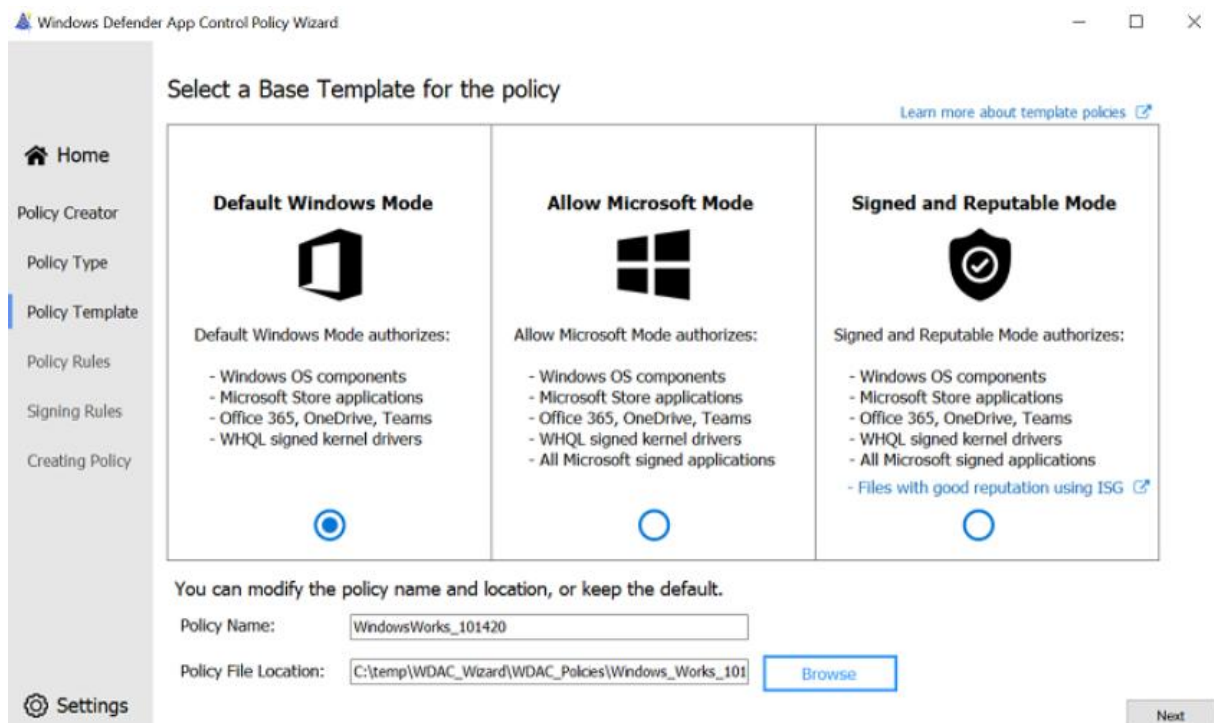
4.1 WDAC Wizard

De WDAC Wizard is een handige tool die gemaakt is door Microsoft om het aanmaken en beheren van Application Control beleidsregels aanzienlijk te vereenvoudigen. In tegenstelling tot andere tools word dit niet standaard meegeleverd met Windows. Als je deze wizard wilt gebruiken ga je deze kunnen downloaden via GitHub waar dit door Microsoft zelf word aangeboden.

[WDAC Wizard](#)

Waarom is deze tool nu zo handig denk je. Dit komt omdat dit heel overzichtelijke structuur heeft. Hierdoor is het risico op fouten maken bij de policies aan te maken veel kleiner. De interface is heel duidelijk gemaakt zodat ook mensen die er niet heel veel over kennen gemakkelijk policies kunnen aanmaken.

Wat nog een belangrijk voordeel is van deze wizard is dat het heel snel is. Je hebt heel rap je policy en kan deze dan ook direct testen. Wat het de ideale tool maakt als je rap iets nieuw wilt uitrollen en wilt uittesten. Of als je een snel een fout moet gaan oplossen. Vanaf dat je dan deze policy hebt kan je deze via groepsbeleid of via powershell toepassen door de eenvoudige exportmogelijkheden.



Afbeelding 3: WDAC Wizard

4.2 Group Policies

Via de Group Policy Management Console (GPMC) kun je op een eenvoudige en centrale manier applicaties blokkeren in een Windows domein. Door handmatig een lijst te maken met de ongewenste toepassingen, kun je nauwkeurig bepalen welk je wilt blokkeren binnen je organisatie.

Een groot voordeel van deze aanpak is dat je de beleidsregels in één keer kunt toepassen op het volledige domein. Dit zorgt voor een eenduidige beveiliging die voor iedereen gelijk is om te voorkomen dat er ergens iets vergeten word. Wat nog een voordeel is van Group Policy is de flexibiliteit ervan, je kan deze toepassen op het hele domein tegelijk, maar ook aan aparte OU's of aan beveiligingsgroepen. Zo kan je bijvoorbeeld de groep van het onthaal een strenger beleid geven als de groep van de IT dienst.

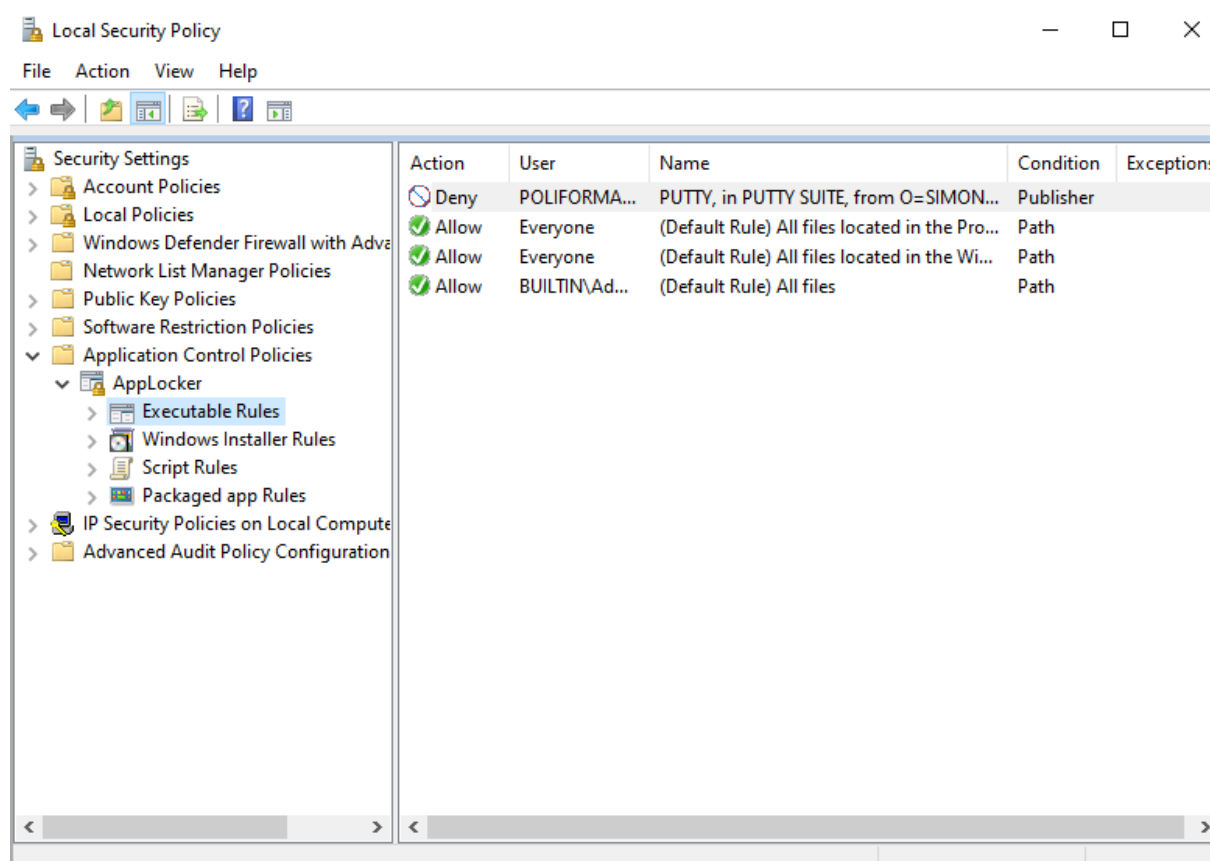
Wat deze methode extra handig maakt is het overzicht dat je hiervan krijgt van de geblokkeerde toepassingen. Je krijgt een duidelijke lijst te zien welke regels er actief staan en op welke gebruikers of groepen dit actief staat. Hierdoor word het beheer ervan heel schaalbaar, overzichtelijk en makkelijk aanpasbaar indien nodig.

4.3 AppLocker

Applocker is een Tool die standaard ingebouwd is bij bepaalde edities van Windows, zoals Windows 10/11 Enterprise en Education en in de Windows server versies. Met Applocker kun je zelf op je eigen computer rules instellen om applicaties te blokkeren.

Je kunt Applocker openen door te zoeken naar “secpol.msc”. In het venster dat nu opent kan je onder “application control policies” de sectie van Applocker vinden. Van daaruit kan je eenvoudig je regels aanmaken met behulp van een wizard interface. Hier kan je dan specifiek je eigen rules in maken op lokale computers.

Dit werking om deze rules aan te maken is identiek zoals Group policy. Hierdoor wordt het beheer hiervan ook heel handig en duidelijk omdat je een mooi overzicht krijgt van alle actieve regels en voor wie ze zijn. Dit maakt het configureren van Application Control veel handiger dan andere methodes. Nog een voordeel van Applocker is dat je dit zowel lokaal kan gebruiken als op een server via GPO.



Afbeelding 4: AppLocker

4.4 Powershell

Als je Application Control wilt instellen op een standalone computer die niet in een domain zit en waar ook geen Applocker op aanwezig is omdat de windows versie dit niet ondersteund. Gaat je zo goed als enige optie Powershell zijn, je kan eventueel ook in de instellingen doen maar dit is heel beperkt. Powershell is hiervoor dan de meest uitgebreide, nauwkeurige en flexibele manier. Hiermee kan je gedetailleerde beleidsregels maken en toepassen volledig afgestemd op jou wensen.

Deze aanpak heeft zowel voor als nadelen. Het grootste voordeel is de controle en flexibiliteit, je kunt praktisch alles van toegestane of geblokkeerde applicaties definiëren. Je kan dit doen door middel van uitgevercertificaten, padregels, hashregels enzovoort. Hierdoor word het geschikt voor geavanceerd gebruik en beveiliging die heel specifiek moet zijn.

Maar Powershell brengt ook zijn nadelen met zich mee. Wat een groot nadeel is, is dat het heel overweldigend kan zijn als je Powershell niet goed onder de knie hebt. De commando's die je nodig hebt zijn vaak heel complex waardoor het risico op fouten maken aanzienlijk groter word. Daarom word het sterk aangeraden om bij het gebruik van Powershell goed te documenteren en back-ups te maken van je systeem voor je hieraan begint.

```
1 New-CIPolicy -Level Publisher -FilePath "C:\WDAC\MyPolicy.xml" -UserPEs -Fallback Hash
2
3 ConvertFrom-CIPolicy -XmlFilePath "C:\WDAC\MyPolicy.xml" -BinaryFilePath "C:\WDAC\MyPolicy.cip"
4 |
5 Copy-Item "C:\WDAC\MyPolicy.cip" "C:\Windows\System32\CodeIntegrity\SIPolicy.p7b"
6 Restart-Computer
```

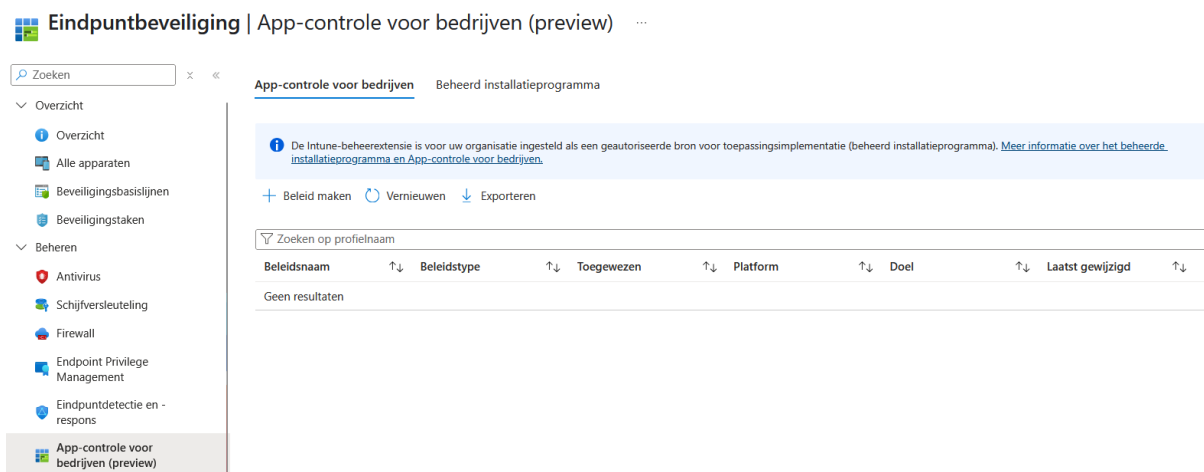
Afbeelding 5: Powershell voorbeeld

4.5 Microsoft Intune

Microsoft Intune is een cloudgebaseerd beheersplatform waar je centraal apparaten, applicaties en beveiligingsinstellingen kan beheren in een organisatie. Met Intune kan je MDAC policies instellen en uitrollen naar alle beheerde apparaten binnen je organisatie zoals je met de Group Policy Manager doet. Dit maakt het een hele krachtige tool voor organisaties met een moderne en cloudgerichte infrastructuur.

Een groot voordeel van Microsoft Intune is het gebruiksgemak. Je kan hier heel handig in werken en heeft een duidelijk grafische interface waar overal ook uitleg bij staat in de Microsoft Endpoint Manager Admin Center. Je hoeft hier dus geen ingewikkelde Powershell scripts gaan uitvoeren en je moet ook niet op alle computers apart gaan instellen. Alles word over het netwerk toegepast zodra de apparaten met Intune zijn gekoppeld.

Maar ook dit heeft zijn nadelen natuurlijk. In tegenstelling tot Powershell waar je tot in het kleinste detail kan werken is Intune veel minder flexibel. Niet alle geavanceerde MDAC-opties zijn hier beschikbaar. Dus als je iets specifiek moet instellen zoals een bepaalde hash bijvoorbeeld zal je nog steeds met Powershell moeten werken.



Afbeelding 6: Microsoft Intune Portaal

4.6 Adaptive Application Control

Adaptive Application Control is een slimme beveiligingsfunctie van Microsoft Defender die gebruik maakt van machine learning om automatisch te bepalen welke applicaties toegestaan zijn en welke geblokkeerd moeten worden.

In de plaats van dat er een systeembeheerder handmatig een lijst moet maken met toegestane en geblokkeerde applicaties moet maken. Gaat Adaptive Application Control dit zelf doen en zelf een eigen gemaakte database opmaken die gebaseerd is op het gedrag van applicaties die in de organisatie gebruikt worden.

Het systeem analyseert hierbij naar:

- Welke regelmatig worden gebruikt
- Wie ze geïnstalleerd heeft
- Of ze gesignd zijn door een betrouwbare uitgever
- Of ze voorkomen in veilige configuraties van andere bedrijven

Met deze gegevens gaat het systeem zelf beslissen over welke apps veilig zijn of niet. Hierdoor is dit veel minder arbeidsintensief en vermindert het risico op fouten door manuele configuratie.

Het grote voordeel van Adaptive Application control is duidelijk de automatisering ervan en de tijdsbesparing op het configureren en het beheren ervan voor de systeembeheerder. Maar er is ook een belangrijke beperking aan het systeem. Adaptive Application control is uitsluitend bedoeld voor windows-server omgevingen. Dus niet voor Windows-clients waardoor je dus nog steeds beter kan kiezen voor een systeem waar je ook je endpoints mee kan configureren.

5 How To Get Started

Nu we weten wat de verschillende opties zijn en hoe MDAC in zijn werk gaat en wat het doet, is het tijd om eens een kijkje te gaan nemen in aan de praktische kant van het verhaal. Ik gebruik hiervoor een testopstelling die ik in VMware heb klaargezet met een windows server 2022 als domain controller in AD en een windows 10 client die lid is van het domain.

Ik ga hieronder stap voor stap uitleggen hoe je op de meest gebruikte manier een bestand kan blokkeren. Als voorbeeld ga ik gebruik maken van puTTY.msi. Welk je wilt blokkeren is niet van groot belang, het is vooral heel belangrijk dat het een msi, dll of een exe file is. MDAC werkt alleen op uitvoerbare bestanden en niet op bijvoorbeeld tekstbestanden en documenten die niet uitvoerbaar zijn, hiervoor kan je beter gebruik maken van NTFS-permissies om deze te blokkeren.

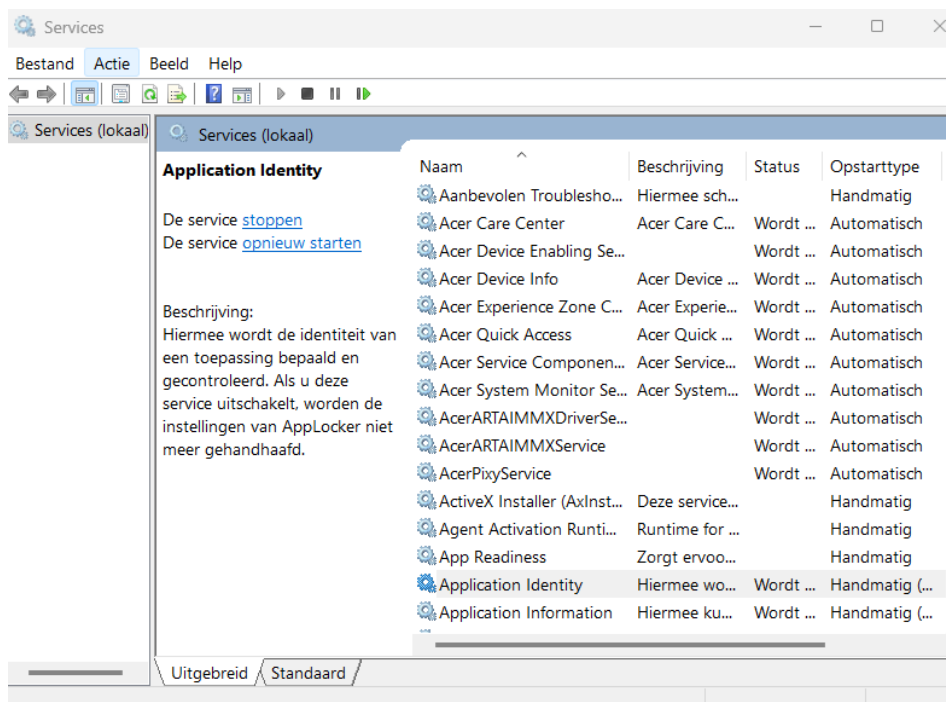
Ten eerste zijn er verschillende mogelijkheden waar je Application Control mee kunt instellen, die afhankelijk zijn van hoe je netwerk eruit ziet. Als het een klein bedrijf is met weinig users kan Applocker en GPO handig zijn. Maar als het een groot bedrijf is kan Applocker al rap onoverzichtelijk worden en kan daarvoor het portaal van Microsoft Intune veel handiger zijn. Dus voor de keuze wat je gebruikt hiervoor hangt dus vooral van de grote van het netwerk af.

Ten tweede gaat bij mij de keuze er vooral van afhangen in de beperkte tools die ik zelf bij de hand heb. En om een duidelijke uitleg te geven die iedereen kan volgen en kan snappen maar natuurlijk ook wel een geldige manier is om mee te werken. Daarom heb ik gekozen om met Applocker te werken omdat dit de duidelijkste methode is waar je toch een uitgebreide keuze hebt in je mogelijkheden.

5.1 Voorbereiding

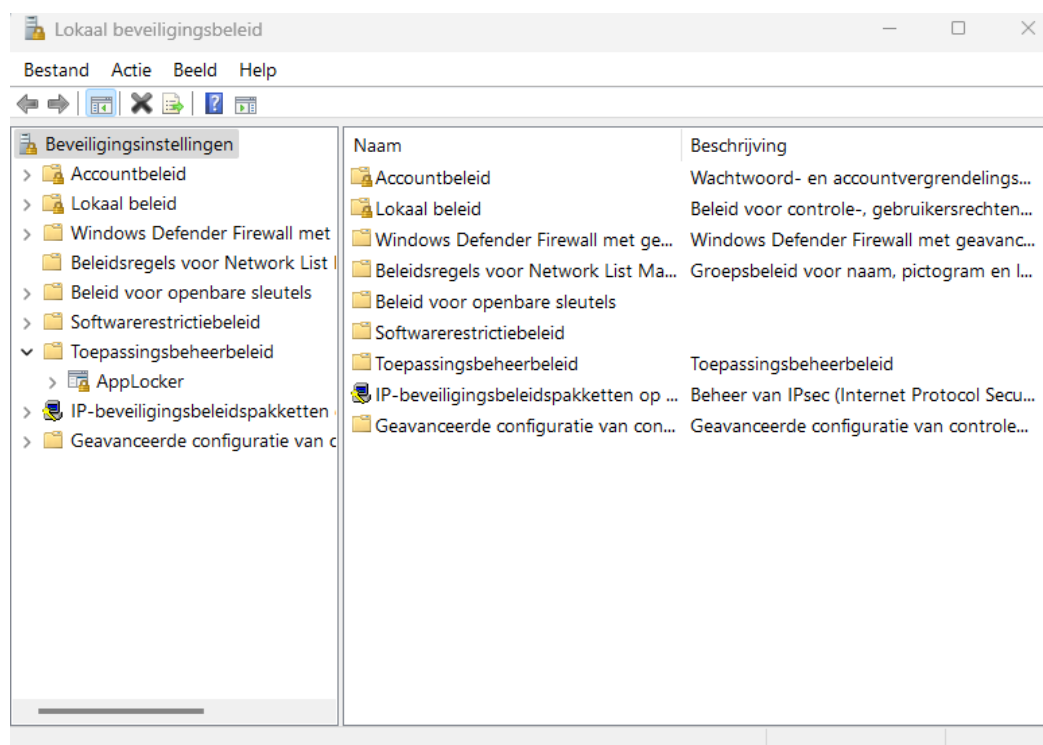
Zoals vermeld ga ik een uitleg geven over de werking van Applocker, grotendeels omdat dit de duidelijkste methode is maar ook omdat ik niet veel meer tools bij de hand heb om de andere methodes te laten zien.

Voordat je in Applocker zelf gaat instellen zijn er 2 belangrijke services die je eerst moet aanzetten, omdat dit anders niet gaat werken. Je zal eerst naar services moeten gaan door dit in de zoekbalk in te typen en daar ga je moeten zoeken naar "Application Identity". Het is heel belangrijk om deze service te starten want zonder gaat Application Control niet werken.



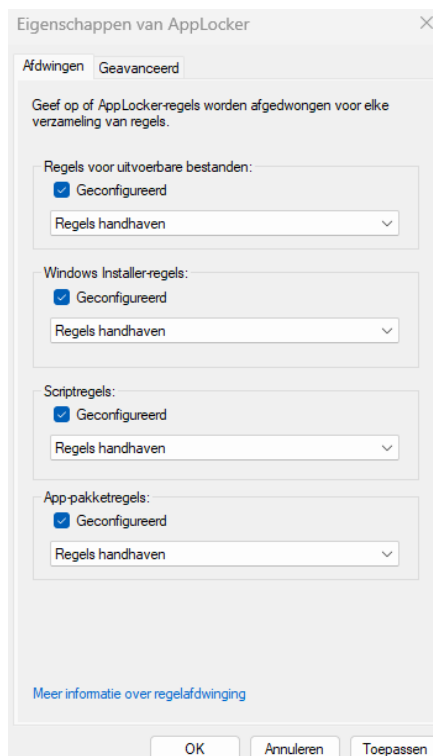
Afbeelding 7: services

Hierna ga je de GUI van Applocker zelf opendoen, dit doe je door eerst win + r in te geven en daar “secpol.msc” in uit te voeren. Eenmaal daar zal je de folder “Toepassingsbeheerbeleid moeten openen en met de rechtermuisklik op Applocker naar de properties gaan hiervan.



Afbeelding 8: beleidsportaal

In het venster dat nu tevoorschijn is gekomen ga je moeten zien dat alles van het eerste tabblad is aangevinkt. Voor de rest hoef je hier niets in te doen. Je krijgt hier de optie om te kiezen uit mogelijkheden, “Regels handhaven” en “Alleen controle”. Voor ons experiment laten we dit gewoon staan op “Regels handhaven”. Het verschil tussen deze twee mogelijkheden is dat bij “Regels handhaven” ook daadwerkelijk de regels gevolgd worden die je instelt. Dus als je instelt om een app te blokkeren dan word die ook geblokkeerd. In tegenstelling tot “Alleen controle” gaat dit enkel opvolgen dat je regels werken maar gaat dit niet blokkeren, enkel loggen zonder dat de eindgebruiker hier iets van ervaart. Dit word vooral gebruikt als je een nieuw beleid wilt maken en eerst wilt zien of dit gaat werken vooraleer je dit in het netwerk zet.



Afbeelding 9: Applocker properties

Hierna ga je de tab van Applocker openklikken en ga je naar “Executable rules”, hier zullen alle regels in komen te staan die je gaat aanmaken. Zoals je zal zien gaat dit nog leeg zijn omdat je natuurlijk nog niets ingesteld zal hebben gehad. Maar wat hier ook belangrijk zal zijn is dat je met de rechter muisklik op “Executable rules” eerst nog “Automatically generate rules” zal moeten uitvoeren. Dit gaat drie rules aanmaken voor de administrator dat die wel alles kan uitvoeren en de block rules dus niet voor hem tellen. Zodat je de administrator nergens voor kan uitsluiten.

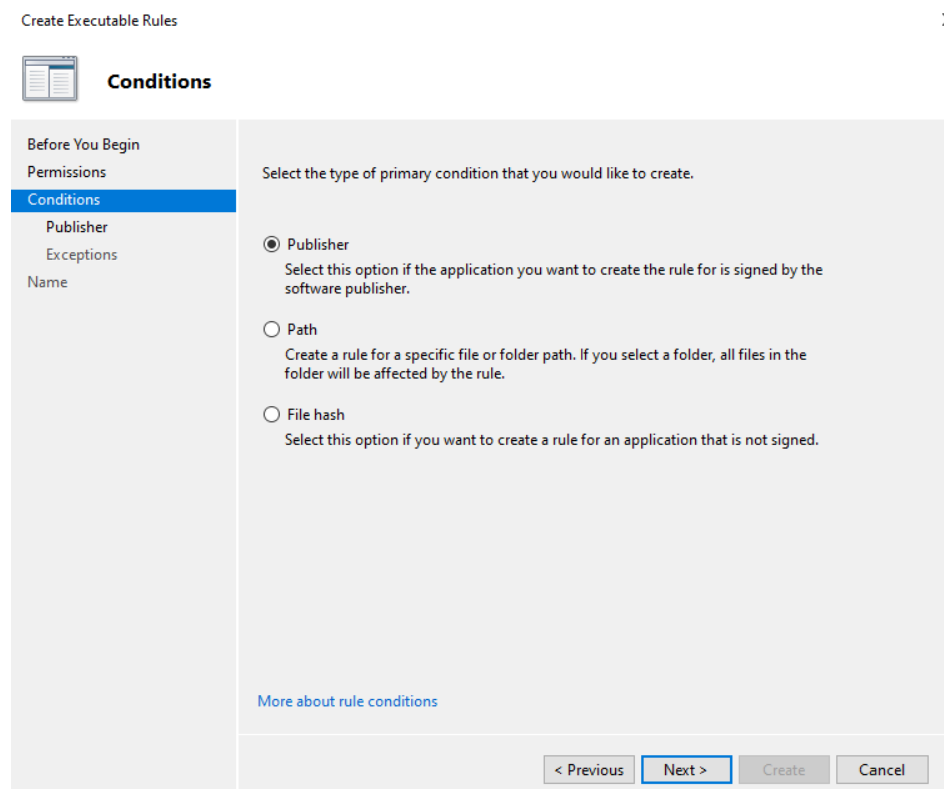
5.2 Rules aanmaken

Nu je al het voorbereidende werk gedaan hebt kunnen we beginnen aan het uiteindelijke doel van dit project en dat is het aanmaken van rules om bepaalde apps niet te kunnen gebruiken.

Om je regel aan te maken ga je net zoals hiervoor op “Executable rules” klikken en ga je naar “Create New Rule”. Eerst krijg je een pagina met een kleine toelichting maar hier hoeft je niks te doen en kan je eventueel op skip aanduiden zodat dit de volgende keer automatisch word overgeslagen. Op de volgende pagina moet je kiezen of je het wilt toelaten of blokkeren, maar wij gaan nu voor dit voorbeeld kiezen om te blokkeren. Je kan ook ineens toelichten voor welke user of groep deze rule moet dienen. Standaard staat dit op “Everyone”.

Nu heb je drie opties waar je uit kan kiezen:

- Publisher
- Path
- File hash



Create Executable Rules

Conditions

Before You Begin
Permissions
Conditions
Publisher
Exceptions
Name

Select the type of primary condition that you would like to create.

☒ **Publisher**
Select this option if the application you want to create the rule for is signed by the software publisher.

☐ **Path**
Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.

☐ **File hash**
Select this option if you want to create a rule for an application that is not signed.

[More about rule conditions](#)

< Previous Next > Create Cancel

Afbeelding 10: Conditions

5.2.1 publisher

als je een gesigneerde applicatie wilt blokkeren of toelaten dan is deze optie het handigste. Hiermee duid je gewoon de applicatie aan die je wilt hebben en word het geblokkeerd via het certificaat. En zo kunnen dus ook andere applicaties geblokkeerd worden die hetzelfde certificaat gebruiken.

5.2.2 Path


Deze optie gaat het beste zijn als je een map hebt waar verschillende applicaties instaan die je allemaal wilt blokkeren.

5.2.3 File hash

Dit werkt zoals de naam zegt op de hash van het bestand. Dit is een goede optie als je één specifieke app wilt hebben en ook enkel die versie van het bestand. Maar als de app bijvoorbeeld geupdate word dan krijgt die een andere hash en gaat deze regel ook niet meer werken.

Ik ga voor dit voorbeeld gebruik maken van de publisher optie. Nu je op de volgende pagina bent kan je zien dat je nu de applicatie kan gaan aanduiden dat je wilt hebben. Je kan hier gewoon heel handig de browse functie gebruiken en zo zoeken naar jouw applicatie. Wat hier nu wel heel belangrijk is, is dat je de slider op “File name” zet in de plaats van “File version”. Dit is omdat als je dit laat staan gaat hij die versie vergelijken maar zoals bij de functie “File hash” van daarnet gaat dit dus niet meer werken na bijvoorbeeld een update. Als je het op “File name” zet dan gaat hij de naam vergelijken en de naam blijft meestal altijd hetzelfde.

Create Executable Rules ×

**Publisher**

Before You Begin

Permissions

Conditions

Publisher

Exceptions

Name

Browse for a signed file to use as a reference for the rule. Use the slider to select which properties define the rule; as you move down, the rule becomes more specific. When the slider is in the any publisher position, the rule is applied to all signed files.

Reference file:

Any publisher

Publisher: O=SIMON TATHAM, S=CAMBRIDGESHIRE, C=GB

Product name: PUTTY SUITE

File name: PUTTY

File version: *

☐ Use custom values

< Previous

Next >

Create

Cancel

Afbeelding 11: Applicatie kiezen

Op de volgende pagina ga je exceptions moeten kiezen, maar dit laten we gewoon leeg en klik je op next.

The screenshot shows a window titled 'Create Executable Rules' with a close button (X) in the top right corner. On the left is a sidebar with a tree view containing: 'Before You Begin', 'Permissions', 'Conditions', 'Publisher', 'Exceptions' (highlighted in blue), and 'Name'. The main area is titled 'Exceptions' and contains the following text: 'To add an exception, select the type of exception and then click Add. Exceptions are optional and allow you to exclude files that would normally be included in the rule. To continue configuring this rule without adding an exception, click Next.' Below this, the 'Primary condition' is listed as 'PUTTY, in PUTTY SUITE, from O=SIMON TATHAM, S=CAMBRIDGESHIRE, C=GB'. There is an 'Add exception:' section with a dropdown menu currently showing 'Publisher'. Below that is an 'Exceptions:' section containing a table with two columns: 'Exception' and 'Type'. The table is currently empty. To the right of the table are three buttons: 'Add...', 'Edit', and 'Remove'. At the bottom of the window are four buttons: '< Previous', 'Next >' (highlighted with a blue border), 'Create', and 'Cancel'.

Op de laatste pagina kan je de naam instellen op de naam die je zelf wilt. Hier kan je natuurlijk het beste een duidelijke naam voor kiezen dat je achteraf nog weet waarvoor de rule dient en dan klik je op create.

Nu dat de rule aangemaakt is komt deze bij in de lijst van alle rules te staan en kan je gaan testen of je rule werkt. Wat ook belangrijk is om te weten is dat App control pas in werking gaat na de eerste opstart. Dus als je wilt testen kan je best de computer opnieuw opstarten en inloggen met de user waarvoor de rule is aangemaakt.

6 Panopto video

Via de link hieronder vind je mijn video die ik heb opgenomen voor de hands-on experiment van dit onderwerp

<https://ap.cloud.panopto.eu/Panopto/Pages/Viewer.aspx?id=2edeac80-324a-4c5a-8d71-b2ed012915f3>

7 Logboek

Datum	Activiteit	Tijd
20/03/2025	Opzoeken over het onderwerp	4 uur
29/03/2025	Opzoeken over het onderwerp	3 uur
02/04/2025	Template maken en voorwoord schrijven	1 uur
04/04/2025	Opzoeken en eerste deel schrijven	3 uur
06/04/2025	Opzoeken en schrijven van wat het is	4 uur
08/04/2025	Opzoeken en schrijven van de werking	3 uur
09/04/2025	Begrijpen en schrijven van de werking	4 uur
15/05/2025	Systemen leren begrijpen	5 uur
21/05/2025	Schrijven van nieuwe info	2 uur
22/05/2025	Praktische werking uitzoeken	4 uur
23/05/2025	Info bijwerken en opzoeken en praktische werking	4 uur
27/05/2025	Schrijven van praktische werking	2 uur
28/05/2025	Uitgebreidere teksten schrijven	5 uur
29/05/2025	Uitgebreidere teksten schrijven	3 uur
30/05/2025	Hands-on experiment uittesten	2 uur
30/05/2025	Video opnemen	30 min

8 Afbeeldingen

Afbeelding 1: Microsoft Defender Application Control.....	2
Afbeelding 2: foutmelding.....	4
Afbeelding 3: WDAC Wizard.....	5
Afbeelding 4: AppLocker	7
Afbeelding 5: Powershell voorbeeld	8
Afbeelding 6: Microsoft Intune Portaal	9
Afbeelding 7: services	12
Afbeelding 8: beleidsportaal.....	13
Afbeelding 9: Applocker properties.....	14
Afbeelding 10: Conditions	15
Afbeelding 11: Applicatie kiezen	17

9 Bibliografie

Basics of deploying windows applocker using Intune. (sd). Opgehaald van youtube:
<https://www.youtube.com/watch?v=3vncjM2Vk-o>

Blocking an application with group policy. (sd). Opgehaald van youtube:
<https://www.youtube.com/watch?v=Tn0AulzbP6U>

Microsoft. (2024, december 16). *Windows Defender Application Control management with Configuration Manager.* Opgehaald van <https://learn.microsoft.com/en-us/intune/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager>

Microsoft. (2025, oktober 3). *Application Control for Windows.* Opgehaald van <https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/appcontrol>

Microsoft. (sd). *Veelgestelde vragen over Smart App Control.* Opgehaald van <https://support.microsoft.com/nl-nl/windows/veelgestelde-vragen-over-smart-app-control-285ea03d-fa88-4d56-882e-6698afdb7003#:~:text=Hoe%20werkt%20Smart%20App%20Control,Smart%20App%20Control%20deze%20uitvoeren.>

Windows Applocker basics. (sd). Opgehaald van youtube:
<https://www.youtube.com/watch?v=xVVgXnorpvA>