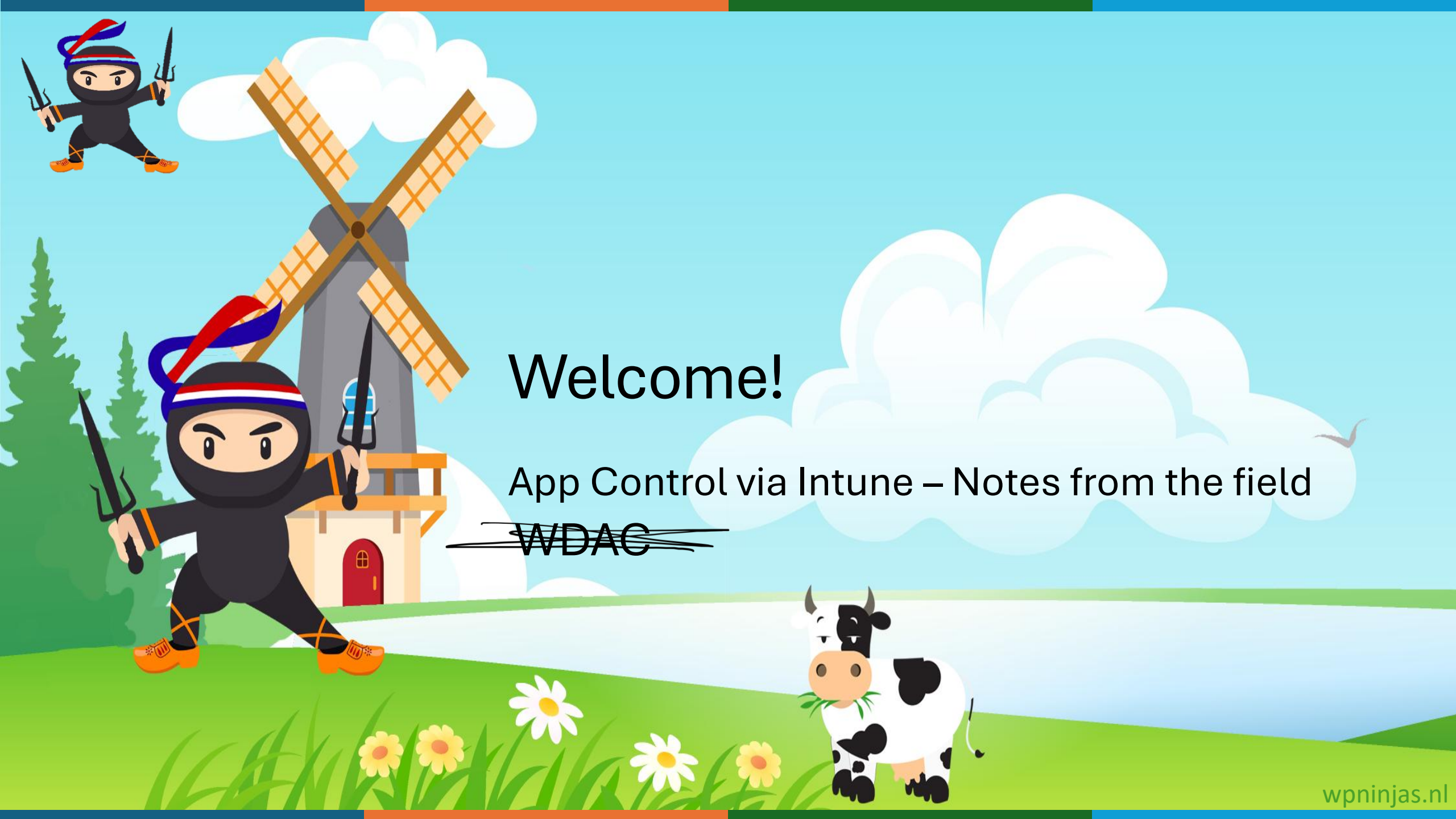


Welcome!

App Control via Intune – Notes from the field

~~WDAC~~

Thank you Sponsors

Gold

liquidware

2Pint

PINK

RECAST SOFTWARE

Silver

PATCH MY PC

Technical Partners

CONSULTEQ

PROXSYS

Daalmans consulting

Secure At Work

Questions

Who uses WDAC in production? (not in a lab)

Who uses Applocker?

Third Party tooling for similar stuff?

Niels Kok

- Consultant

Calendar

- Introduction to WDAC
- Configuration (Demo)
- Tooling (Demo)
- Challenges (Demo, Kinda)
- Tips & Tricks (Demo, Kinda)

Introduction

App Control

Scope

EXECUTABLE FILES (.EXE, .COM)

DYNAMIC-LINK LIBRARIES (.DLL, .OCX)

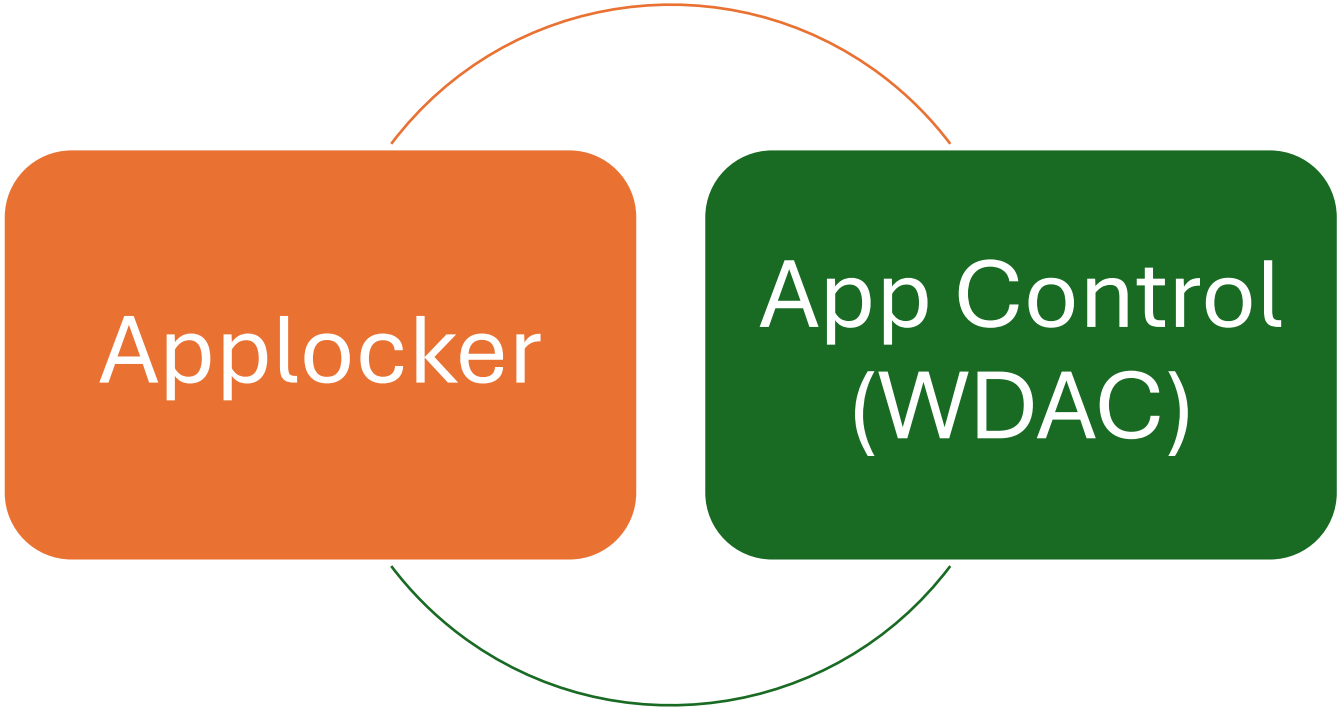
SCRIPTS (.PS1, .VBS, .JS, .CMD, .BAT)

INSTALLER FILES (.MSI, .MSP, .MST)

PACKAGES APPS (.APPX, .MSIX, .APPXBUNDLE/.MSIXBUNDLE)

DRIVERS (.SYS)

Options for App Control



Configuration (Demo)

Demo Content

Applocker

- How to configure (via Intune)
- Updating policies

App Control (WDAC)

- How to configure (via Intune)
- Updating policies

Forgot the managed installer

Event Viewer

File Action View Help

- System
- User Experience Virtualization
- Windows
  - AAD
  - AccelLib-AccelCx
  - All-User-Install-Agent
  - AppHost
  - AppID
  - ApplicabilityEngine
  - Application Server-Applications
  - Application-Experience
  - AppLocker
    - EXE and DLL
    - MSI and Script
    - Packaged app-Deployment
    - Packaged app-Execution
  - AppModel-Runtime
  - AppReadiness
  - Apps
  - Apps-API
  - AppXDeployment
  - AppXDeployment-Server
  - AppXDeployment-Server-UndockedDeh
  - AppxPackagingOM
  - ASN1
  - AssignedAccess
  - AssignedAccessBroker
  - ATAPort
  - Audio
  - Authentication
  - Authentication User Interface
  - BackgroundTaskInfrastructure
  - BackgroundTransfer-ContentPrefetcher
  - Base-Filtering-Engine-Connections
  - Base-Filtering-Engine-Resource-Flows

MSI and Script Number of events: 1,369 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	12/5/2024 7:53:36 PM	AppLocker	8041	None
Information	12/5/2024 7:53:36 PM	AppLocker	8037	None
Information	12/5/2024 7:53:36 PM	AppLocker	8037	None
Information	12/5/2024 7:53:36 PM	AppLocker	8041	None
Information	12/5/2024 7:53:36 PM	AppLocker	8038	None
Error	12/5/2024 7:53:36 PM	AppLocker	8029	None
Information	12/5/2024 7:53:36 PM	AppLocker	8038	None
Error	12/5/2024 7:53:36 PM	AppLocker	8029	None
Information	12/5/2024 7:53:18 PM	AppLocker	8041	None
Information	12/5/2024 7:53:18 PM	AppLocker	8037	None
Information	12/5/2024 7:53:17 PM	AppLocker	8037	None
Information	12/5/2024 7:53:17 PM	AppLocker	8041	None

Event 8029, AppLocker

General Details

C:\Program Files (x86)\Microsoft Intune Management Extension\Content\DetectionScripts\64e5583f-d377-4881-99c6-061e5575c2cf_1.ps1 was prevented from running due to Config CI policy.

Log Name:	Microsoft-Windows-AppLocker/MSI and Script		
Source:	AppLocker	Logged:	12/5/2024 7:53:36 PM
Event ID:	8029	Task Category:	None
Level:	Error	Keywords:	
User:	SYSTEM	Computer:	LP-945599b2528f
OpCode:	Info		

Store Applications

Block store via Intune is not enough

Challenges

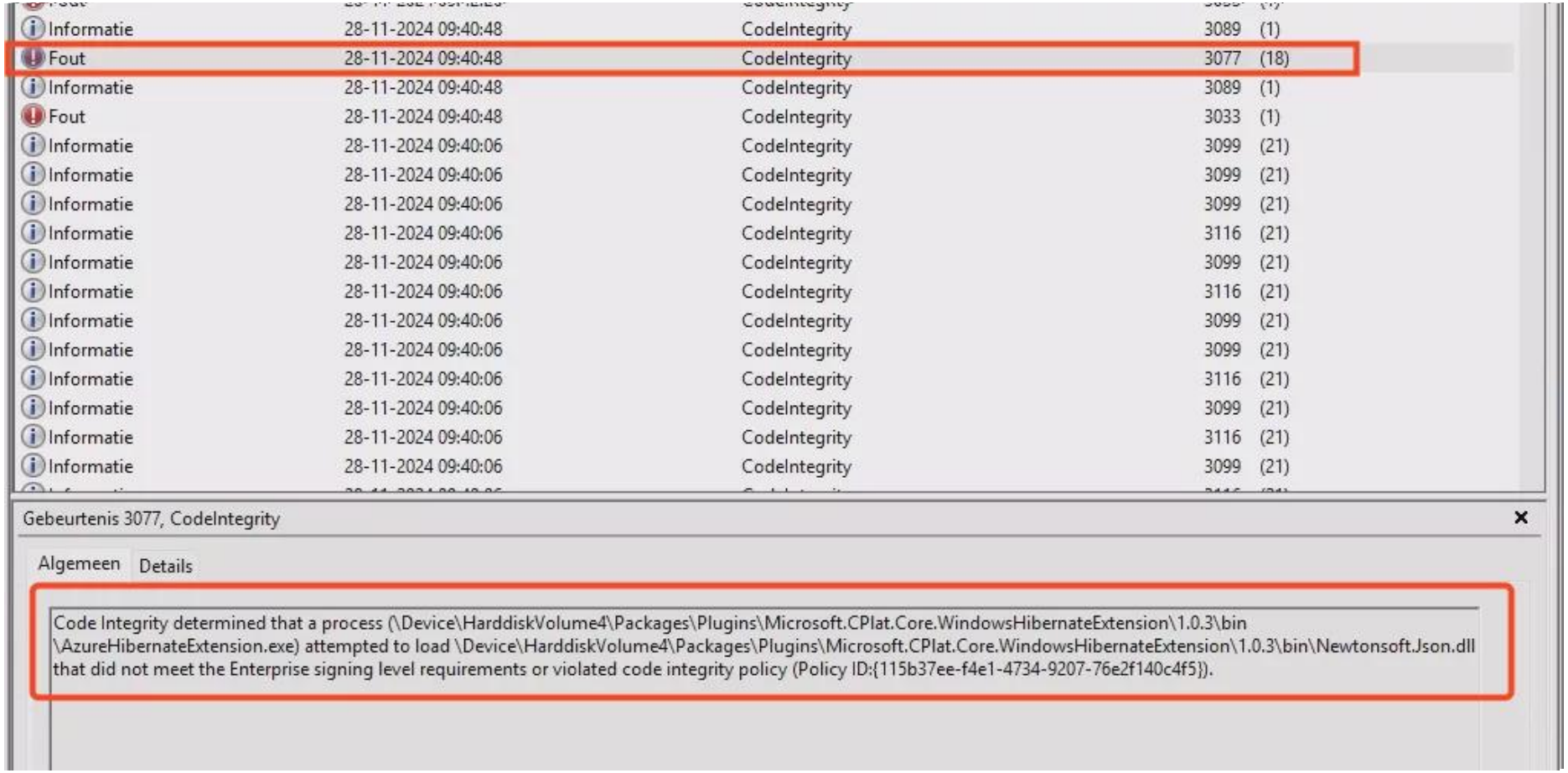
Windows 365

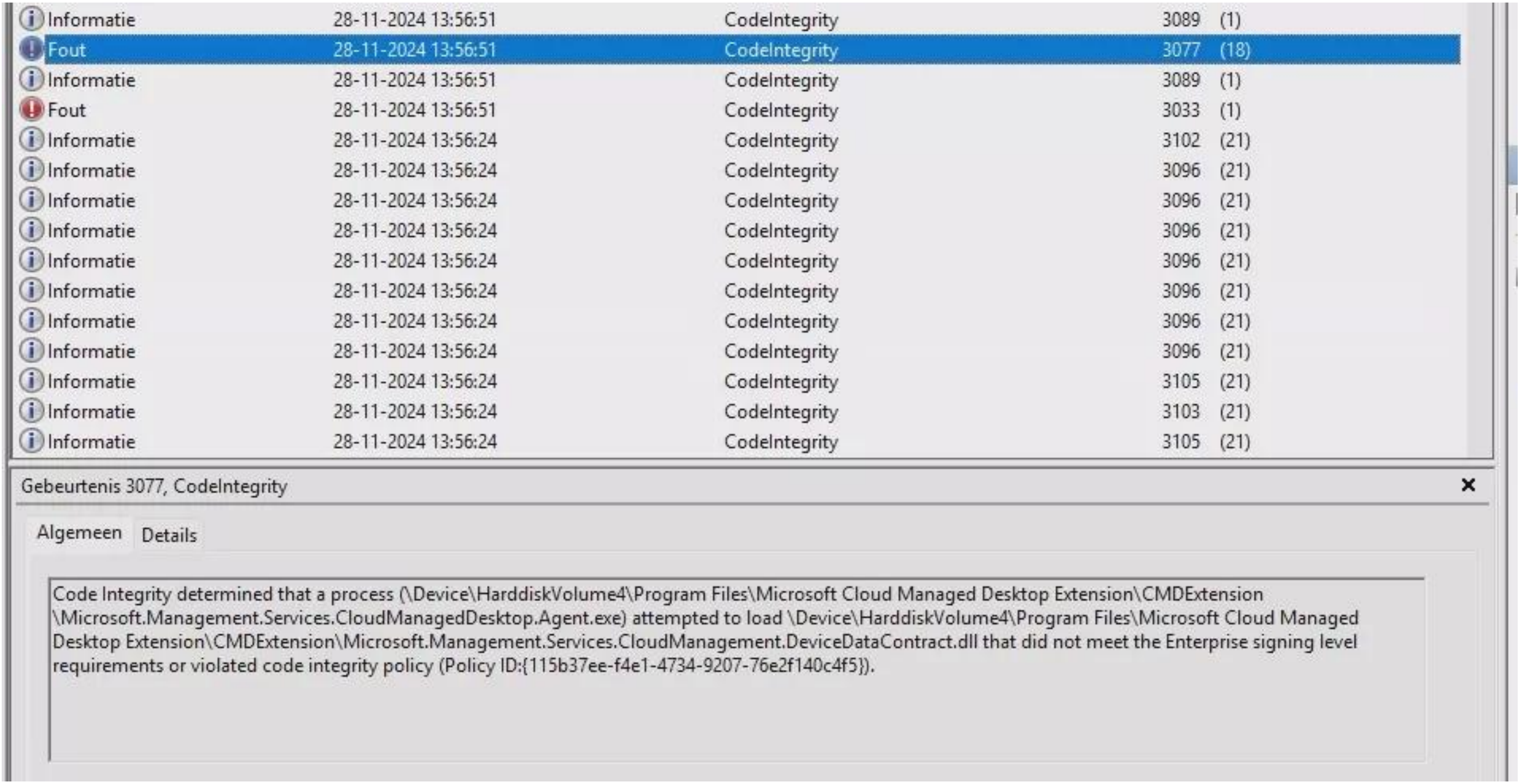
Informatie	28-11-2024 07:40:43	Windows Error Reporting	1001	Geen
Informatie	28-11-2024 07:40:44	edgeupdate	0	Geen
Fout	28-11-2024 07:40:42	Application Error	1000	Toepassingscrash-gebeu
Fout	28-11-2024 07:40:42	.NET Runtime	1026	Geen
Informatie	28-11-2024 07:39:56	MsiInstaller	1042	Geen
Informatie	28-11-2024 07:39:56	MsiInstaller	1034	Geen
Fout	28-11-2024 07:39:56	MsiInstaller	11723	Geen
Informatie	28-11-2024 07:39:55	MsiInstaller	1040	Geen
Informatie	28-11-2024 07:39:55	MsiInstaller	1042	Geen
Informatie	28-11-2024 07:39:55	MsiInstaller	1035	Geen
Informatie	28-11-2024 07:39:55	MsiInstaller	11728	Geen

Gebeurtenis 1000, Application Error

Algemeen Details

Toepassingsnaam met fout: Microsoft.Management.Services.CloudManagedDesktop.Agent.exe, versie: 1.2.2864.237, tijdstempel: 0xd7c42042
Naam van foutmodule: KERNELBASE.dll, versie: 10.0.26100.2161, tijdstempel: 0x31da495c
Uitzonderingscode: 0xe0434352
Foutoffset: 0x00000000000c831a
Foutproces-id: 0x1958
Begintijd van foutieve toepassing: 0x1DB416071E8BCE3
Faulting-toepassingspad: C:\Program Files\Microsoft Cloud Managed Desktop Extension\CMDExtension
\Microsoft.Management.Services.CloudManagedDesktop.Agent.exe
Faulting-modulepad: C:\Windows\System32\KERNELBASE.dll
Rapport-id: d7a42260-db61-4d2b-bee6-ac3d1ca6d2d6
Faulting-pakket volledige naam:
Faulting-pakket-relatieve toepassings-id:

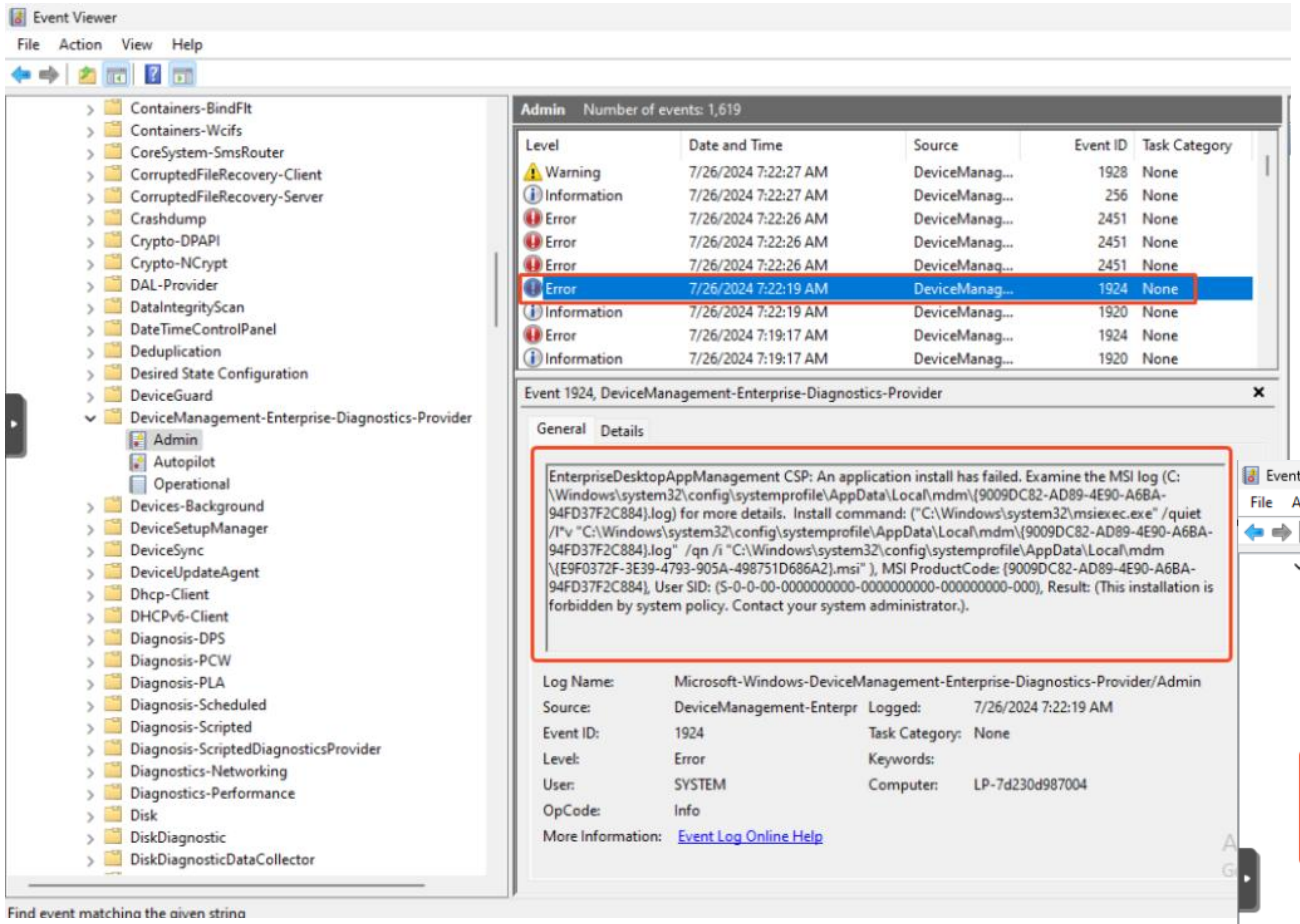

Informatie 28-11-2024 09:40:48 CodeIntegrity 3089 (1)
Fout 28-11-2024 09:40:48 CodeIntegrity 3077 (18)
Informatie 28-11-2024 09:40:48 CodeIntegrity 3089 (1)
Fout 28-11-2024 09:40:48 CodeIntegrity 3033 (1)
Informatie 28-11-2024 09:40:06 CodeIntegrity 3099 (21)
Informatie 28-11-2024 09:40:06 CodeIntegrity 3099 (21)
Informatie 28-11-2024 09:40:06 CodeIntegrity 3099 (21)
Informatie 28-11-2024 09:40:06 CodeIntegrity 3116 (21)
Informatie 28-11-2024 09:40:06 CodeIntegrity 3099 (21)
Informatie 28-11-2024 09:40:06 CodeIntegrity 3116 (21)
Informatie 28-11-2024 09:40:06 CodeIntegrity 3099 (21)
Informatie 28-11-2024 09:40:06 CodeIntegrity 3099 (21)
Informatie 28-11-2024 09:40:06 CodeIntegrity 3116 (21)
Informatie 28-11-2024 09:40:06 CodeIntegrity 3099 (21)
Informatie 28-11-2024 09:40:06 CodeIntegrity 3116 (21)
Informatie 28-11-2024 09:40:06 CodeIntegrity 3099 (21)
Gebeurtenis 3077, CodeIntegrity
Algemeen
Details
Code Integrity determined that a process (\Device\HarddiskVolume4\Packages\Plugins\Microsoft.CPlat.Core.WindowsHibernateExtension\1.0.3\bin\AzureHibernateExtension.exe) attempted to load \Device\HarddiskVolume4\Packages\Plugins\Microsoft.CPlat.Core.WindowsHibernateExtension\1.0.3\bin\Newtonsoft.Json.dll that did not meet the Enterprise signing level requirements or violated code integrity policy (Policy ID:{115b37ee-f4e1-4734-9207-76e2f140c4f5}).

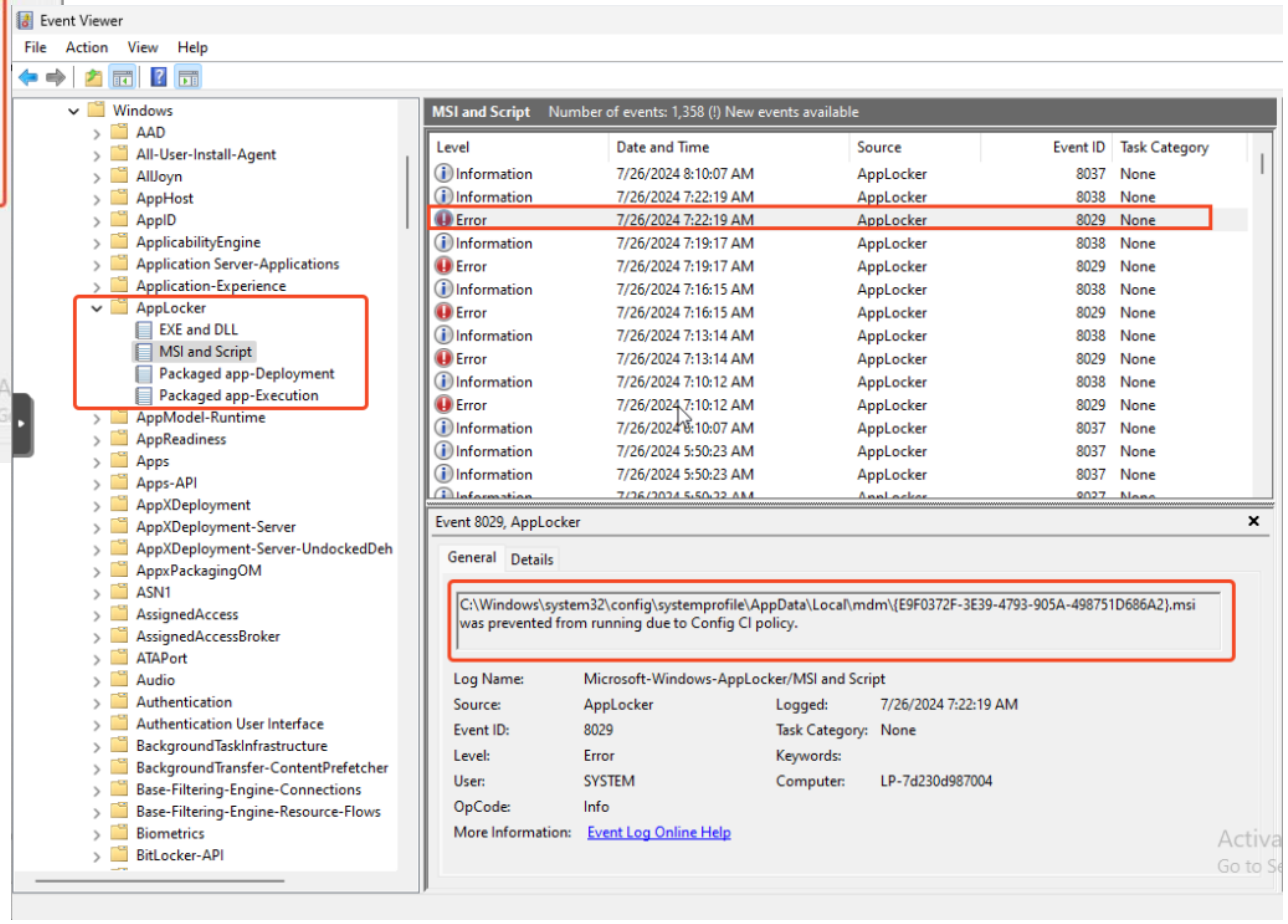

Informatie 28-11-2024 13:56:51 CodeIntegrity 3089 (1)
Fout 28-11-2024 13:56:51 CodeIntegrity 3077 (18)
Informatie 28-11-2024 13:56:51 CodeIntegrity 3089 (1)
Fout 28-11-2024 13:56:51 CodeIntegrity 3033 (1)
Informatie 28-11-2024 13:56:24 CodeIntegrity 3102 (21)
Informatie 28-11-2024 13:56:24 CodeIntegrity 3096 (21)
Informatie 28-11-2024 13:56:24 CodeIntegrity 3096 (21)
Informatie 28-11-2024 13:56:24 CodeIntegrity 3096 (21)
Informatie 28-11-2024 13:56:24 CodeIntegrity 3096 (21)
Informatie 28-11-2024 13:56:24 CodeIntegrity 3096 (21)
Informatie 28-11-2024 13:56:24 CodeIntegrity 3096 (21)
Informatie 28-11-2024 13:56:24 CodeIntegrity 3096 (21)
Informatie 28-11-2024 13:56:24 CodeIntegrity 3105 (21)
Informatie 28-11-2024 13:56:24 CodeIntegrity 3103 (21)
Informatie 28-11-2024 13:56:24 CodeIntegrity 3105 (21)
Gebeurtenis 3077, CodeIntegrity
Algemeen
Details
Code Integrity determined that a process (\Device\HarddiskVolume4\Program Files\Microsoft Cloud Managed Desktop Extension\CMDExtension \Microsoft.Management.Services.CloudManagedDesktop.Agent.exe) attempted to load \Device\HarddiskVolume4\Program Files\Microsoft Cloud Managed Desktop Extension\CMDExtension\Microsoft.Management.Services.CloudManagement.DeviceDataContract.dll that did not meet the Enterprise signing level requirements or violated code integrity policy (Policy ID:{115b37ee-f4e1-4734-9207-76e2f140c4f5}).

Microsoft Certificates

- Microsoft Azure 3rd Party code sign
- Microsoft Azure code sign

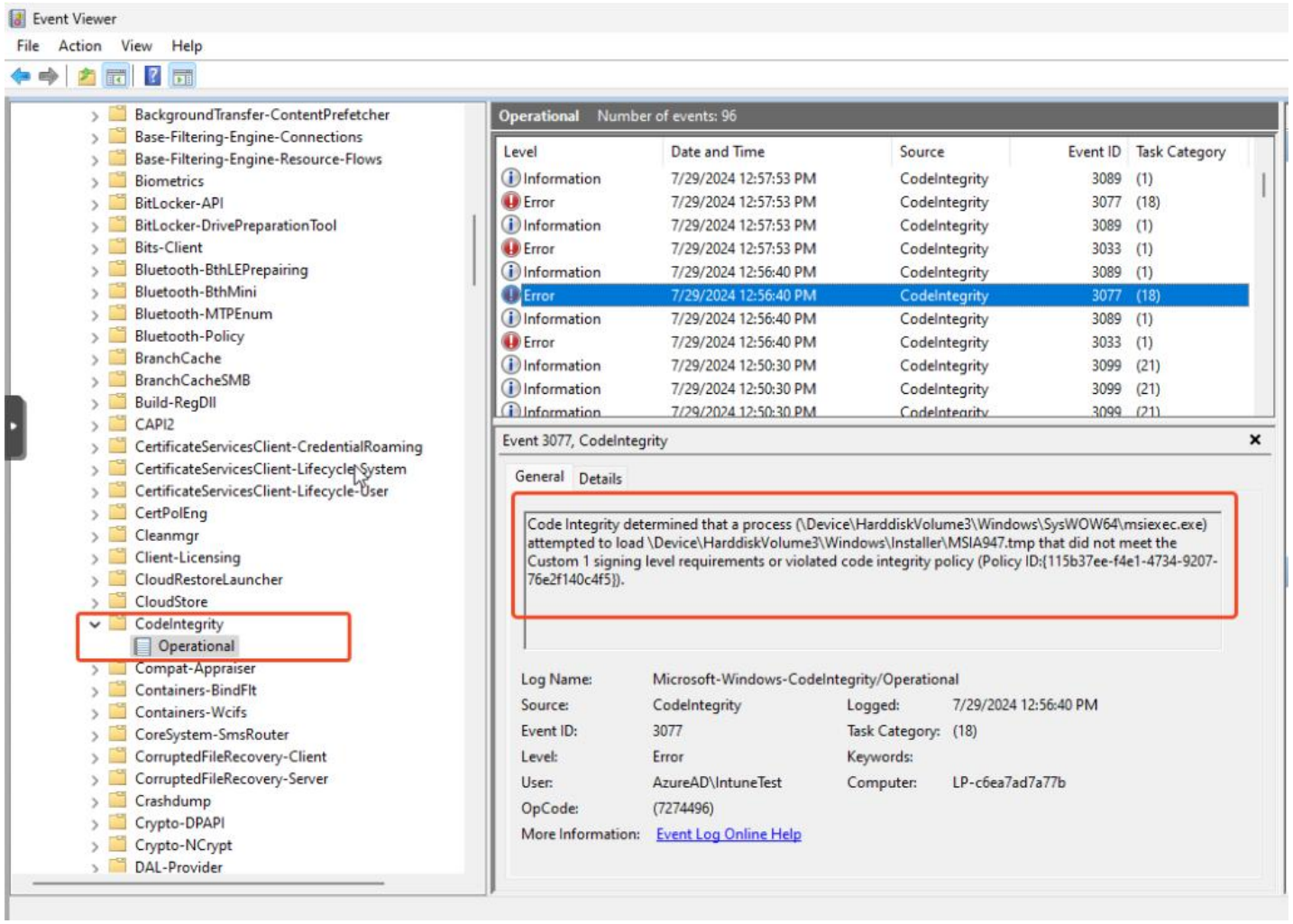
EPM


Event Viewer
File Action View Help
Admin Number of events: 1,619
Level Date and Time Source Event ID Task Category
Warning 7/26/2024 7:22:27 AM DeviceManag... 1928 None
Information 7/26/2024 7:22:27 AM DeviceManag... 256 None
Error 7/26/2024 7:22:26 AM DeviceManag... 2451 None
Error 7/26/2024 7:22:26 AM DeviceManag... 2451 None
Error 7/26/2024 7:22:26 AM DeviceManag... 2451 None
Error 7/26/2024 7:22:19 AM DeviceManag... 1924 None
Information 7/26/2024 7:22:19 AM DeviceManag... 1920 None
Error 7/26/2024 7:19:17 AM DeviceManag... 1924 None
Information 7/26/2024 7:19:17 AM DeviceManag... 1920 None
Containers-BindFlt
Containers-Wcifs
CoreSystem-SmsRouter
CorruptedFileRecovery-Client
CorruptedFileRecovery-Server
Crashdump
Crypto-DPAPI
Crypto-NCrypt
DAL-Provider
DataIntegrityScan
DateTimeControlPanel
Deduplication
Desired State Configuration
DeviceGuard
DeviceManagement-Enterprise-Diagnostics-Provider
Admin
Autopilot
Operational
Devices-Background
DeviceSetupManager
DeviceSync
DeviceUpdateAgent
Dhcp-Client
DHCPv6-Client
Diagnosis-DPS
Diagnosis-PCW
Diagnosis-PLA
Diagnosis-Scheduled
Diagnosis-Scripted
Diagnosis-ScriptedDiagnosticsProvider
Diagnostics-Networking
Diagnostics-Performance
Disk
DiskDiagnostic
DiskDiagnosticDataCollector
Event 1924, DeviceManagement-Enterprise-Diagnostics-Provider
General Details
EnterpriseDesktopAppManagement CSP: An application install has failed. Examine the MSI log (C:\Windows\system32\config\systemprofile\AppData\Local\mdm\{9009DC82-AD89-4E90-A6BA-94FD37F2C884}.log) for more details. Install command: ("C:\Windows\system32\msiexec.exe" /quiet /l*v "C:\Windows\system32\config\systemprofile\AppData\Local\mdm\{9009DC82-AD89-4E90-A6BA-94FD37F2C884}.log" /qn /i "C:\Windows\system32\config\systemprofile\AppData\Local\mdm\{E9F0372F-3E39-4793-905A-498751D686A2}.msi"), MSI ProductCode: {9009DC82-AD89-4E90-A6BA-94FD37F2C884}, User SID: (S-0-0-00-0000000000-0000000000-000000000-000), Result: (This installation is forbidden by system policy. Contact your system administrator.).
Log Name: Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Admin
Source: DeviceManagement-Enterpr Logged: 7/26/2024 7:22:19 AM
Event ID: 1924 Task Category: None
Level: Error Keywords:
User: SYSTEM Computer: LP-7d230d987004
OpCode: Info
More Information: Event Log Online Help
Find event matching the given string


Event Viewer
File Action View Help
MSI and Script Number of events: 1,358 (!) New events available
Level Date and Time Source Event ID Task Category
Information 7/26/2024 8:10:07 AM AppLocker 8037 None
Information 7/26/2024 7:22:19 AM AppLocker 8038 None
Error 7/26/2024 7:22:19 AM AppLocker 8029 None
Information 7/26/2024 7:19:17 AM AppLocker 8038 None
Error 7/26/2024 7:19:17 AM AppLocker 8029 None
Information 7/26/2024 7:16:15 AM AppLocker 8038 None
Error 7/26/2024 7:16:15 AM AppLocker 8029 None
Information 7/26/2024 7:13:14 AM AppLocker 8038 None
Error 7/26/2024 7:13:14 AM AppLocker 8029 None
Information 7/26/2024 7:10:12 AM AppLocker 8038 None
Error 7/26/2024 7:10:12 AM AppLocker 8029 None
Information 7/26/2024 6:10:07 AM AppLocker 8037 None
Information 7/26/2024 5:50:23 AM AppLocker 8037 None
Information 7/26/2024 5:50:23 AM AppLocker 8037 None
Windows
AAD
All-User-Install-Agent
AllJoyn
AppHost
AppID
ApplicabilityEngine
Application Server-Applications
Application-Experience
AppLocker
EXE and DLL
MSI and Script
Packaged app-Deployment
Packaged app-Execution
AppModel-Runtime
AppReadiness
Apps
Apps-API
AppXDeployment
AppXDeployment-Server
AppXDeployment-Server-UndockedDeh
AppxPackagingOM
ASN1
AssignedAccess
AssignedAccessBroker
ATAPort
Audio
Authentication
Authentication User Interface
BackgroundTaskInfrastructure
BackgroundTransfer-ContentPrefetcher
Base-Filtering-Engine-Connections
Base-Filtering-Engine-Resource-Flows
Biometrics
BitLocker-API
Event 8029, AppLocker
General Details
C:\Windows\system32\config\systemprofile\AppData\Local\mdm\{E9F0372F-3E39-4793-905A-498751D686A2}.msi was prevented from running due to Config CI policy.
Log Name: Microsoft-Windows-AppLocker/MSI and Script
Source: AppLocker Logged: 7/26/2024 7:22:19 AM
Event ID: 8029 Task Category: None
Level: Error Keywords:
User: SYSTEM Computer: LP-7d230d987004
OpCode: Info
More Information: Event Log Online Help

```
11        </Rule>
12      </Rules>
13      <!--EKUS-->
14      <EKUs />
15      <!--File Rules-->
16      <FileRules />
17      <!--Signers-->
18      <Signers>
19        <Signer ID="ID_SIGNER_A_52B9BEC54643470999EE4163CEFD367D_1" Name=".NET Foundation Projects Code Signing CA">
20          <CertRoot Type="TBS" Value="B6D27A37A95C0A174C66496B3225B11A6250846BBC31FCA10D69D61F92DF5084" />
21          <CertPublisher Value="WiX Toolset (.NET Foundation)" />
22        </Signer>
23        <Signer ID="ID_SIGNER_B_F7EA725C0DB04E40806CAC8DF84D02D7_1" Name="Microsoft Code Signing PCA 2011">
24          <CertRoot Type="TBS" Value="F6F717A43AD9ABDDC8CEFDDE1C505462535E7D1307E630F9544A2D14FE8BF26E" />
25          <CertPublisher Value="Microsoft Corporation" />
26        </Signer>
27      </Signers>
28      <!--Driver Signing Scenarios-->
29      <SigningScenarios>
30        <SigningScenario Value="131" ID="ID_SIGNINGSCENARIO_DRIVERS_1" FriendlyName="Auto generated policy on 07-29-2024">
31          <ProductSigners />
32        </SigningScenario>
33        <SigningScenario Value="12" ID="ID_SIGNINGSCENARIO_WINDOWS" FriendlyName="Auto generated policy on 07-29-2024">
34          <ProductSigners>
35            <AllowedSigners>
```

Teams Meeting Add-in



Blogpost QR codes

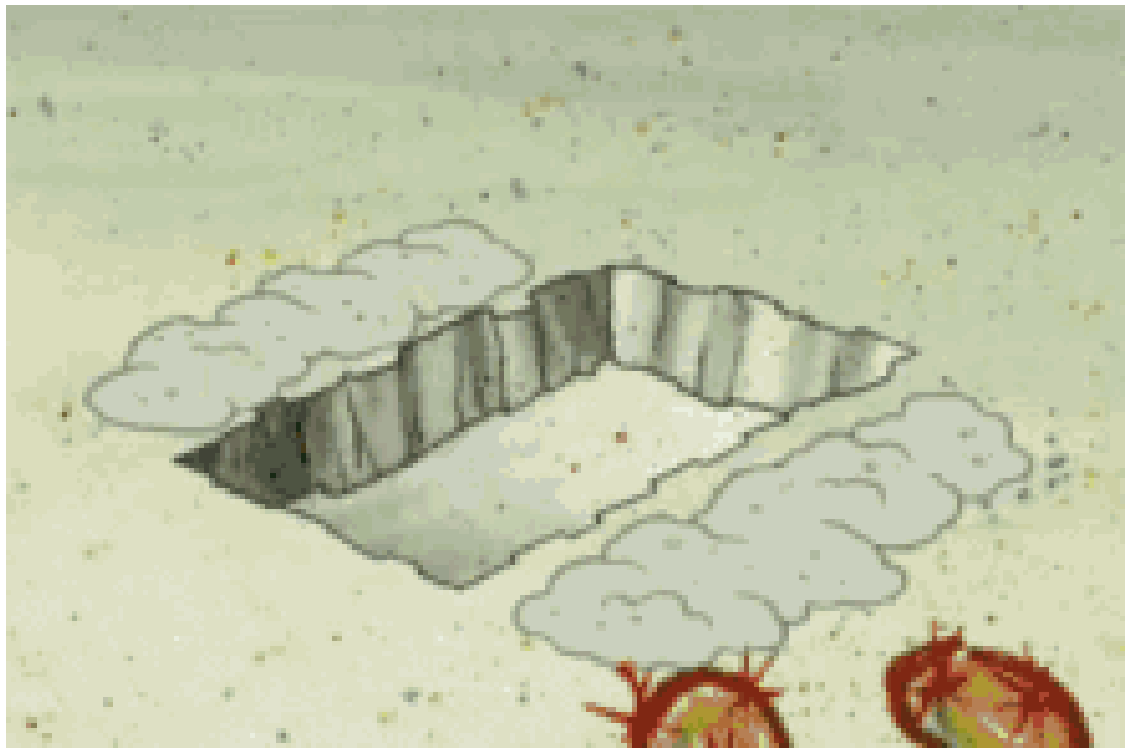
W365 blog

Teams Meeting Add-in

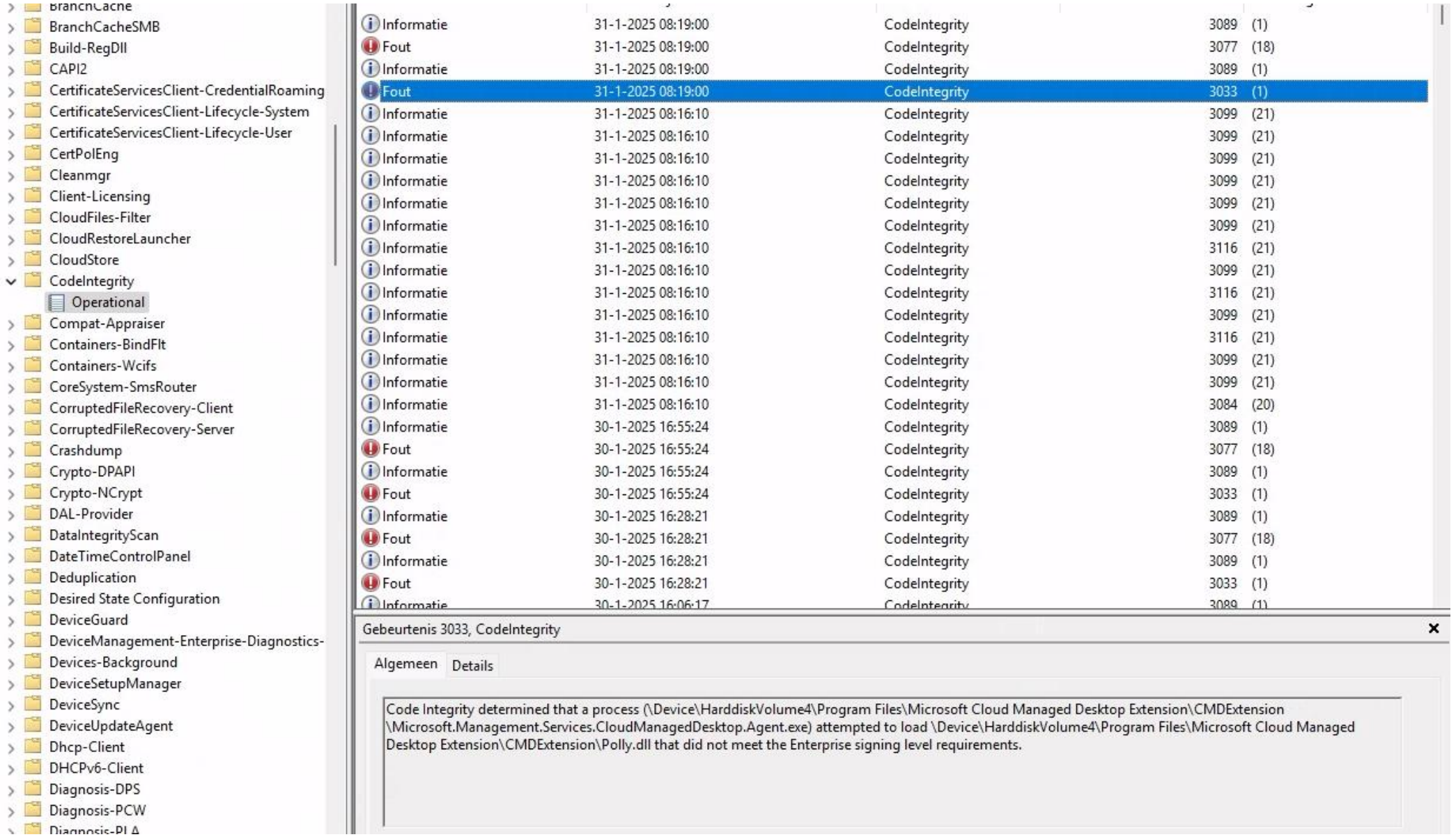
EPM


I'M


A FEW
MOMENTS LATER
VLIPSY



Cloud Managed Desktop Agent (Windows 365)



Probably EPM agent

- CloudRestoreLauncher
- CloudStore
- CodeIntegrity
  - Operational
- Compat-Appraiser
- Containers-BindFlt
- Containers-Wcifs
- CoreSystem-SmsRouter
- CorruptedFileRecovery-Client
- CorruptedFileRecovery-Server
- Crashdump
- Crypto-DPAPI
- Crypto-NCrypt
- DAL-Provider
- DataIntegrityScan
- DateTimeControlPanel
- Deduplication
- Desired State Configuration
- DeviceGuard
- DeviceManagement-Enterprise-Diagnostics-
- Devices-Background
- DeviceSetupManager
- DeviceSync
- DeviceUpdateAgent
- Dhcp-Client
- DHCPv6-Client
- Diagnosis-DPS
- Diagnosis-PCW
- Diagnosis-PLA

Informatie	30-1-2025 15:02:09	CodeIntegrity	3089	(1)
Fout	30-1-2025 15:02:09	CodeIntegrity	3033	(1)
Informatie	30-1-2025 14:34:38	CodeIntegrity	3089	(1)
Fout	30-1-2025 14:34:38	CodeIntegrity	3077	(18)
Informatie	30-1-2025 14:34:38	CodeIntegrity	3089	(1)
Fout	30-1-2025 14:34:38	CodeIntegrity	3033	(1)
Informatie	30-1-2025 14:34:32	CodeIntegrity	3089	(1)
Fout	30-1-2025 14:34:32	CodeIntegrity	3077	(18)
Informatie	30-1-2025 14:34:32	CodeIntegrity	3089	(1)
Fout	30-1-2025 14:34:32	CodeIntegrity	3033	(1)
Informatie	30-1-2025 14:30:04	CodeIntegrity	3089	(1)
Fout	30-1-2025 14:30:04	CodeIntegrity	3077	(18)
Informatie	30-1-2025 14:30:04	CodeIntegrity	3089	(1)
Fout	30-1-2025 14:30:04	CodeIntegrity	3033	(1)
Informatie	30-1-2025 14:27:51	CodeIntegrity	3099	(21)
Informatie	30-1-2025 14:27:51	CodeIntegrity	3099	(21)
Informatie	30-1-2025 14:27:51	CodeIntegrity	3099	(21)

Gebeurtenis 3033, CodeIntegrity

Algemeen | Details

Code Integrity determined that a process (\Device\HarddiskVolume4\Windows\System32\rundll32.exe) attempted to load \Device\HarddiskVolume4\Windows\Installer\MSI12A1.tmp-\WixToolset.Dtf.WindowsInstaller.dll that did not meet the Enterprise signing level requirements.

- CertificateServicesClient-Lifecycle-User
- CertPolEng
- Cleanmgr
- Client-Licensing
- CloudFiles-Filter
- CloudRestoreLauncher
- CloudStore
- CodeIntegrity
  - Operational
- Compat-Appraiser
- Containers-BindFlt
- Containers-Wcifs
- CoreSystem-SmsRouter
- CorruptedFileRecovery-Client
- CorruptedFileRecovery-Server
- Crashdump
- Crypto-DPAPI
- Crypto-NCrypt
- DAL-Provider
- DataIntegrityScan
- DateTimeControlPanel
- Deduplication
- Desired State Configuration
- DeviceGuard
- DeviceManagement-Enterprise-Diagnostics-
- Devices-Background
- DeviceSetupManager
- DeviceSync
- DeviceUpdateAgent
- Dhcp-Client
- DHCPv6-Client
- Diagnosis-DPS

Informatie	30-1-2025 15:38:13	CodeIntegrity	3089	(1)
Fout	30-1-2025 15:38:13	CodeIntegrity	3033	(1)
Informatie	30-1-2025 15:02:09	CodeIntegrity	3089	(1)
Fout	30-1-2025 15:02:09	CodeIntegrity	3077	(18)
Informatie	30-1-2025 15:02:09	CodeIntegrity	3089	(1)
Fout	30-1-2025 15:02:09	CodeIntegrity	3033	(1)
Informatie	30-1-2025 14:34:38	CodeIntegrity	3089	(1)
Fout	30-1-2025 14:34:38	CodeIntegrity	3077	(18)
Informatie	30-1-2025 14:34:38	CodeIntegrity	3089	(1)
Fout	30-1-2025 14:34:38	CodeIntegrity	3033	(1)
Informatie	30-1-2025 14:34:32	CodeIntegrity	3089	(1)
Fout	30-1-2025 14:34:32	CodeIntegrity	3077	(18)
Informatie	30-1-2025 14:34:32	CodeIntegrity	3089	(1)
Fout	30-1-2025 14:34:32	CodeIntegrity	3033	(1)
Informatie	30-1-2025 14:30:04	CodeIntegrity	3089	(1)
Fout	30-1-2025 14:30:04	CodeIntegrity	3077	(18)
Informatie	30-1-2025 14:30:04	CodeIntegrity	3089	(1)
Fout	30-1-2025 14:30:04	CodeIntegrity	3033	(1)
Informatie	30-1-2025 14:27:51	CodeIntegrity	3099	(21)
Informatie	30-1-2025 14:27:51	CodeIntegrity	3099	(21)
Informatie	30-1-2025 14:27:51	CodeIntegrity	3099	(21)
Informatie	30-1-2025 14:27:51	CodeIntegrity	3099	(21)

Gebeurtenis 3033, CodeIntegrity

Algemeen | Details

Code Integrity determined that a process (\Device\HarddiskVolume4\Windows\System32\rundll32.exe) attempted to load \Device\HarddiskVolume4\Windows\Installer\MSI5C90.tmp-0\Microsoft.Deployment.WindowsInstaller.dll that did not meet the Enterprise signing level requirements.

Tools

Tools

- App Control Wizard
- App Control Manager
- Aaronlocker

Tips & Tricks

EventLogs

- Applications and Services logs - Microsoft - Windows - CodeIntegrity - Verbose
- Applications and Services logs - Microsoft - Windows - AppLocker - EXE and DLL
- Applications and Services logs - Microsoft - Windows - AppLocker - Packaged app-Deployment
- Applications and Services logs - Microsoft - Windows - AppLocker - Packaged app-Execution
- Applications and Services logs - Microsoft - Windows - AppID - Operational
- Applications and Services logs - Microsoft - Windows - CAPI2 - Operational
- Applications and Services logs - Microsoft - Windows - DeviceGuard - Operational
- *Applications and Services logs - Microsoft - Windows - PowerShell - **
- *Windows - Application*
- *Windows - System*

Defender for Endpoint

Advanced hunting

Help resources | Query resources report | Schema refere

New query*

Schema | Functions | Queries

Search

Favorites

Your favorites list is empty. To add a schema, click the schema menu and select "Add to Favorites"

Alerts & behaviors

- AlertEvidence
- AlertInfo
- BehaviorEntities
- BehaviorInfo

Apps & identities

- AADSignInEventsBeta
- AADSpnSignInEventsBeta
- CloudAppEvents
- IdentityInfo
- IdentityLogonEvents

Run query | Last 7 days | Save | Share link | Create detection rule

Query

```
1  DeviceEvents
2  | where ActionType startswith "AppControlCodeIntegrity"
3  |   or ActionType startswith "AppControlCIScriptBlocked"
4  |   or ActionType startswith "AppControlCIScriptAudited"
```

Getting started | Results | Query history

Export | Link to incident | Take actions | Show empty columns | 1 of 22 selected | Search | 00:00.535 | Low | Chart type | Full screen

Filters: Add filter

Timestamp	DeviceId	DeviceName	ActionType	FileName	FolderPath	SHA1
13 Jan 2025 13:14:...	62ba7e78bc49f62b6...	desktop-j1rjfke	AppControlCodeIntegrit...			e7f6ded001bc17dbc...
13 Jan 2025 13:14:...	62ba7e78bc49f62b6...	desktop-j1rjfke	AppControlCodeIntegrit...			e7f6ded001bc17dbc...
13 Jan 2025 13:14:...	62ba7e78bc49f62b6...	desktop-j1rjfke	AppControlCodeIntegrit...	7z2409-x64.exe	\Users\nt\Downloads	
13 Jan 2025 13:14:...	62ba7e78bc49f62b6...	desktop-j1rjfke	AppControlCodeIntegrit...	7z2409-x64.exe	\Device\HarddiskVolum...	e7f6ded001bc17dbc...
13 Jan 2025 12:46:...	62ba7e78bc49f62b6...	desktop-j1rjfke	AppControlCodeIntegrit...	System.Windows.Forms....	\Windows\assembly\Na...	

ManagedInstaller on AVD

Driver blocklist failes – Blocklist Microsoft

Dell drivers

Conclusion/Questions