TLP:GREEN

OR-8 CONFIGURATIEHANDLEIDING

Monitoring & Detectie – SOC Operational Readiness – **Application Control (WDAC)**

Best Practice versie 1.2

Complexiteit document

Eenvoudig

Samenwerken maakt

DIGITAAL

VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot de supplychain, netwerken, systemen en (gevoelige) informatie.

De wereld van cyberdreigingen verandert snel en vraagt om gezamenlijke inspanning om weerbaar te zijn. Dit vraagt om samen te werken aan breder toegepaste én verbeterde SOC-dienstverlening. Het programma Versterken SOC Stelsel Rijk (VSSR) is opgezet om hieraan bij te dragen.

Een belangrijk onderdeel van SOC-diensten zijn de monitoring- en detectiediensten. Deze zijn erop gericht om een veelheid aan loggegevens en andere (meta-)datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie te analyseren, aggregeren en correleren. Monitoring en detectiesystemen kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan.

Om een SOC effectief en doelmatig in te zetten is het noodzakelijk dat er een aantal onderwerpen binnen een organisatie zijn ingericht. VSSR levert diverse producten die rijksorganisaties ondersteunen bij het inrichten van een SOC en de daarvoor benodigde randvoorwaarden.

Achtergrond

VSSR levert verschillende kennisproducten. Dit document maakt onderdeel uit van een set van miniproducten die rijksorganisaties helpt om een aantal SOC operationele randvoorwaarden in te richten.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor Windows IT-beheerders, Systeemeigenaren, IT-Assetmanagers, Uitbestedingsmanagers, Security vertegenwoordigers en functionarissen betrokken bij informatiebeveiliging.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	19-03-2025	Initiële versie
V1.1	03-11-2025	Toevoeging "Bijlage I – Configuratiestatus checklist"
V1.2	07-07-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Checklist basisbeveiliging (OR-5)	Zie "Checklist basisbeveiliging ..(OR-5)" onder SOC Operational Readiness (Configuratie & Logging)
Generiek implementatieplan voor OR-6 t/m OR-9	Zie "Generiek implementatieplan" onder Platform/Applicatie Hardening & Malware bescherming (OR-6 t/m OR-9). Onderdeel van SOC Operational Readiness (Configuratie & Logging)
Microsoft WDAC Documentatie	https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/
Microsoft Security baseline	https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

Term	Omschrijving
Windows Defender Application Control (WDAC)	Onderdeel van Windows 10/11 Enterprise waarmee applicaties alleen mogen draaien als ze aan vooraf gedefinieerde policies voldoen.
Audit Mode	WDAC-modus waarbij potentiële blokkades worden gelogd, maar niet daadwerkelijk worden tegengehouden.
Enforce Mode	WDAC-modus waarbij niet-toegestane applicaties daadwerkelijk worden geblokkeerd.
Base Policy	De hoofdbeleidsregel voor WDAC, waarin de meeste beveiligingsinstellingen gedefinieerd staan.
Supplemental Policy	Aanvullend beleid dat de Base Policy uitbreidt met extra toegestane of geblokkeerde applicaties.
Multiple Policy Format	WDAC-formaat voor het gebruik van meerdere, flexibele beleidsregels (Base en Supplemental).
UMCI (User Mode Code Integrity)	Beschermingslaag die ook code in gebruikersmodus controleert.

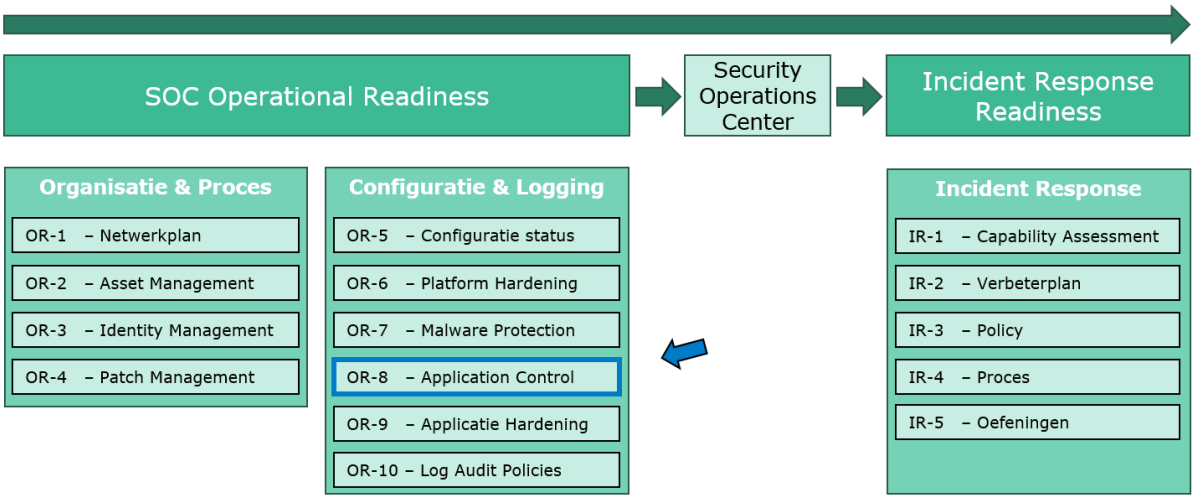
Ter verduidelijking van de overige terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

2 Context miniproducten

Dit document maakt onderdeel uit van de SOC Readiness Assistance **miniproducten**. De SOC Readiness Assistance miniproducten ondersteunen uw organisatie bij de voorbereidingen die nodig zijn voor het optimaal benutten van een SOC(-dienst). Deze producten hebben een samenhangende opbouw maar kunnen ook los van elkaar worden gebruikt. De producten zijn in drie groepen te verdelen:

1) **Organisatie & Proces:** Helpt bij het inrichten van processen met als doel het SOC van de juiste informatie te voorzien om goed te kunnen monitoren.
2) **Configuratie & Logging:** Helpt bij het inrichten van basisbeveiliging met als doel om beter beschermd te zijn en de juiste logdata bij een SOC aan te kunnen leveren.
3) **Incident Response:** Met behulp van monitoring & Detectie zal een SOC security melding genereren. De Incident Response producten helpen bij het inrichten van de opvolging van deze meldingen binnen uw organisatie.

Onderstaande weergave toont dit document als onderdeel van **Configuratie & Logging** in het VSSR-Minipoducten raamwerk.



Figuur 1 - Dit document als onderdeel van het VSSR-Miniproducten raamwerk

De twee productgroepen behorende bij *SOC Operational Readiness* bestaan telkens uit een vergelijkbare set document die in figuur 1 per groep zijn weergegeven. Niet elk product bestaat uit exact de zelfde componenten maar veelal wordt de zelfde structuur gebruikt waarbij dit document de configuratiehandleiding is voor Application Control (OR-8), binnen **Configuratie & Logging**, behandelt.

3 Inleiding

Deze configuratiehandleiding biedt een praktische leidraad voor het opzetten van WDAC in een Windows End User computing-omgeving. Dit document richt zich op het toelaten en blokkeren van applicaties. Het beschrijft hoe u WDAC in audit mode inzet voor inzicht in huidig gebruik, hoe u daarna overstapt op enforce mode voor daadwerkelijke blokkade, en hoe u logging inricht om de gebeurtenissen te monitoren. Zo ontstaat een solide basisconfiguratie voor Application Control.

Deze handleiding biedt niet alleen een theoretisch overzicht van WDAC, maar ook een praktische benadering, gebaseerd op best practices en de tools die Microsoft beschikbaar stelt voor de configuratie, zoals de Microsoft Security Compliance Toolkit (MSCT).

Een belangrijk hulpmiddel binnen deze handleiding is de WDAC Wizard, een intuïtieve tool die het opstellen en beheren van WDAC-beleid vereenvoudigt. De Wizard biedt een visuele interface waarmee IT-beheerders eenvoudig beleidsregels kunnen configureren zonder complexe PowerShell-scripts of Groepsbeleid-instellingen (GPO) te hoeven schrijven.

3.1 Doel

Het doel van deze handleiding is om een praktisch stappenplan te bieden voor het configureren van een WDAC-beleid. Hierbij wordt toegelicht hoe u:

- WDAC installeert en configureert met de WDAC Wizard.
- Een basisbeleid opstelt dat aansluit bij de behoeften van kleine tot middelgrote organisaties.
- Logging en monitoring effectief inzet om de status van WDAC binnen de organisatie te volgen.

3.2 Wat is WDAC?

Windows Defender Application Control is een beveiligingstechnologie waarmee u bepaalt welke code op een systeem mag worden uitgevoerd. Wanneer WDAC correct is geconfigureerd, blokkeert het alle applicaties en scripts die niet expliciet zijn toegestaan. WDAC helpt organisaties zich te beschermen tegen verschillende aanvalsmethoden, waaronder:

- Malware en ransomware die vaak op systemen wordt uitgevoerd zonder dat gebruikers dit direct in de gaten hebben.
- Onbetrouwbare software, bijvoorbeeld afkomstig van onveilige websites of downloadlocaties.

3.3 Relatie met andere handleidingen

Deze handleiding richt zich uitsluitend op de configuratie van WDAC. Een aparte Implementatiehandleiding behandelt de stapsgewijze uitrol, testprocedures en beheerstrategieën. Het is raadzaam deze handleidingen in samenhang te gebruiken om zowel de technische inrichting als de organisatorische afstemming te borgen.

3.4 Leeswijzer

Dit document biedt een gedetailleerde handleiding voor het configureren van Windows Defender Application Control (WDAC). Het helpt IT-beheerders bij het beperken van ongeautoriseerde applicaties en het verhogen van de digitale weerbaarheid van organisaties.

Opbouw van het document:

- **Voorwoord & Inleiding:** Beschrijft de noodzaak van WDAC binnen een SOC-omgeving en legt uit hoe het helpt bij het beveiligen van systemen.
- **Basisprincipes van WDAC:** Uitleg over trustmodellen, signing en de randvoorwaarden voor een succesvolle implementatie.
- **Installatie van de WDAC Wizard**: Stap-voor-stap instructies voor het installeren en gebruiken van de WDAC-configuratietool.
- **Configuratie van het WDAC-beleid:** Gids voor het instellen van het juiste beleid, inclusief sjablonen en aangepaste regels.
- **Logging en Monitoring:** Overzicht van de logbestanden en event-ID's die helpen bij het monitoren van WDAC-activiteit.

4 Basisprincipes van Windows Defender Application Control (WDAC)

WDAC vertegenwoordigt een fundamentele verschuiving in Windows-beveiliging, van een reactieve naar een proactieve benadering. Als onderdeel van Windows Enterprise biedt het een policy-gedreven methode om applicatie-uitvoering te controleren. In tegenstelling tot traditionele antivirusprogramma's die reageren op bekende dreigingen, werkt WDAC preventief door alleen goedgekeurde code toe te staan.

Belangrijke kenmerken van WDAC zijn:

- Kernel-niveau bescherming tegen ongeautoriseerde code-uitvoering
- Flexibele beleidsopties voor verschillende beveiligingsniveaus
- Integratie met moderne Windows-beveiligingsfuncties
- Ondersteuning voor zowel lokaal als gecentraliseerd beheer

In moderne IT-omgevingen, vooral met Microsoft 365 E3/E5 licenties, wordt WDAC vaak aanbevolen als primaire applicatie-beheersingsoplossing.

4.1 Trustmodellen en Signing

De effectiviteit van WDAC is gebaseerd op verschillende vertrouwensmechanismen die de legitimiteit van code verifiëren. Het systeem maakt gebruik van code signing certificaten om digitale handtekeningen van bekende software-uitgevers te valideren. Dit proces omvat automatische validatie van Microsoft's kernel-mode code-signing vereisten en biedt tevens ondersteuning voor organisatie-specifieke certificaten.

Device Guard signing voegt hier een extra dimensie aan toe door organisaties in staat te stellen hun intern ontwikkelde applicaties te ondertekenen. Deze functionaliteit integreert naadloos met enterprise certificaatbeheer en biedt flexibele opties voor het beheer van vertrouwde uitgevers. De integratie met Microsoft's Intelligent Security Graph voegt hier een dynamische component aan toe door continue updates van bekende, vertrouwde software te leveren en nieuwe applicaties automatisch te categoriseren op basis van hun reputatie.

- **Code Signing Certificaten**
  - Verificatie van digitale handtekeningen van bekende software-uitgevers
  - Automatische validatie van Microsoft's kernel mode code signing vereisten
- **Ondersteuning voor organisatie-specifieke certificaten**
  - Device Guard Signing
  - Mogelijkheid om intern ontwikkelde applicaties te ondertekenen
- **Integratie met enterprise certificaatbeheer**
  - Flexibele opties voor het beheer van vertrouwde uitgevers
  - Microsoft's Intelligent Security Graph
- **Reputatie-gebaseerde beoordeling van applicaties**
  - Continue updates van bekende, vertrouwde software
  - Automatische categorisering van nieuwe applicaties

4.2 Randvoorwaarden

Om de configuraties in deze handleiding te kunnen implementeren, moet aan een aantal essentiële randvoorwaarden worden voldaan:

- **U beschikt** over Windows 10/11 Enterprise of Education
- **U beschikt** over voldoende beheerdersrechten voor de configuratie
- **U maakt** gebruik van Intune voor centraal beheer van uw systemen.
- **U heeft** de WDAC Wizard gedownload en geïnstalleerd (van de officiële Microsoft-website)
- **U heeft** basiskennis van PowerShell (optioneel, maar aanbevolen)
- **U heeft** een stabiele netwerkconnectiviteit (indien u extra online-beveiligingsfuncties gebruikt)
- **U zorgt** ervoor dat alle Windows-systemen up-to-date zijn met de laatste patches en updates

Let op: Indien u Microsoft Intune gebruikt voor gecentraliseerd beheer, kunt u de in dit document beschreven WDAC-beleidsregels via Intune uitrollen.

5 Installatie en configuratie van de WDAC Wizard

Een effectieve implementatie van Windows Defender Application Control (WDAC) vereist een goed doordachte configuratie. Binnen Intune-beheerde omgevingen wordt WDAC doorgaans centraal uitgerold via Intune-beleidsregels en niet per afzonderlijk systeem met een wizard. Toch kan de WDAC Wizard nuttig zijn bij het initiëren van een WDAC-configuratie, het testen van beleidsregels en het genereren van een basisbeleid dat vervolgens via Intune kan worden uitgerold.

De WDAC Wizard is vooral geschikt voor kleinere en middelgrote organisaties of voor beheerders die eerst een testbeleid willen opstellen voordat zij dit op grote schaal implementeren. Voor grote organisaties met een uitgebreide IT-omgeving is het gebruik van Intune de aanbevolen methode voor centrale uitrol en beheer.

5.1 Waarom kiezen voor de WDAC Wizard?

De WDAC Wizard is een gebruiksvriendelijk hulpprogramma dat speciaal is ontworpen om het opstellen en beheren van WDAC-beleid te vereenvoudigen. Hoewel het ook mogelijk is om WDAC volledig via PowerShell of via groepsbeleid (GPO) te configureren, kan de Wizard het volgende bieden:

- **Visuele interface:** U kunt de belangrijkste instellingen aanwijzen en selecteren in plaats van PowerShell-commando's uit het hoofd te leren. Dit verkleint de kans op configuratiefouten.
- **Snellere leercurve:** Zeker voor kleinere organisaties met een beperkt IT-team is de Wizard laagdrempeliger dan uitgebreide scripts of complexe groepsbeleidsinstellingen.
- **Flexibele beleidsopties:** U kunt gemakkelijk schakelen tussen een Base Policy of een Supplemental Policy en de Wizard begeleidt u bij het kiezen van de juiste instellingen, zoals Signed and Reputable Mode.
- **Snelle aanpassingen:** In omgevingen waar weinig capaciteit is voor continu beheer, maakt de Wizard het eenvoudig om bestaande WDAC-configuraties te wijzigen of aan te vullen.

Kortom, de WDAC Wizard biedt een balans tussen krachtige configuratiemogelijkheden en gebruiksgemak, waardoor het een ideale keuze is voor kleine tot middelgrote organisaties die snel en zonder al te veel complexiteit willen starten met WDAC.

5.2 Installatie van WDAC Wizard

De WDAC Wizard wordt niet op alle systemen geïnstalleerd. In plaats daarvan wordt deze tool gebruikt op een beheerderssysteem of testapparaat om een initieel WDAC-beleid te genereren en te valideren voordat het wordt uitgerold via Microsoft Intune.

5.3 Installatieprocedure

- Selecteer een geschikt testsysteem
  - Installeer de WDAC Wizard op een beheerderssysteem met Windows 10/11 Enterprise of een testapparaat dat representatief is voor de bedrijfsomgeving (Denk aan applicaties die vanuit het bedrijf gebruikt worden).
  - Dit systeem moet niet in productie worden gebruikt, maar dient om het beleid te ontwikkelen en testen.
- Download de WDAC Wizard
  - Verkrijg de tool via de officiële Microsoft-website. (Download pagina)
  - Zorg ervoor dat het systeem voldoet aan de minimale vereisten voor de WDAC Wizard, zoals een compatibele Windows-versie en voldoende beheerdersrechten.

- Voer de installatie uit
  - Gebruik administrator mode om de Wizard te installeren.
  - Volg de instructies van de installatiewizard en accepteer de standaardinstellingen.
  - Controleer de functionaliteit
- Open de WDAC Wizard en verifieer dat alle functies correct werken.
  - Zorg ervoor dat het systeem toegang heeft tot alle benodigde certificaten, applicaties en loggegevens die nodig zijn om het WDAC-beleid effectief op te bouwen.

Belangrijk: Waarom niet op alle systemen installeren?

De WDAC Wizard is een configuratietool, geen component die constant nodig is op eindgebruikerssystemen. Het gegenereerde WDAC-beleid wordt geëxporteerd als XML-bestand en vervolgens via Intune uitgerold naar alle beheerde apparaten.

Installatie op elk afzonderlijk systeem is onnodig en niet schaalbaar; in plaats daarvan moet centraal beheer via Intune worden toegepast.

6 Configuratie van het WDAC-Beleid (WDAC Wizard)

Een goed geconfigureerd WDAC-beleid is essentieel voor het effectief afdwingen van applicatiecontrole binnen een organisatie. In dit hoofdstuk wordt stap voor stap uitgelegd hoe een WDAC-beleid wordt opgezet, aangepast en geïmplementeerd.

We beginnen met het kiezen van het juiste beleidstype en basissjabloon, gevolgd door de configuratie van specifieke beleidsregels. Daarbij worden verschillende methoden besproken om applicaties toe te staan of te blokkeren, zoals het gebruik van bestands-hashes, uitgeverscertificaten en bestandslocaties. Daarnaast wordt uitgelegd hoe het beleid veilig kan worden opgeslagen en uitgerold naar de organisatie, bijvoorbeeld via Microsoft Intune.

Een doordachte configuratie is cruciaal om een balans te vinden tussen beveiliging en werkbaarheid. Daarom wordt in dit hoofdstuk ook aandacht besteed aan best practices voor beleidsbeheer en hoe WDAC zo efficiënt mogelijk kan worden ingezet zonder onnodige verstoringen voor eindgebruikers.

6.1 Het juiste beleidstype kiezen

Bij het opzetten van WDAC is de keuze van het juiste beleidstype een cruciale eerste stap. De WDAC Wizard ondersteunt twee hoofdformaten: het Multiple Policy Format en het Single Policy Format. Voor de meeste organisaties wordt het Multiple Policy Format aanbevolen vanwege de grotere flexibiliteit die het biedt voor toekomstige aanpassingen. Dit format maakt incrementele beleidsuitbreiding mogelijk en ondersteunt verschillende gebruikersscenario's binnen de organisatie.

Het Single Policy Format kan geschikt zijn voor kleinere omgevingen waar eenvoud in beheer voorop staat. Dit format is direct toepasbaar zonder aanvullende configuratie, maar biedt minder flexibiliteit voor toekomstige aanpassingen. De keuze tussen deze formats hangt af van de specifieke behoeften en groeiverwachtingen van uw organisatie.

6.2 Het basisbeleidstype bepalen

- Kies **Base Policy** als u voor de eerste keer een volledig nieuw WDAC-beleid maakt.
- Kies **Supplemental Policy** alleen als u een bestaand Base Policy wilt uitbreiden en al een basisbeleid hebt.

Opmerking: Heeft u nog geen bestaande Base Policy, dan is de standaardkeuze altijd een Base Policy.

6.3 Een effectief basissjabloon kiezen

De WDAC Wizard biedt diverse sjablonen voor de basisregels. De aanbeveling voor kleine tot middelgrote organisaties is doorgaans:

Signed and Reputable Mode: Staat applicaties toe die digitaal ondertekend zijn door vertrouwde uitgevers en die op basis van Microsoft's Intelligent Security Graph (ISG) als 'reputable' worden beschouwd.

Dit biedt een goede balans tussen beveiliging en bruikbaarheid, omdat het al veelgebruikte en betrouwbare software toestaat, terwijl onbekende of niet-ondertekende applicaties worden geblokkeerd.

6.4 Configureren van de beleidsregels

Een effectief WDAC-beleid combineert algemene beveiligingsinstellingen met specifieke regels voor uw organisatie. De basis wordt gevormd door een aantal kerncomponenten die de algemene beveiliging waarborgen:

Script Enforcement: Controleert de uitvoering van scripts in uw omgeving. Houd deze functie ingeschakeld tenzij uw organisatie specifieke, niet-ondertekende scripts nodig heeft.

User Mode Code Integrity: Biedt extra bescherming tegen schadelijke code in gebruikersmodus, een essentiële beveiligingslaag voor moderne systemen.

Intelligent Security Graph integratie: Gebruikt Microsoft's real-time informatie over applicatiebetrouwbaarheid voor betere besluitvorming.

Naast deze basisinstellingen hebben organisaties vaak behoefte aan maatwerk voor specifieke applicaties of tools. WDAC biedt hiervoor drie typen aangepaste regels:

- File Hash Rules Deze regels bieden de meest nauwkeurige controle door bestanden te identificeren op basis van hun unieke hash-waarde. Ideaal voor kritieke applicaties waarbij u absolute zekerheid wilt over welk bestand wordt uitgevoerd. Houd er wel rekening mee dat elke software-update een nieuwe hash genereert, waardoor de regel moet worden bijgewerkt.
- File Path Rules Door te werken met bestandslocaties in plaats van specifieke bestanden bieden deze regels meer flexibiliteit. Ze zijn bijzonder nuttig in dynamische omgevingen waar software regelmatig wordt bijgewerkt. De keerzijde is dat een aanvaller mogelijk bestanden kan verplaatsen of hernoemen om de beveiliging te omzeilen.
- Publisher Rules Deze regels vertrouwen alle software van een specifieke uitgever. Ze zijn zeer efficiënt in beheer omdat ze automatisch nieuwe versies en updates toestaan van dezelfde uitgever. Gebruik deze regels alleen voor uitgevers die u volledig vertrouwt en evalueer regelmatig of dit vertrouwen nog gerechtvaardigd is.

Bij het configureren van uw WDAC-beleid is het belangrijk om deze verschillende regeltypen strategisch in te zetten. Begin met de kernbeveiligingsinstellingen als basis, en voeg daar alleen die aangepaste regels aan toe die echt noodzakelijk zijn voor uw bedrijfsvoering. Documenteer waarom elke aangepaste regel is toegevoegd en evalueer regelmatig of deze nog nodig is. Dit zorgt voor een balans tussen security en bruikbaarheid, waarbij de beveiliging zo sterk mogelijk blijft zonder de dagelijkse werkzaamheden te hinderen.

6.5 Het Beleid opslaan

Het zorgvuldig opslaan en documenteren van uw WDAC-beleid is essentieel voor effectief beheer op lange termijn. Begin met het kiezen van een duidelijke, beschrijvende bestandsnaam die de inhoud, datum en het doel van het beleid weerspiegelt. Documenteer vervolgens grondig welke configuratiekeuzes zijn gemaakt en waarom deze zijn gekozen. Het maken van back-ups van werkende configuraties voorkomt problemen bij toekomstige aanpassingen.

Een gedegen versiebeheer systeem helpt bij het bijhouden van wijzigingen en maakt het mogelijk om indien nodig terug te keren naar een eerdere, stabiele versie. Plan regelmatige evaluaties van het beleid om ervoor te zorgen dat het blijft aansluiten bij de veranderende behoeften van uw organisatie.

- **Kies** de gewenste locatie en bestandsnaam (bijv. 04022025_*WDAC_BasisBeleid.xml*).
- **Klik** op **Create Policy** om het beleid als XML-bestand op te slaan.
- Het **XMLbestand** is nu opgeslagen en gereed om uitgerold te worden via Intune.

6.6 Centraal beheer en uitrol met Intune

Microsoft Intune biedt een krachtige oplossing voor het centraal beheren van Windows-apparaten binnen uw organisatie. Door de integratie van WDAC (Windows Defender Application Control) met Intune kunt u beveiligingsbeleid effectief uitrollen en beheren.

Een WDAC-beleid kan aanzienlijke impact hebben op de werking van applicaties. Daarom wordt aangeraden om het beleid eerst in Audit Mode te implementeren en te testen op een kleine groep apparaten voordat het op grote schaal wordt afgedwongen (Enforce Mode).

Voordelen van uitrol via Intune:

- **Schaalbare implementatie** – In één keer WDAC-instellingen pushen naar alle Intune-beheerde apparaten.
- **Audit Mode voor veilige tests** – Test eerst zonder directe blokkades om compatibiliteitsproblemen vroegtijdig te detecteren.
- **Versiebeheer** – Beheer eenvoudig oude en nieuwe versies van het WDAC-beleid en draai wijzigingen terug indien nodig.
- **Compliance handhaven** – Controleer via Intune-rapportages of apparaten voldoen aan de WDAC-regels en ontvang meldingen bij afwijkingen.

6.7 Implementatie in Intune

Bij de implementatie van WDAC in Intune wordt aanbevolen om eerst Audit Mode te gebruiken op een beperkte testgroep, voordat het beleid op alle apparaten wordt toegepast.

Intune-portal openen

- Ga naar Intune en navigeer naar Devices > Configuration profiles.
- Klik op Create profile.

Platform en configuratie selecteren

- Kies Windows 10/11 als platform.
- Selecteer de Custom optie voor OMA-URI of scripts.

WDAC configureren (Audit Mode in testgroep)

- Upload het WDAC XML-bestand en zorg dat het beleid in Audit Mode staat, zodat acties worden gelogd zonder applicaties direct te blokkeren.
- Wijs het testbeleid toe aan een kleine pilotgroep (bijvoorbeeld IT-beheerders of testgebruikers die zijn geonboard naar Defender for Endpoint).

Test en valideer de impact

- Controleer Advanced Hunting logs in Microsoft Defender for Endpoint (DFE) om inzicht te krijgen in welke applicaties zouden worden geblokkeerd. (Zie hoofdstuk 7.2 voor uitleg)

Pas het beleid aan op basis van de bevindingen uit de testgroep. Worden in **Audit Mode** applicaties geregistreerd als geblokkeerd terwijl ze essentieel zijn voor bedrijfsprocessen? Dan moet het beleid worden herzien om deze applicaties expliciet toe te staan. Dit kan door uitzonderingen toe te voegen op basis van **file hash, publisher of pad**, zodat kritieke software niet onbedoeld wordt beperkt wanneer het beleid later in **Enforce Mode** wordt gezet.

Uitrol naar de volledige organisatie (Enforce Mode)

- Zodra het testbeleid is gevalideerd, kan **Audit Mode** worden omgezet naar **Enforce Mode**.
- **Breid de uitrol geleidelijk uit** naar de volledige organisatie om verstoringen te minimaliseren.
- Monitor via Defender for Endpoint en Intune-compliance rapportages of het beleid correct wordt toegepast.

7 Logging en Monitoring

Een goed geconfigureerd **Windows Defender Application Control (WDAC)**-beleid is pas effectief als het actief wordt gemonitord. Organisaties die via **Microsoft Intune** zijn aangesloten op **Microsoft Defender for Endpoint (DFE)** kunnen WDAC-logboeken centraal verzamelen en analyseren. Dit zorgt ervoor dat beheerders inzicht krijgen in geblokkeerde of toegestane applicaties en vroegtijdig misconfiguraties of ongewenste beperkingen kunnen identificeren.

7.1 Locatie van logboeken

Wanneer een apparaat is gekoppeld aan **Microsoft Intune** en geïntegreerd met **Microsoft Defender for Endpoint**, worden WDAC-logboekgegevens automatisch doorgestuurd naar DFE. Beheerders kunnen deze gegevens raadplegen via de **Advanced Hunting**-functie in het **Microsoft Defender Security Center** (*https://security.microsoft.com*).

7.2 Toegang tot WDAC-logs via Advanced Hunting

Om toegang te krijgen tot de WDAC-logs voor Hunting werkzaamheden:

1. Log in op Microsoft Defender Security Center.
2. Ga naar Hunting en kies Advanced Hunting.

Voer de volgende **Kusto Query Language (KQL)-query** uit om WDAC-gerelateerde gebeurtenissen te analyseren. te analyseren. Deze query maakt gebruik van loggegevens van alle **Intune-beheerde apparaten** die zijn gekoppeld aan **Microsoft Defender for Endpoint (DFE)**:

```
DeviceEvents
| where ActionType startswith "AppControl"
| project Timestamp, DeviceName, ActionType, FileName, InitiatingProcessAccountName
| order by Timestamp desc
```

Deze query toont **recent gedetecteerde WDAC-gebeurtenissen**, zoals geblokkeerde applicaties of scripts, inclusief details over apparaat, gebruiker en het exacte tijdstip van de gebeurtenis.

7.3 Relevante gebeurtenis-ID’s

WDAC-logboeken binnen Defender for Endpoint bevatten de volgende kerngebeurtenissen die belangrijk zijn voor monitoring:

- **3076** – Een applicatie zou worden geblokkeerd (Audit-modus).
- **3077** – Een applicatie zou worden toegestaan (Audit-modus).
- **3090** – Scriptbeveiliging heeft een script geblokkeerd (Audit-modus).
- **3091** – Scriptbeveiliging heeft een script toegestaan (Audit-modus).

Door deze gebeurtenissen te correleren, kunnen beheerders ongewenste blokkades detecteren en het beleid verfijnen voordat het in *Enforce Mode* wordt gezet.

7.4 Monitoring in een kleine/middelgrote organisatie

In kleinere en middelgrote organisaties kan WDAC-monitoring effectief worden uitgevoerd via Microsoft Defender for Endpoint (DFE). In plaats van handmatige controles op afzonderlijke apparaten, kunnen beheerders centraal inzicht krijgen in WDAC-gebeurtenissen via Advanced Hunting in het Microsoft Defender Security Center.

Voor een eerste implementatie is het aan te raden om regelmatig rapporten en logs te bekijken binnen DFE. Dit helpt bij het identificeren van geblokkeerde applicaties en het verfijnen van het WDAC-beleid zonder onnodige verstoringen voor eindgebruikers.

Bijlage I – Configuratiestatus checklist

Level	Configuration Control	Status
L1	WDAC in Audit Mode – Fundamental for visibility before full enforcement. (H 6.7)	
	WDAC Wizard Usage – Simplifies setup, great for smaller teams. (H 4 & 5)	
	Single Policy Format – Straightforward "one policy" approach. (H 6.1)	
L2	WDAC in Enforce Mode – Moves from visibility to real blocking. (H 6.6)	
	Script Enforcement – Adds coverage for scripts to block malicious code. (H 6.4)	
	File Path Rules – Adds flexible allow/block rules by folder path. (H 6.4)	
	Signed & Reputable Mode – Relies on digital signatures plus Microsoft ISG. (H 6.3)	
	Basic Code Signing Certificates – Trusts known third-party or MS certs. (H 4.1)	
L3	Multiple Policy Format – More complex layering of policies. (H 6.1)	
	User Mode Code Integrity (UMCI) - Extends code integrity checks to user mode. (H6.4)	
	File Hash Rules – Highly granular control at the hash level. (H 6.4)	
	Publisher Rules – Trust entire software publishers automatically. (H 6.4)	
	Device Guard Signing – Sign your in-house apps, advanced enterprise trust. (H 4.1)	
L4	Supplemental Policies – Extend base policies seamlessly for new scenarios. (H 6.2)	
	Integration with Intune – Centralized deployment/rollback at scale. (H 6.6)	
	Expanded Logging & Monitoring – Using DFE Advanced Hunting to monitor logs. (H 7)	
L5	Full Intelligent Security Graph Integration (H 6.3)	
	Ongoing Policy Refinement – Continuous improvement and frequent fine-tuning. (H7.4)	

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://www.ncsc.nl/vssr

info@ncsc.nl

vssr.info@minjenv.nl (Rijksoverheid)

Maart 2025