6 Months of WDAC on enforced mode - notes from the field

Thank you Sponsors

wpninjas.au

Microsoft

DEVICIE

About Jose

Role

CTO at Devicie

From

Brazil (Aussie for the last 10 years)

Blog

intune.tech

Certifications

Some here and there

Hobbies

Cycling
Squash
Reading technical stuff

Contact

jose@wpninjas.au

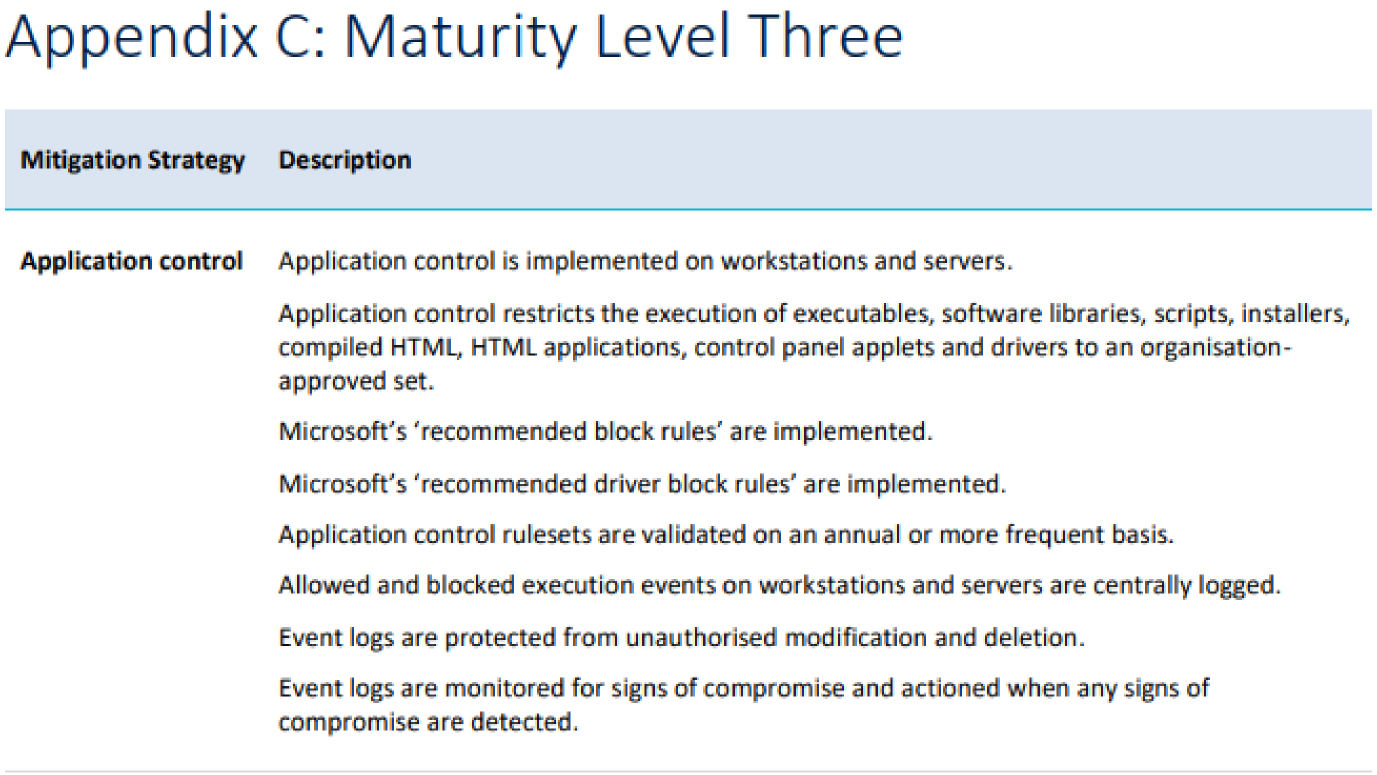
Agenda

- Why WDAC?
- What is WDAC?
- Pre-Requisites
- Intune Policy Options
- Tips & Tricks

Why WDAC?

Essential 8 number 1 Mitigation Strategy

Australian Cyber Security Centre

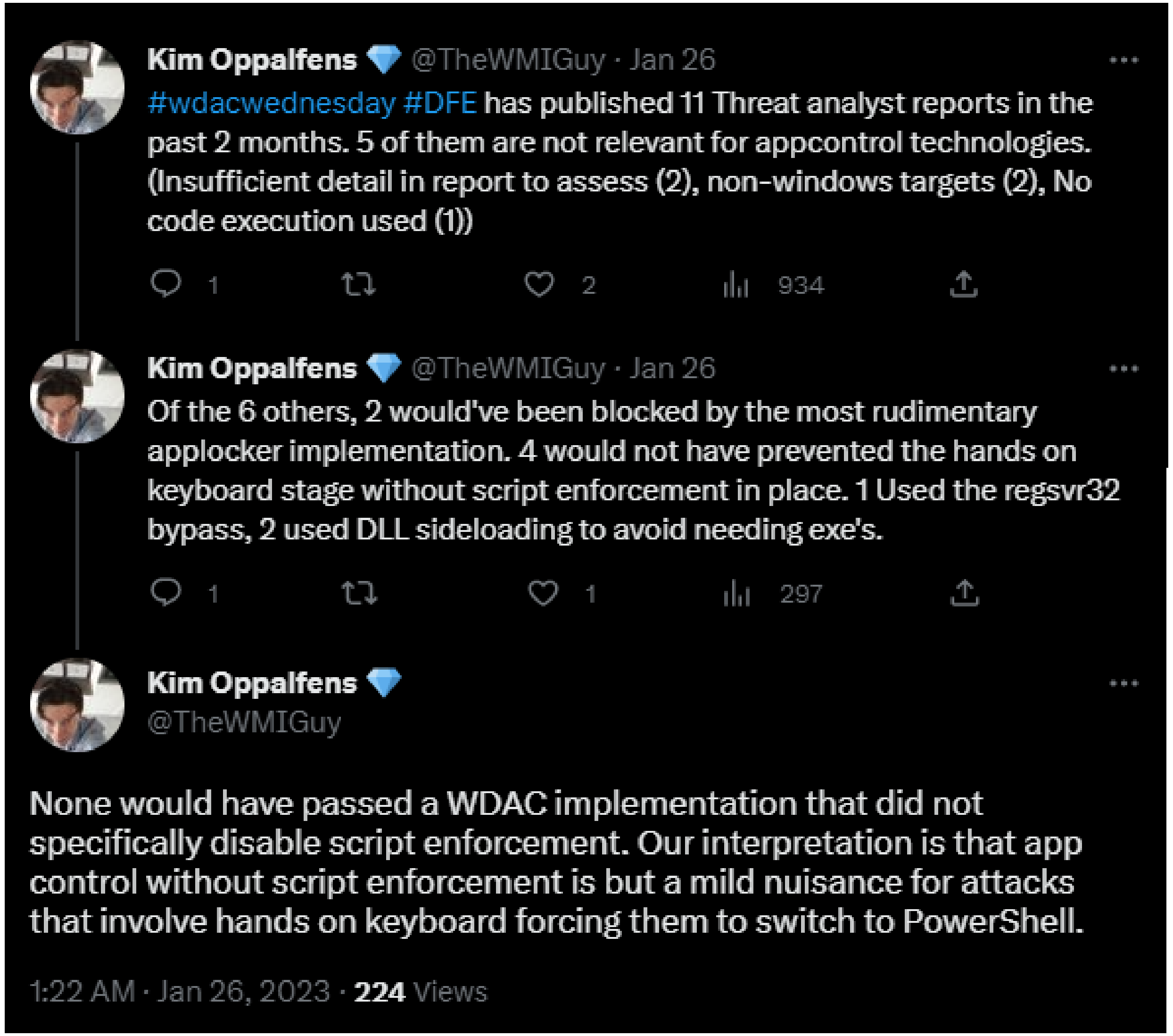


Appendix C: Maturity Level Three

Mitigation Strategy	Description
Application control	Application control is implemented on workstations and servers. Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers to an organisation-approved set. Microsoft's 'recommended block rules' are implemented. Microsoft's 'recommended driver block rules' are implemented. Application control rulesets are validated on an annual or more frequent basis. Allowed and blocked execution events on workstations and servers are centrally logged. Event logs are protected from unauthorised modification and deletion. Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.

PROTECT - Essential Eight Maturity Model (November 2022).pdf (cyber.gov.au)

Script Enforcement (Constrained Language Mode)



Kim Oppalfens @TheWMIGuy · Jan 26

#wdacwednesday #DFE has published 11 Threat analyst reports in the past 2 months. 5 of them are not relevant for appcontrol technologies. (Insufficient detail in report to assess (2), non-windows targets (2), No code execution used (1))

Kim Oppalfens @TheWMIGuy · Jan 26

Of the 6 others, 2 would've been blocked by the most rudimentary applocker implementation. 4 would not have prevented the hands on keyboard stage without script enforcement in place. 1 Used the regsvr32 bypass, 2 used DLL sideloading to avoid needing exe's.

Kim Oppalfens
@TheWMIGuy

None would have passed a WDAC implementation that did not specifically disable script enforcement. Our interpretation is that app control without script enforcement is but a mild nuisance for attacks that involve hands on keyboard forcing them to switch to PowerShell.

1:22 AM · Jan 26, 2023 · **224** Views

The year of WDAC

PowerShell Security - Friedrich Weinmann - PSConfEU 2022

What is WDAC?

Windows Defender Application Control

Windows Defender Application Control is designed to protect devices against malware and other untrusted software. It prevents malicious code from running by ensuring that only approved code, that you know, can be run.

File Rule Levels

- ~~Hash~~
- ~~FileName~~
- ~~FilePath~~
- ~~SignedVersion~~
- ~~Publisher~~
- ~~FilePublisher~~
- ~~LeafCertificate~~
- ~~PcaCertificate~~
- ~~RootCertificate~~
- ~~WHQL~~
- ~~WHQLPublisher~~
- ~~WHQLFilePublisher~~

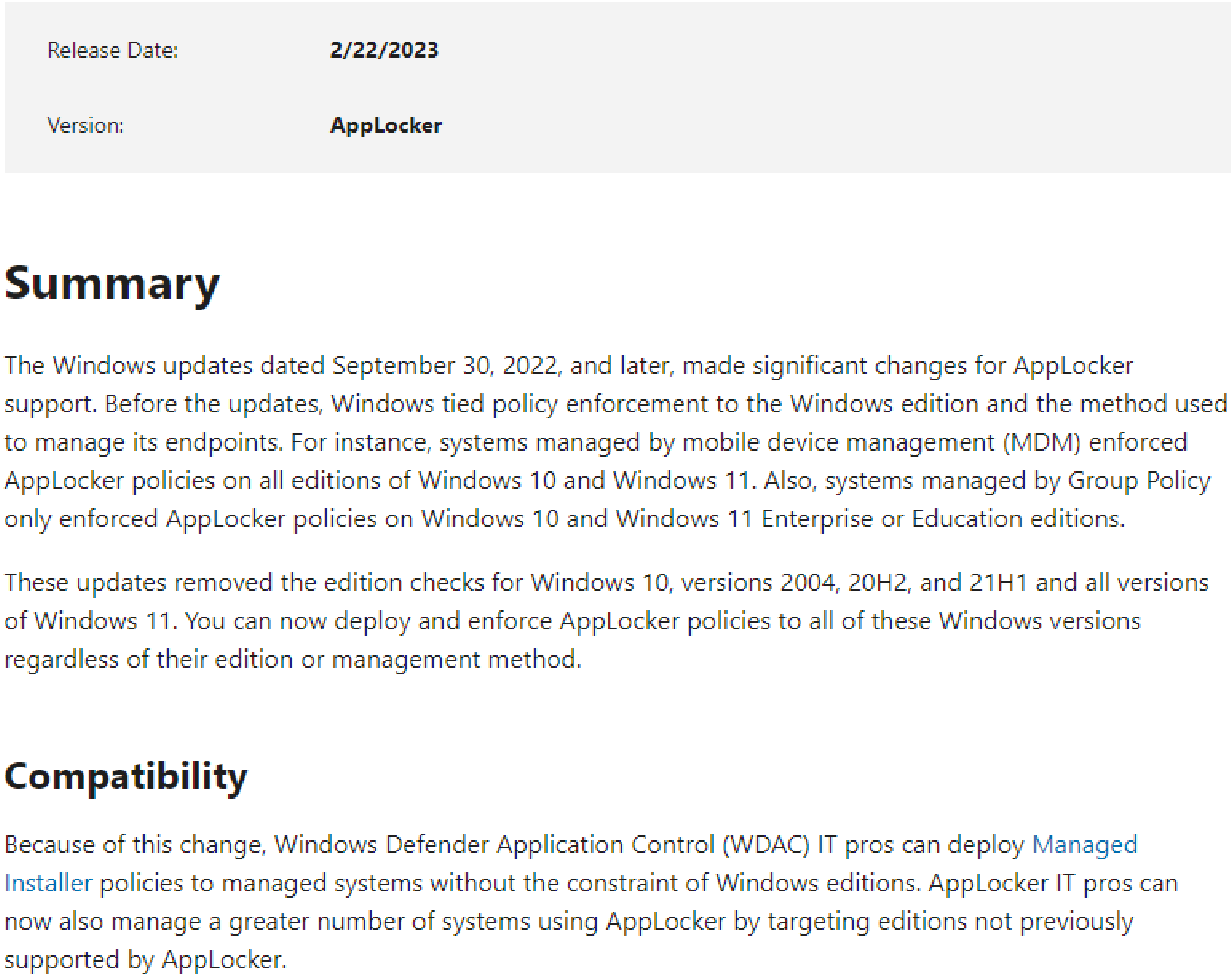
Managed Installer

Understand Windows Defender Application Control (WDAC) policy rules and file rules (Windows) | Microsoft Learn

Pre-Requisites

Pre-Requisites

- Intune
- ~~Windows 10, 11 Enterprise~~
- Microsoft Defender for Endpoint
- TIME
- Business Change Management



Release Date:	**2/22/2023**
Version:	**AppLocker**

Summary

The Windows updates dated September 30, 2022, and later, made significant changes for AppLocker support. Before the updates, Windows tied policy enforcement to the Windows edition and the method used to manage its endpoints. For instance, systems managed by mobile device management (MDM) enforced AppLocker policies on all editions of Windows 10 and Windows 11. Also, systems managed by Group Policy only enforced AppLocker policies on Windows 10 and Windows 11 Enterprise or Education editions.

These updates removed the edition checks for Windows 10, versions 2004, 20H2, and 21H1 and all versions of Windows 11. You can now deploy and enforce AppLocker policies to all of these Windows versions regardless of their edition or management method.

Compatibility

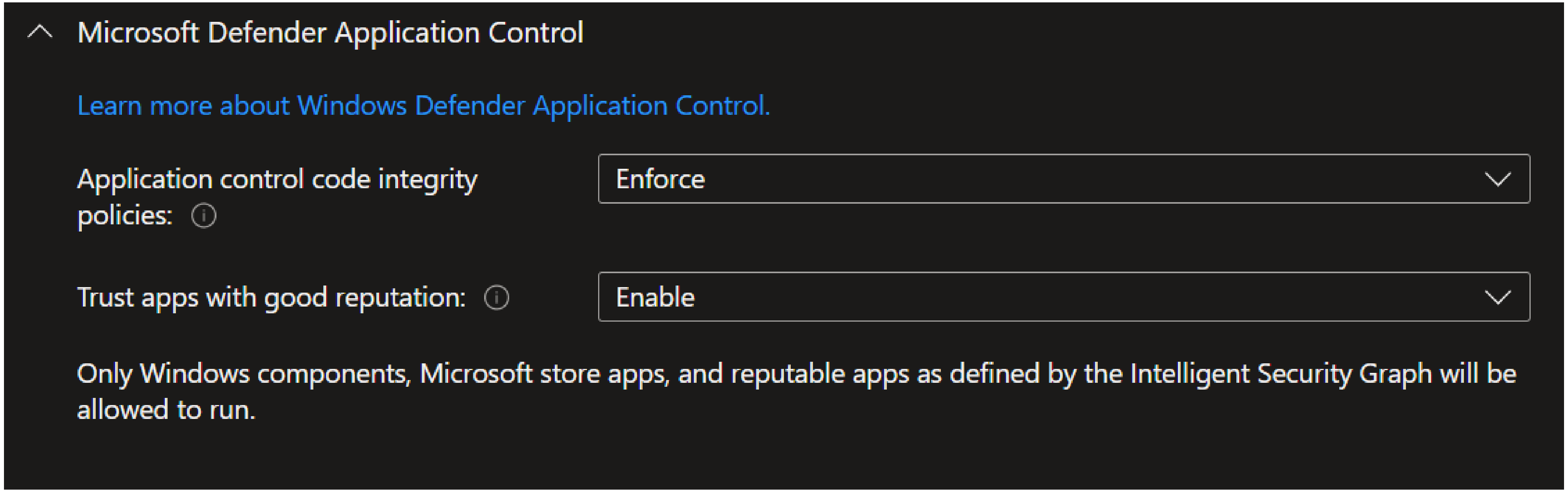
Because of this change, Windows Defender Application Control (WDAC) IT pros can deploy Managed Installer policies to managed systems without the constraint of Windows editions. AppLocker IT pros can now also manage a greater number of systems using AppLocker by targeting editions not previously supported by AppLocker.

KB5024351—Removal of Windows edition checks for AppLocker - Microsoft Support

Intune Policy Options

Intune Policies – built-in

- Windows components
- Third-party hardware and software kernel drivers
- Microsoft Store-signed apps
- [Optional] Reputable apps as defined by the Intelligent Security Graph (ISG)



Microsoft Defender Application Control

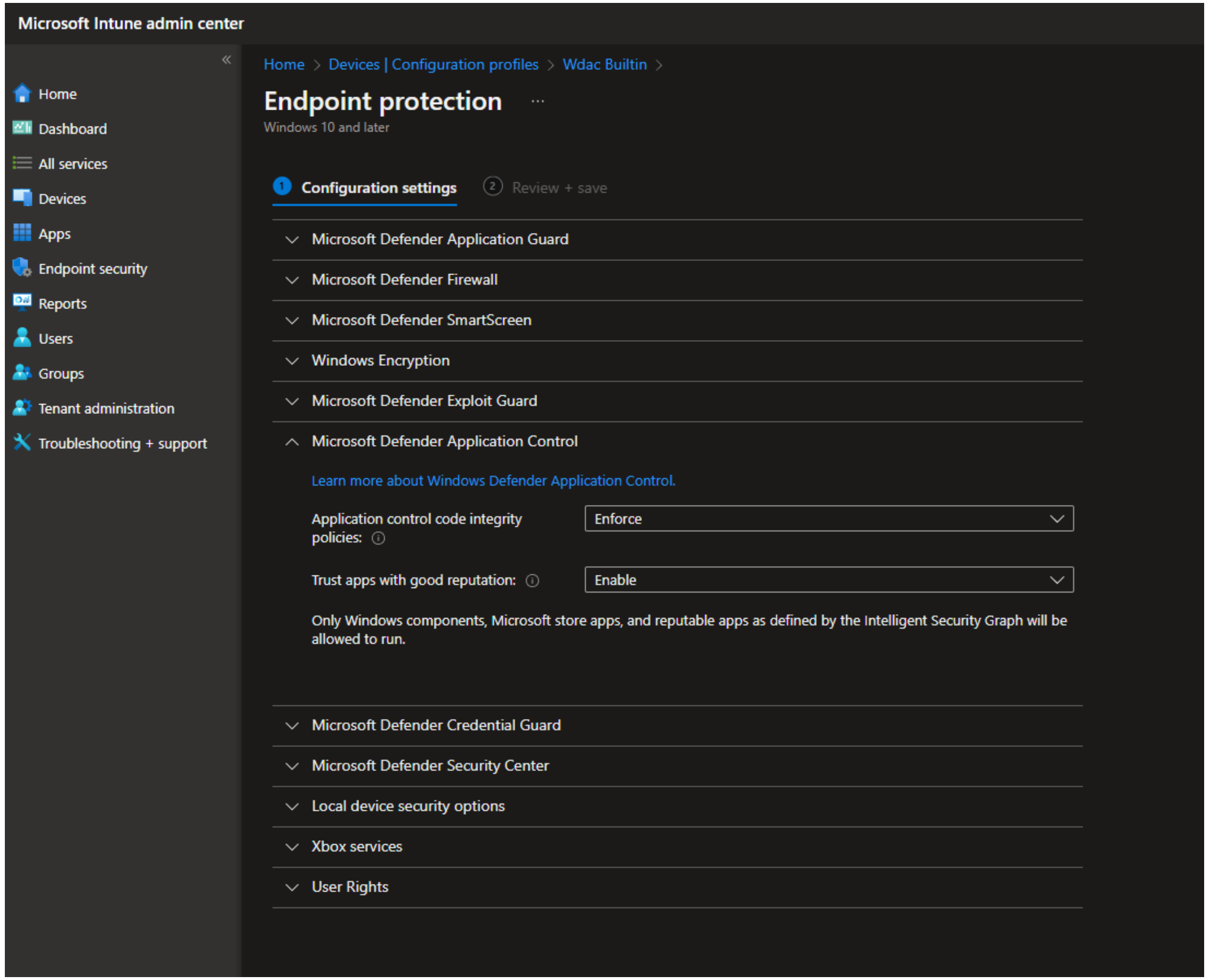
Learn more about Windows Defender Application Control.

Application control code integrity policies: Enforce

Trust apps with good reputation: Enable

Only Windows components, Microsoft store apps, and reputable apps as defined by the Intelligent Security Graph will be allowed to run.

Intune Policies – built-in



Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices | Configuration profiles > Wdac Builtin >

Endpoint protection

Windows 10 and later

1 Configuration settings
2 Review + save
Microsoft Defender Application Guard
Microsoft Defender Firewall
Microsoft Defender SmartScreen
Windows Encryption
Microsoft Defender Exploit Guard
Microsoft Defender Application Control
Learn more about Windows Defender Application Control.

Application control code integrity policies: Enforce

Trust apps with good reputation: Enable

Only Windows components, Microsoft store apps, and reputable apps as defined by the Intelligent Security Graph will be allowed to run.

Microsoft Defender Credential Guard
Microsoft Defender Security Center
Local device security options
Xbox services
User Rights

Devices | Configuration profiles |Create Profile | Windows 10 and later | Endpoint Protection

Intune Policies – custom OMA-URI

1. Open the Microsoft Intune portal and create a profile with custom settings.
2. Specify a **Name** and **Description** and use the following values for the remaining custom OMA-URI settings:
   - OMA-URI: ./Vendor/MSFT/ApplicationControl/Policies/_Policy GUID_/Policy
   - Data type: Base64 (file)
   - Certificate file: Upload your binary format policy file. To do this, change your {GUID}.cip file to {GUID}.bin. You don't need to upload a Base64 file, as Intune will convert the uploaded .bin file to Base64 on your behalf.

Deploy WDAC policies using Mobile Device Management (MDM) (Windows) | Microsoft Learn

DEMOS

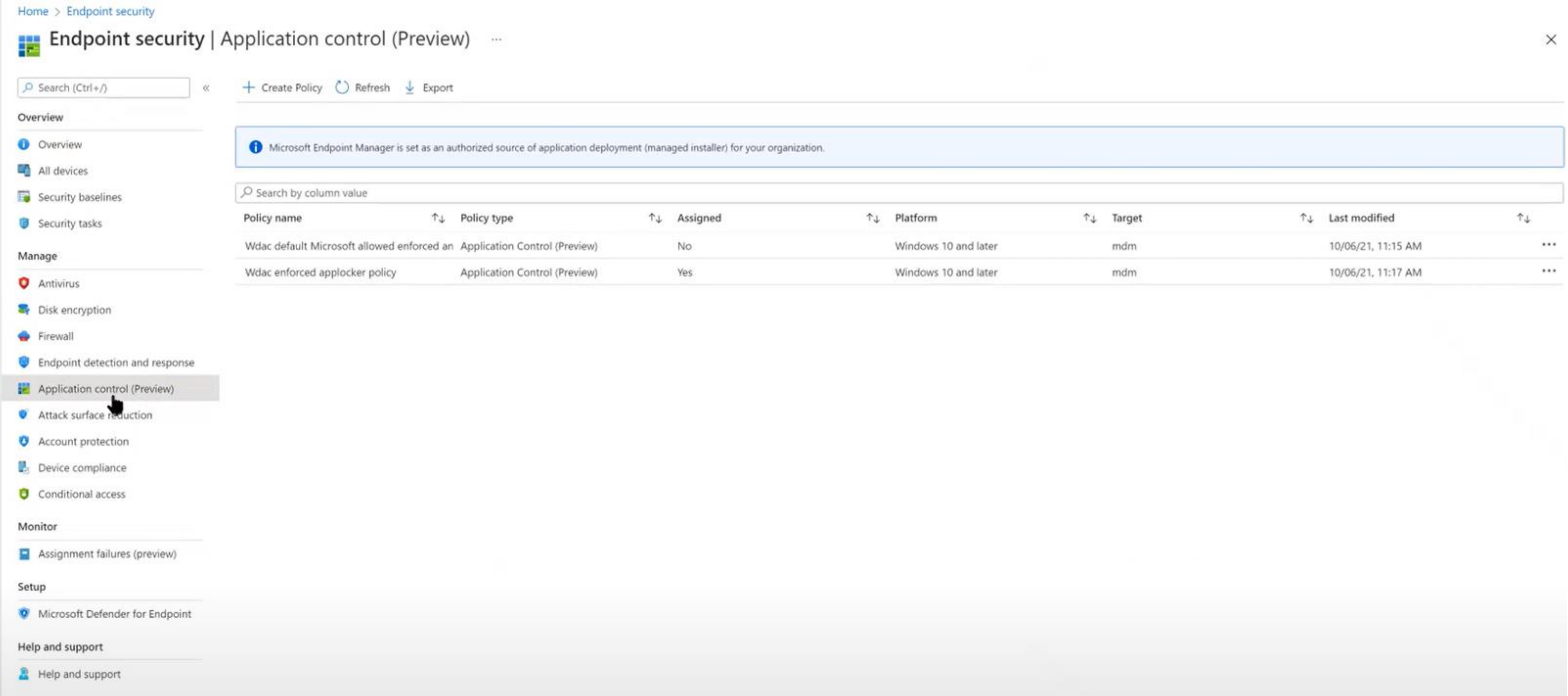
Upload custom policy

Intune Policies – custom OMA-URI

Policies deployed through Intune custom OMA-URI are subject to a 350 KB limit. Customers should create Windows Defender Application Control policies that use signature-based rules, the Intelligent Security Graph, and managed installers where practical.

[Deploy WDAC policies using Mobile Device Management (MDM) (Windows) | Microsoft Learn]

Application Control (Private Preview)



Home > Endpoint security

Endpoint security | Application control (Preview) ...

Search (Ctrl+/) «

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Application control (Preview)
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Monitor

- Assignment failures (preview)

Setup

- Microsoft Defender for Endpoint

Help and support

- Help and support

+ Create Policy Refresh Export

Microsoft Endpoint Manager is set as an authorized source of application deployment (managed installer) for your organization.

Search by column value

Policy name ↑↓	Policy type ↑↓	Assigned ↑↓	Platform ↑↓	Target ↑↓	Last modified ↑↓	
Wdac default Microsoft allowed enforced an	Application Control (Preview)	No	Windows 10 and later	mdm	10/06/21, 11:15 AM	•••
Wdac enforced applocker policy	Application Control (Preview)	Yes	Windows 10 and later	mdm	10/06/21, 11:17 AM	•••

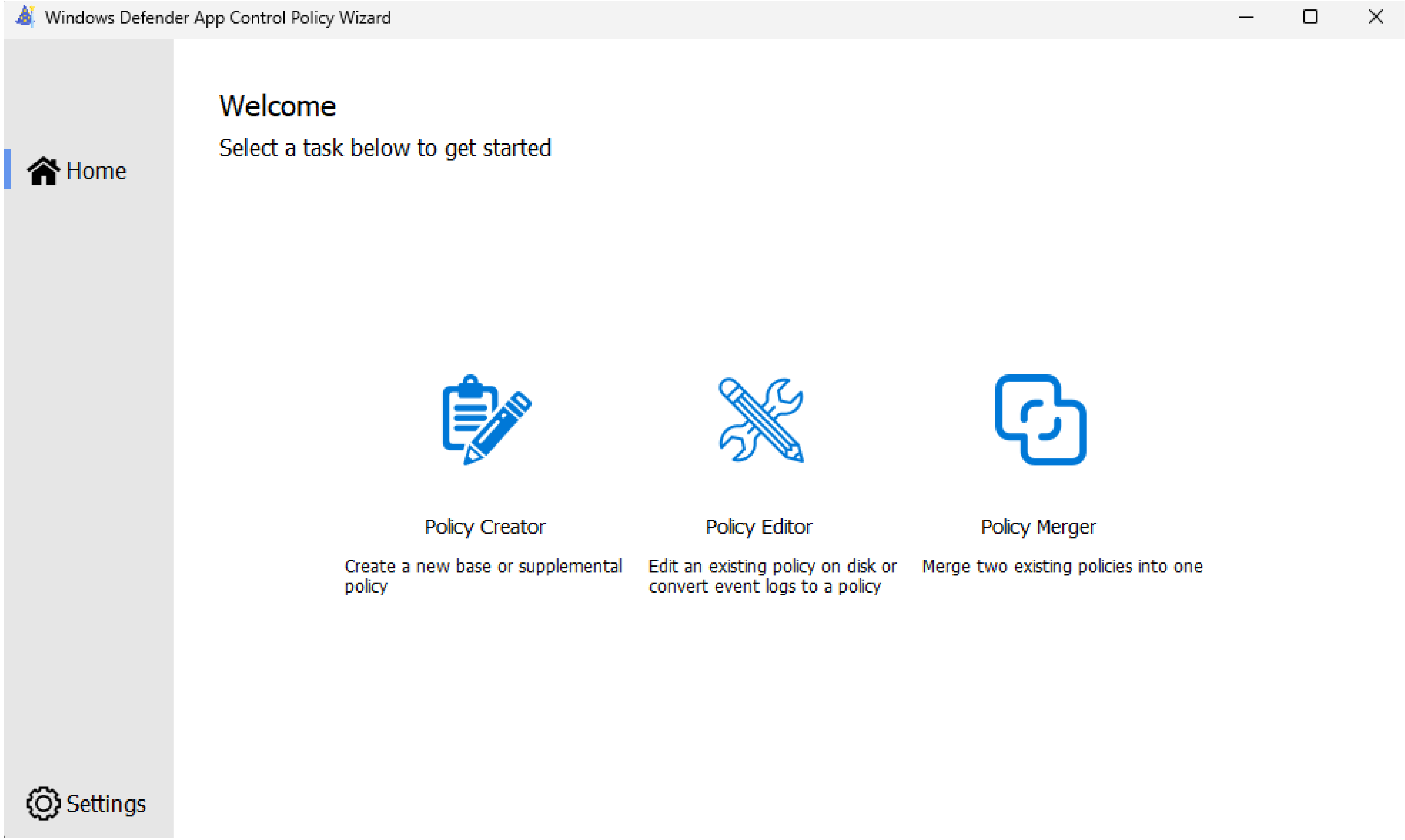
WPNinjasNL Tuesdays Webinar #33 about Windows Defender Application Control - YouTube

Tips & Tricks

Your Friends

wpninjas.au

WDAC Wizard



Windows Defender App Control Policy Wizard

Welcome

Select a task below to get started

Policy Creator

Create a new base or supplemental policy

Policy Editor

Edit an existing policy on disk or convert event logs to a policy

Policy Merger

Merge two existing policies into one

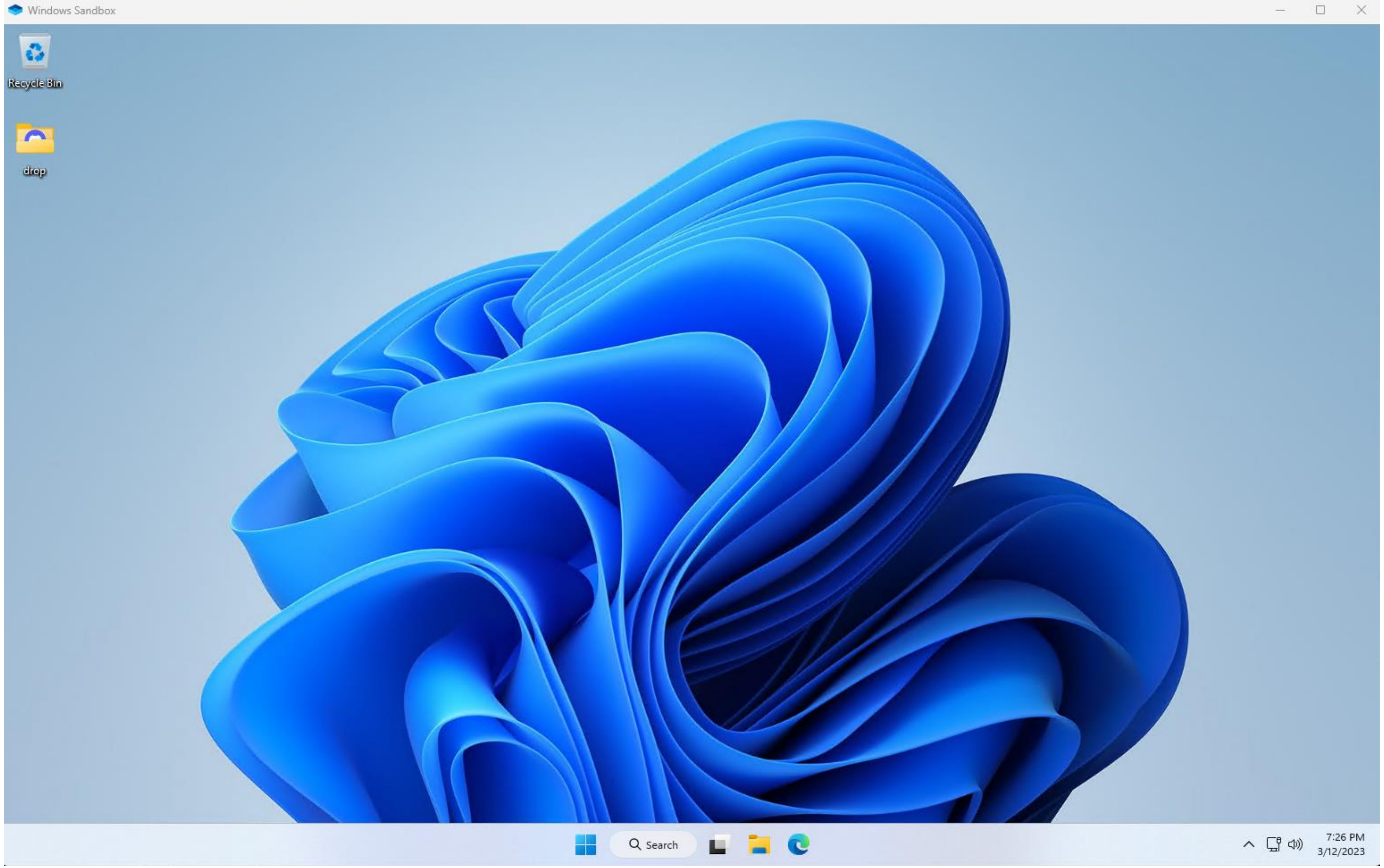
Microsoft WDAC Wizard (webapp-wdac-wizard.azurewebsites.net)

DEMOS

WDAC Wizard Policy creation

Your Friends

Windows Sandbox



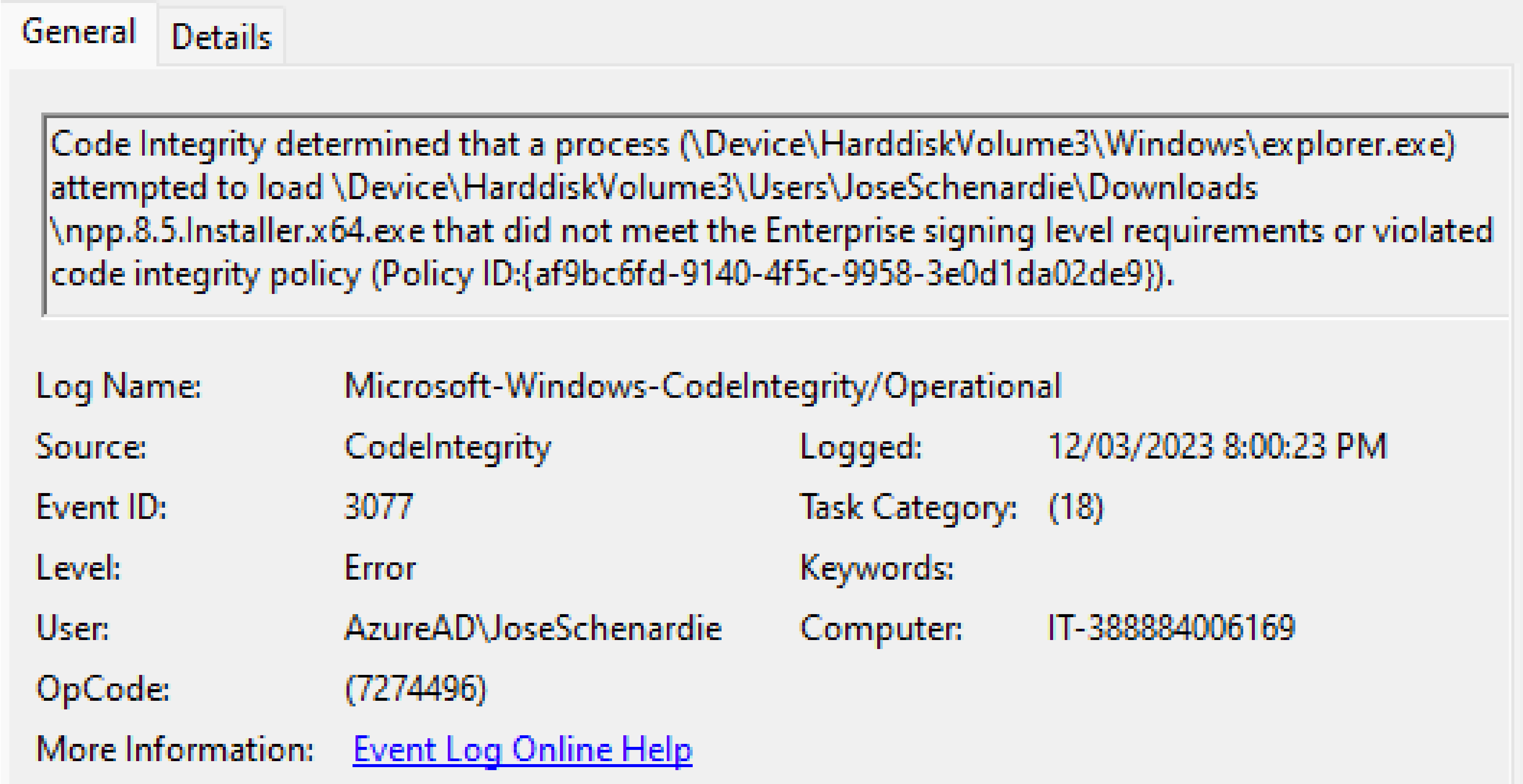
[Windows Sandbox | Microsoft Learn]

DEMOS

One time install via Sandbox

Your Friends

Event Viewer



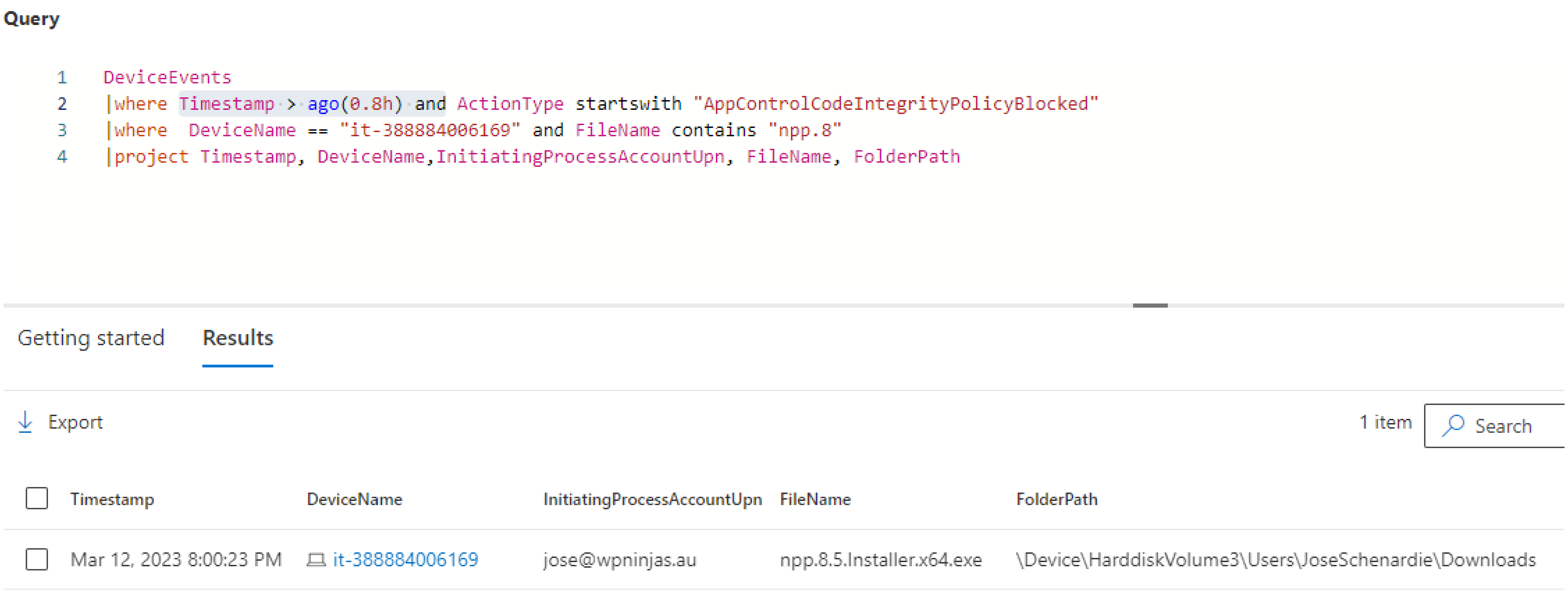
Code Integrity determined that a process (\Device\HarddiskVolume3\Windows\explorer.exe) attempted to load \Device\HarddiskVolume3\Users\JoseSchenardie\Downloads \npp.8.5.Installer.x64.exe that did not meet the Enterprise signing level requirements or violated code integrity policy (Policy ID:{af9bc6fd-9140-4f5c-9958-3e0d1da02de9}).

Log Name:	Microsoft-Windows-CodeIntegrity/Operational		
Source:	CodeIntegrity	Logged:	12/03/2023 8:00:23 PM
Event ID:	3077	Task Category:	(18)
Level:	Error	Keywords:	
User:	AzureAD\JoseSchenardie	Computer:	IT-388884006169
OpCode:	(7274496)		
More Information:	Event Log Online Help		

Applications and Services Logs | Microsoft | Windows| CodeIntegrity | Operational

Your Friends

MDE



Query

```
DeviceEvents
|where Timestamp > ago(0.8h) and ActionType startswith "AppControlCodeIntegrityPolicyBlocked"
|where  DeviceName == "it-388884006169" and FileName contains "npp.8"
|project Timestamp, DeviceName,InitiatingProcessAccountUpn, FileName, FolderPath
```

□	Timestamp	DeviceName	InitiatingProcessAccountUpn	FileName	FolderPath
□	Mar 12, 2023 8:00:23 PM	it-388884006169	jose@wpninjas.au	npp.8.5.Installer.x64.exe	\Device\HarddiskVolume3\Users\JoseSchenardie\Downloads

[Query Application Control events with Advanced Hunting (Windows) | Microsoft Learn]

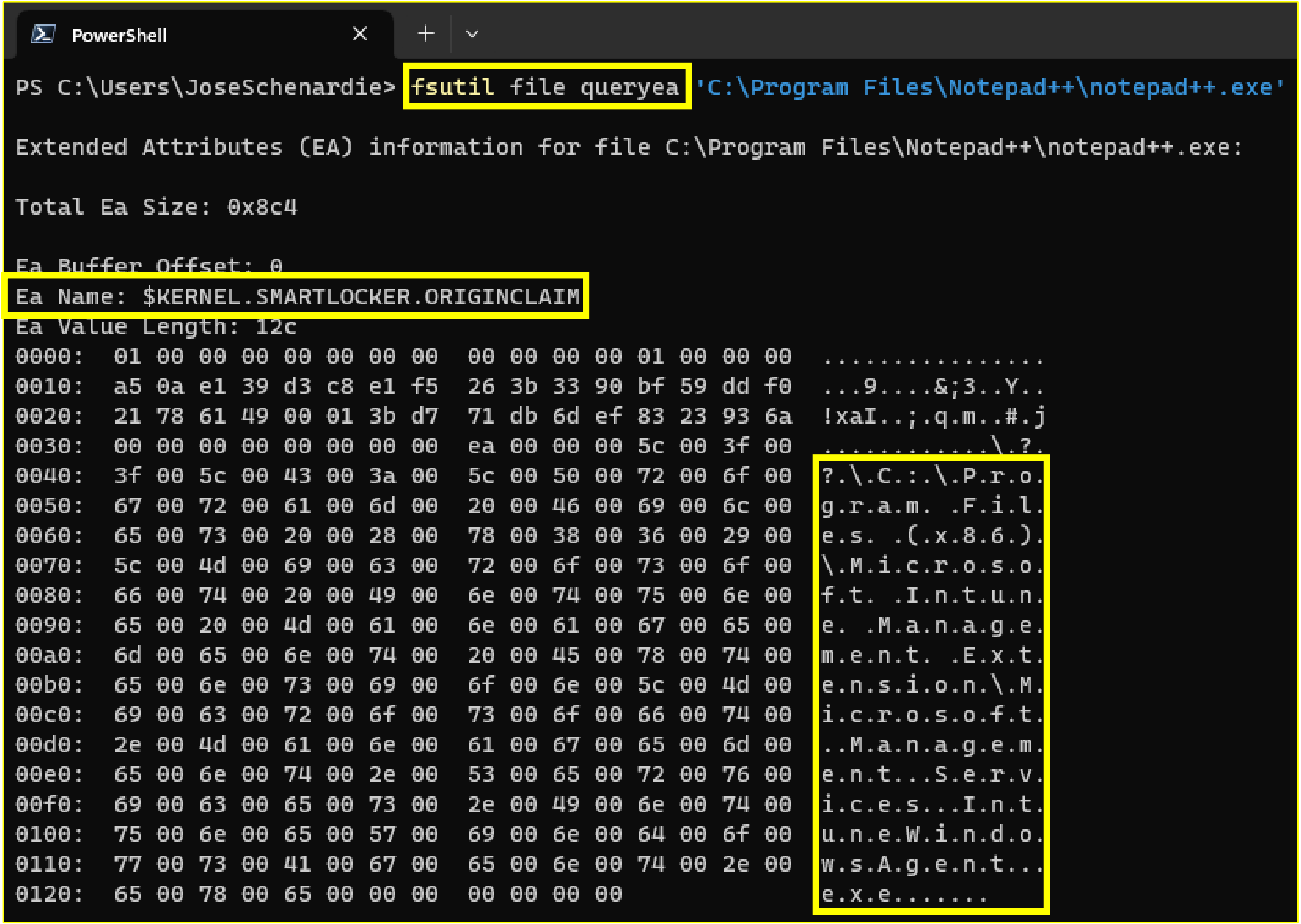
Your Best Friend

as Managed Installer

Allow apps deployed with a WDAC managed installer (Windows) | Microsoft Learn

Querying Extended Attributes

wpninjas.au



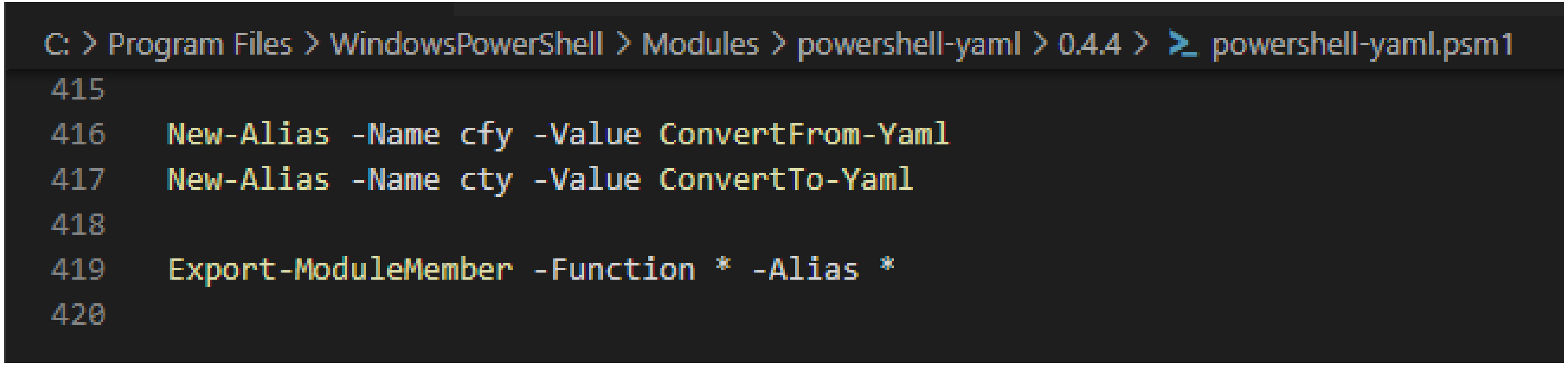
```
PS C:\Users\JoseSchenardie> fsutil file queryea 'C:\Program Files\Notepad++\notepad++.exe'

Extended Attributes (EA) information for file C:\Program Files\Notepad++\notepad++.exe:

Total Ea Size: 0x8c4

Ea Buffer Offset: 0
Ea Name: $KERNEL.SMARTLOCKER.ORIGINCLAIM
Ea Value Length: 12c
0000:  01 00 00 00 00 00 00 00  00 00 00 00 01 00 00 00  ................
0010:  a5 0a e1 39 d3 c8 e1 f5  26 3b 33 90 bf 59 dd f0  ...9....&;3..Y..
0020:  21 78 61 49 00 01 3b d7  71 db 6d ef 83 23 93 6a  !xaI..;.q.m..#.j
0030:  00 00 00 00 00 00 00 00  ea 00 00 00 5c 00 3f 00  ............\.?.
0040:  3f 00 5c 00 43 00 3a 00  5c 00 50 00 72 00 6f 00  ?.\.C.:.\.P.r.o.
0050:  67 00 72 00 61 00 6d 00  20 00 46 00 69 00 6c 00  g.r.a.m. .F.i.l.
0060:  65 00 73 00 20 00 28 00  78 00 38 00 36 00 29 00  e.s. .(.x.8.6.).
0070:  5c 00 4d 00 69 00 63 00  72 00 6f 00 73 00 6f 00  \.M.i.c.r.o.s.o.
0080:  66 00 74 00 20 00 49 00  6e 00 74 00 75 00 6e 00  f.t. .I.n.t.u.n.
0090:  65 00 20 00 4d 00 61 00  6e 00 61 00 67 00 65 00  e. .M.a.n.a.g.e.
00a0:  6d 00 65 00 6e 00 74 00  20 00 45 00 78 00 74 00  m.e.n.t. .E.x.t.
00b0:  65 00 6e 00 73 00 69 00  6f 00 6e 00 5c 00 4d 00  e.n.s.i.o.n.\.M.
00c0:  69 00 63 00 72 00 6f 00  73 00 6f 00 66 00 74 00  i.c.r.o.s.o.f.t.
00d0:  2e 00 4d 00 61 00 6e 00  61 00 67 00 65 00 6d 00  ..M.a.n.a.g.e.m.
00e0:  65 00 6e 00 74 00 2e 00  53 00 65 00 72 00 76 00  e.n.t...S.e.r.v.
00f0:  69 00 63 00 65 00 73 00  2e 00 49 00 6e 00 74 00  i.c.e.s...I.n.t.
0100:  75 00 6e 00 65 00 57 00  69 00 6e 00 64 00 6f 00  u.n.e.W.i.n.d.o.
0110:  77 00 73 00 41 00 67 00  65 00 6e 00 74 00 2e 00  w.s.A.g.e.n.t...
0120:  65 00 78 00 65 00 00 00  00 00 00 00              e.x.e.......
```

Managed installer and ISG technical reference and troubleshooting guide (Windows) | Microsoft Learn

DEMOS

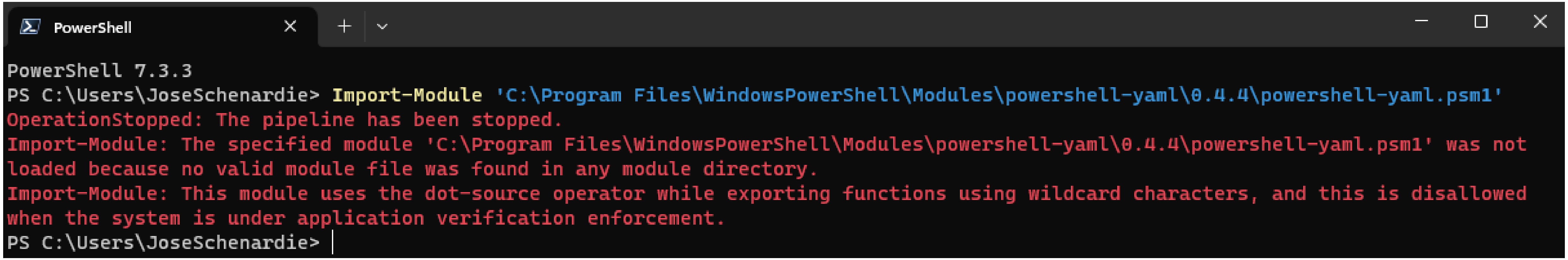
Managed Installer in Action

Your Enemies 01 - Wildcard



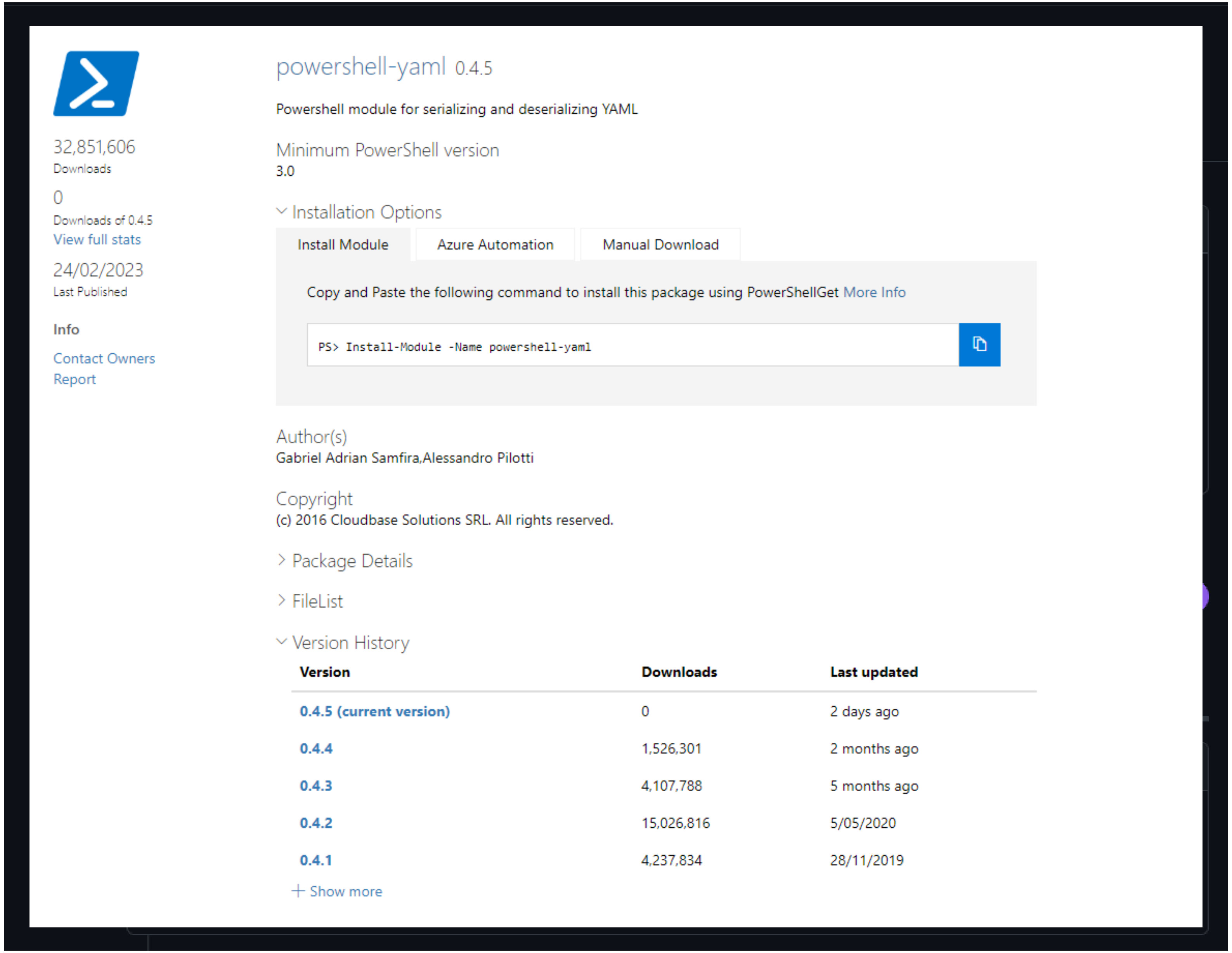
C: > Program Files > WindowsPowerShell > Modules > powershell-yaml > 0.4.4 > powershell-yaml.psm1

```

New-Alias -Name cfy -Value ConvertFrom-Yaml
New-Alias -Name cty -Value ConvertTo-Yaml

Export-ModuleMember -Function * -Alias *

```



```
PowerShell 7.3.3
PS C:\Users\JoseSchenardie> Import-Module 'C:\Program Files\WindowsPowerShell\Modules\powershell-yaml\0.4.4\powershell-yaml.psm1'
OperationStopped: The pipeline has been stopped.
Import-Module: The specified module 'C:\Program Files\WindowsPowerShell\Modules\powershell-yaml\0.4.4\powershell-yaml.psm1' was not
loaded because no valid module file was found in any module directory.
Import-Module: This module uses the dot-source operator while exporting functions using wildcard characters, and this is disallowed
when the system is under application verification enforcement.
PS C:\Users\JoseSchenardie>
```

~~Your Enemies 01 - Wildcard~~



32,851,606
Downloads

0
Downloads of 0.4.5
View full stats

24/02/2023
Last Published

Info

Contact Owners
Report

powershell-yaml 0.4.5

Powershell module for serializing and deserializing YAML

Minimum PowerShell version
3.0

Installation Options

Copy and Paste the following command to install this package using PowerShellGet More Info

```
PS> Install-Module -Name powershell-yaml
```

Author(s)
Gabriel Adrian Samfira,Alessandro Pilotti

Copyright
(c) 2016 Cloudbase Solutions SRL. All rights reserved.

Package Details

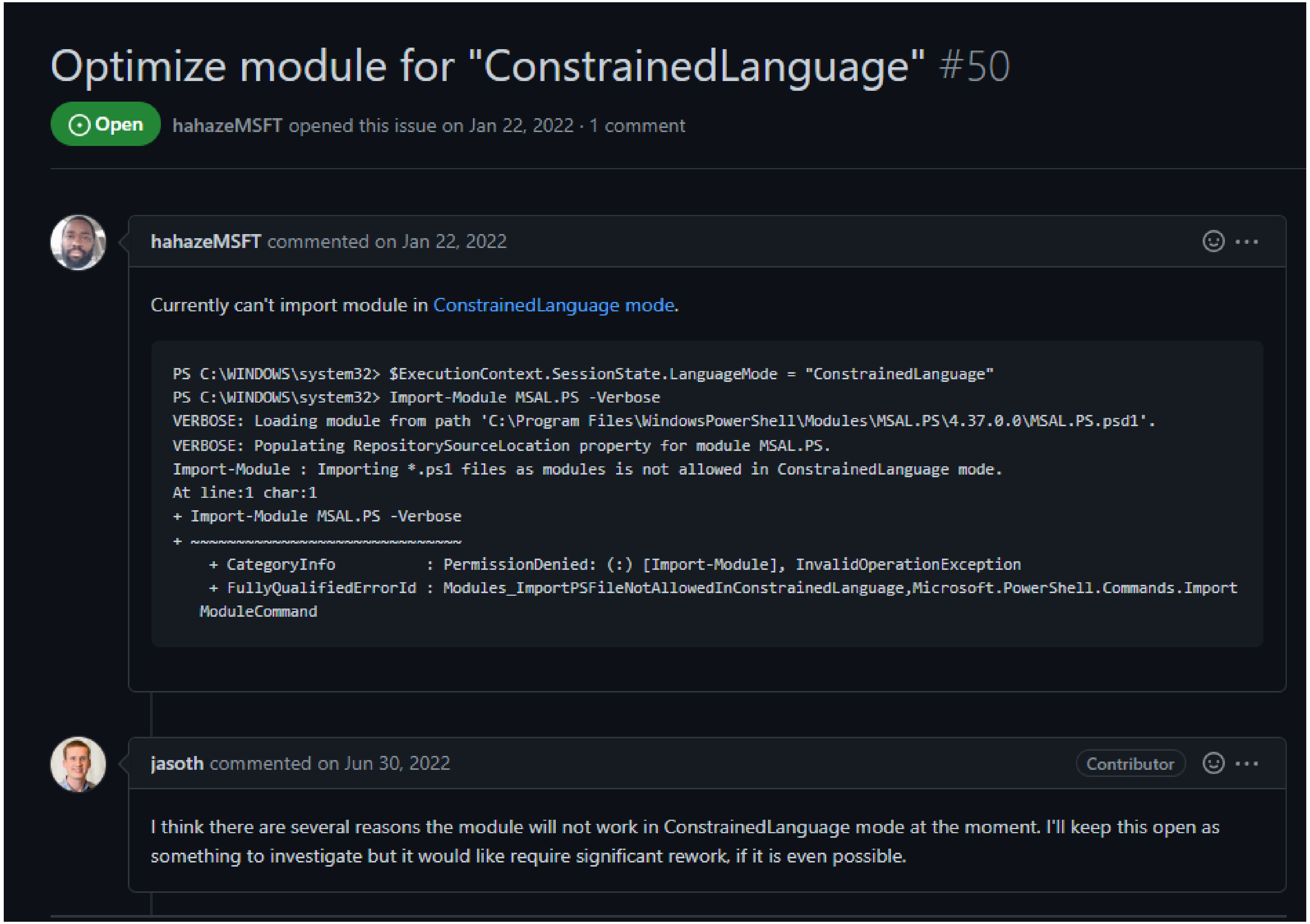
FileList

Version History

Version	Downloads	Last updated
0.4.5 (current version)	0	2 days ago
0.4.4	1,526,301	2 months ago
0.4.3	4,107,788	5 months ago
0.4.2	15,026,816	5/05/2020
0.4.1	4,237,834	28/11/2019

+ Show more

Your Enemies 02 – Dot sourcing



Optimize module for "ConstrainedLanguage" #50

Open hahazeMSFT opened this issue on Jan 22, 2022 · 1 comment

hahazeMSFT commented on Jan 22, 2022

Currently can't import module in ConstrainedLanguage mode.

```
PS C:\WINDOWS\system32> $ExecutionContext.SessionState.LanguageMode = "ConstrainedLanguage"
PS C:\WINDOWS\system32> Import-Module MSAL.PS -Verbose
VERBOSE: Loading module from path 'C:\Program Files\WindowsPowerShell\Modules\MSAL.PS\4.37.0.0\MSAL.PS.psd1'.
VERBOSE: Populating RepositorySourceLocation property for module MSAL.PS.
Import-Module : Importing *.ps1 files as modules is not allowed in ConstrainedLanguage mode.
At line:1 char:1
+ Import-Module MSAL.PS -Verbose
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (:) [Import-Module], InvalidOperationException
    + FullyQualifiedErrorId : Modules_ImportPSFileNotAllowedInConstrainedLanguage,Microsoft.PowerShell.Commands.Import
   ModuleCommand
```

jasoth commented on Jun 30, 2022 Contributor

I think there are several reasons the module will not work in ConstrainedLanguage mode at the moment. I'll keep this open as something to investigate but it would like require significant rework, if it is even possible.

Your Enemies 03 – Auto updaters

Application control, based on managed installer, doesn't support applications that self-update. If an application that was deployed by a managed installer later updates itself, the updated application files won't include the origin information from the managed installer, and they might not be able to run. When you rely on managed installers, you must deploy and install all application updates by using a managed installer, or include rules to authorize the app in the WDAC policy.

Allow apps deployed with a WDAC managed installer (Windows) | Microsoft Learn

Q & A

Thank You