



Microsoft Intune in 2024

Niklas Tinner - #WPNINJAUGCH





Thank you Sponsors



EPIC FUSION
BRING IT ALL TOGETHER



Niklas Tinner

Focus
Senior Endpoint Engineer @baseVISION

From
Switzerland 

My Blog
Oceanleaf.ch 



Interests
Cars, watches, technology

Contact
  @Niklas Tinner



Agenda

● Intune Suite

Vorstellung der relevanten Features & Vergleich

● Endpoint Privilege Management

Demo

● Feature Gewinner

Meine Top 5

Key takeaways:

- **Verstehen der Intune Suite Features und deren Anwendung**
- **Abgleich des eigenen Wissen/Umgebung mit Session**



Was sind eure aktuellen Highlights aus
Intune?



Intune 1 0 1

- Greenfield starten / umdenken
- Entra Join only
- Keep it simple! & running by automation
- First-party Strategie
- Fokus auf Sicherheit

Alles ist möglich, aber es erfordert neues Denken & Engineering!



Technical “Secret Sauce” for Intune

Automation

- Microsoft Graph
- Automation Accounts
- Logic Apps
- Enterprise Apps

Reporting & Monitoring

- Diagnostics settings
- Log Analytics Workspace logs
- Workbooks

Stay up to date!

Intune Suite

Was wisst ihr?





Inhalte



Specialty device
management



Remote
Help

Tunnel for Mobile App
Management

Endpoint Privilege
Management

February 2024

Microsoft Intune
Advanced Analytics

Microsoft Intune Enterprise
Application Management

Microsoft Cloud PKI



Intune Suite Vergleich

Bisher durch 3 rd party Produkt	Intune Suite	Integrated cloud benefit
PatchMyPC	Enterprise App Management	<ul style="list-style-type: none">• Integriert in Intune
Interne PKI	Microsoft Cloud PKI	<ul style="list-style-type: none">• Keine lokale Infrastruktur zur Betreuung• Gesicherte zertifikats-basierte Authentifizierung
Teamviewer	Remote Help	<ul style="list-style-type: none">• Integration zu Intune und Entra
CyberArk EPM	Endpoint Privilege Management	<ul style="list-style-type: none">• Single-pane of glass experience
VPN	Tunnel for Mobile App Management	<ul style="list-style-type: none">• VPN per App, keine Gerätekonfiguration



Notes from the field

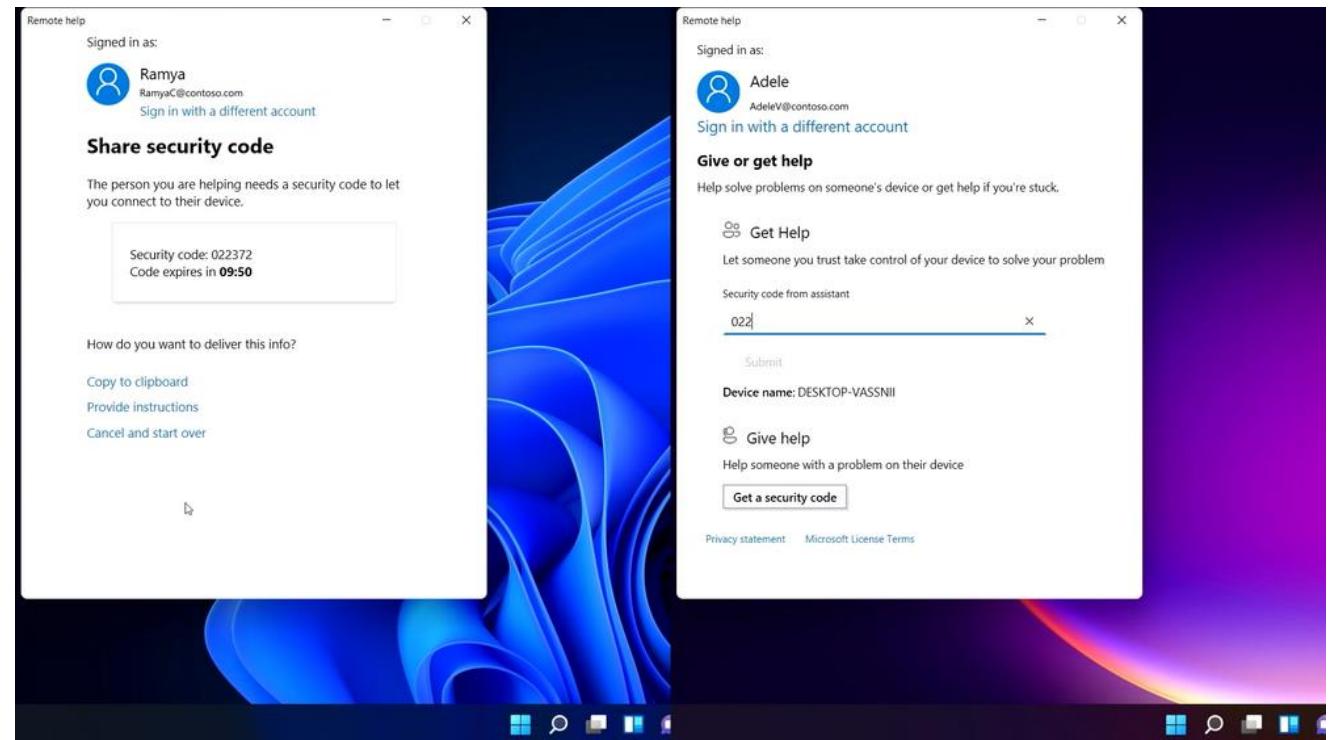
- Endpoint Privilege Management
 - Findet mehr und mehr Kundeninteresse
 - Geringe Konfigurationsoptionen ≠ geringe Möglichkeiten für das Feature
 - Fehlende Features (Support-approved, MSI support ...)
- Andere Features sind oft zu teuer für Kunden und haben zu wenig Möglichkeiten (es gibt aber Verhandlungspotential 😊)





Remote Help

- Cloud-basierte Remote-Unterstützung / Support Szenario
- Integriert in Entra ID für IAM
- Nativ mit Intune
 - Launch session
 - Compliant device check





Enterprise App Management

Wieso ?

-Wer patcht alle Sicherheitslücken und bietet Updates für die Apps?

Wie 🛡️

-Eigener App Katalog von Microsoft

Benefit 🏆

-Simplifizieren
-Update Patches sichern (Vulnerability Management)



Cloud PKI

Wieso ?

- PKI ist komplex und operativ teuer, oft falsch konfiguriert
- 802.1x basierte Authentifizierung

Wie 🌐

- Intune bietet eine Trusted Root CA und einen SCEP Endpunkt

Benefit 🏆

- Verwaltete PKI, kein Aufwand



Endpoint Privilege Management

Wieso ?

-Keine lokale Adminberechtigungen für Enduser notwendig >
Anwendungsspezifische Elevation

Wie 🛡️

-Intune Policies spezifizieren Dateien welche mit erhöhten Berechtigungen
ausgeführt werden dürfen

Benefit 🏆

-Sicherheit auf Endgeräten erhöhen und Supportanfragen verringern



Demo

Microsoft Intune admin center

Home > Endpoint security

Endpoint security | Endpoint Privilege Management

Search

Reports Policies

Overview

Endpoint Privilege Management is now generally available. To use this add-on, your Global or Billing Administrator can start a trial or buy licenses.

Create Policy Refresh Export

Search by profile name

Policy name	Policy type	Assigned	Platform	Target
No results				

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint Privilege Management
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access



Demo

- Elevation rules policy

- Evaluation types

- User confirmed
 - Business justification
 - Windows Auth
- Automatic

- Mehr File Eigenschaften
- Hash
- Zertifikat

Home > Endpoint security | Endpoint Privilege Management > Opt-EndpointSecurity-Rules-AdminTools >

Edit profile - Opt-EndpointSecurity-Rules-AdminTools ...

Settings catalog

① Configuration settings ② Review + save

Privilege Management

Elevation Rules set the conditions for allowing users to get just-in-time access to apps and files on their devices.

+ Add Delete Elevation Rule Name

Elevation type	Rule name	Configure settings
<input type="checkbox"/>	CMD	+ Edit instance
<input type="checkbox"/>	PowerShell	+ Edit instance

Rule properties

Elevation rules policy

Rule name *

PowerShell

Description ⓘ

Elevation conditions

Elevation type *

User confirmed

Validation

Business justification

Child process behavior

Require rule to elevate

File information

Using the principle of least privilege, provide properties that apply to the trusted apps you want to let have elevated privileges. If the rule is too broad, there can be unintended elevations. [Learn more about elevation rules](#)

⚠ This rule could increase the security risk for your organization by allowing a wide range of apps to have elevated privileges. Try adding more file attributes to narrow the scope of this rule.

File name

powershell.exe

File path

C:\Windows\System32\WindowsPow...

Signature source

Use a certificate file in reusable s...

Certificate *

Certificate selected

+ Add or remove a certificate

Certificate type *

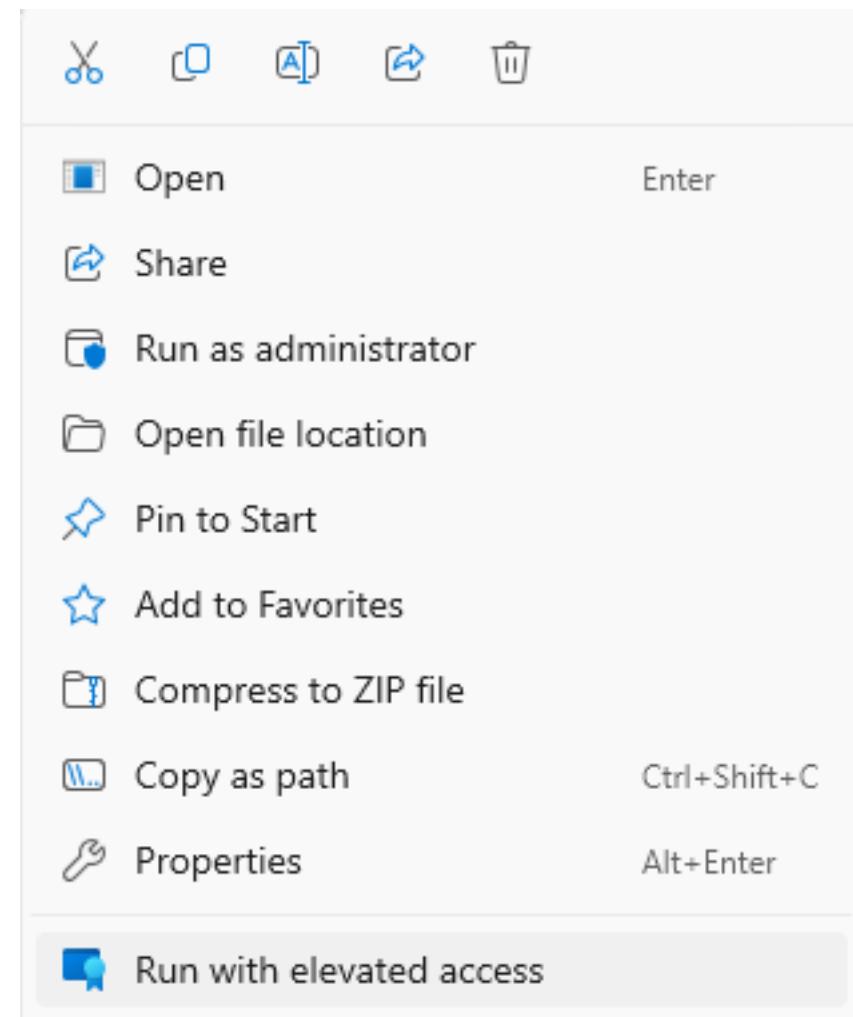
Certificate authority

File hash ⓘ



Demo

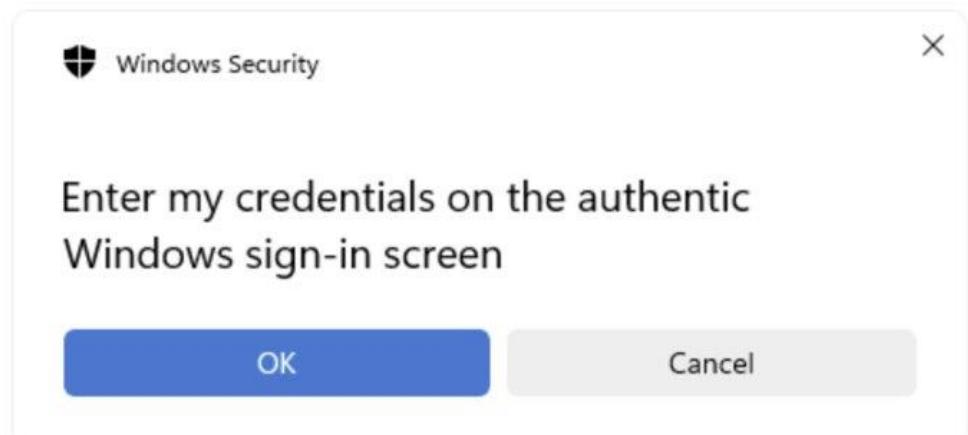
Natives "rechtsklick" Menu erhält neuen Punkt





Demo

Wenn eine Policy für die Datei vorhanden ist, wird EPM ausgeführt und die Validation kann durch den Enduser ausgeführt werden.



Endpoint Privilege Management

Open this app as administrator?

powershell
Verified publisher: Microsoft Windows

Enter business justification
Need to run xyz
15/280

You'll have administrator access to this app.

This information will be sent to your organization's IT admin. [Privacy info](#)

Cancel Continue

Feature Gewinner





Unified Settings Management mit Defender for Endpoint

How does it work?

Wieso ?

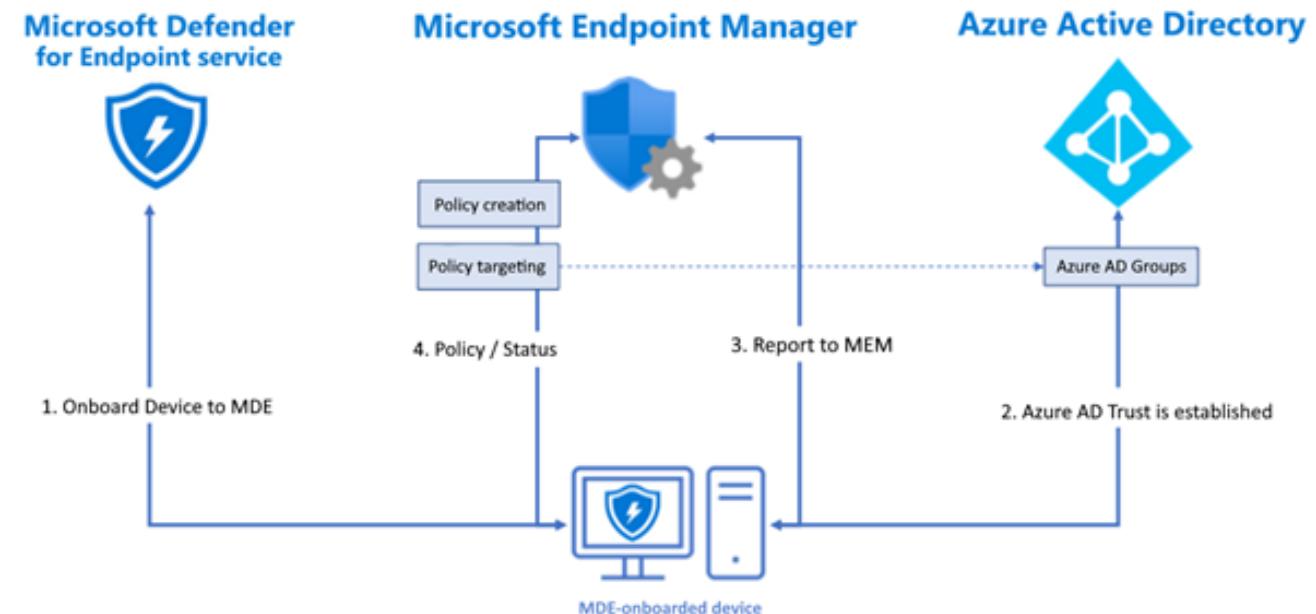
-Zentrale Verwaltung von Security Policies

Wie 🛡️

-Intune connector + MDE onboarding

Benefit 🏆

-Nicht Intune-verwaltete Geräte mit Security ausstatten (macOS,





Driver & firmware update management

Wieso ?

-Bisher keine Möglichkeit

Wie

-WUfB-DS Policies

Benefit

-Commercial Control
für Treiber
(Optionale Updates)

Home > Devices | Driver updates for Windows 10 and later >
Windows-COPE-DriverUpdate-Report ...

Manual approval driver update policy

Sync Delete

Last sync: 03.07.2023, 13:59:46

Properties Recommended drivers Other drivers

Refresh Columns Export

Search Add filter

Showing 1 to 34 of 34 records

Driver name ↑	Version ↑↓	Manufacturer ↑↓	Driver class ↑↓	Release date ↑↓	Status ↑↓	First Deplo... ↑↓	Applicable devices ↑
Intel Corporation - Bluetooth - 22.160.0.4	22.160.0.4	Intel Corporation	OtherHardware	8/25/2022	Needs review	1/0/1	62
Intel - SoftwareComponent - 1.63.1155.1	1.63.1155.1	Intel	OtherHardware	12/17/2021	Needs review	1/0/1	113
Intel - System - 2131.1.4.0	2131.1.4.0	Intel	OtherHardware	11/25/2021	Needs review	1/0/1	118
Intel - SoftwareComponent - 1.41.2021.121	1.41.2021.121	Intel	OtherHardware	3/25/2021	Needs review	1/0/1	48
Intel - Ports - 2131.1.73.0	2131.1.73.0	Intel	OtherHardware	12/30/2021	Needs review	1/0/1	120
Intel - net - 22.160.0.4	22.160.0.4	Intel Corporation	Networking	9/11/2022	Needs review	1/0/1	32
Intel - SoftwareComponent - 2130.1.16.1	2130.1.16.1	Intel	OtherHardware	11/30/2021	Needs review	1/0/1	114
ASIX - Net - 2.20.10.0	2.20.10.0	ASIX	Networking	5/30/2023	Needs review	1/0/1	41
Fibocom Wireless Inc. - Sensor - 4.19042.6.6	4.19042.6.6	Fibocom Wireless Inc.	OtherHardware	3/31/2023	Needs review	1/0/1	26

Manage driver

Intel Corporation - Bluetooth - 22.160.0.4

Manage the approval status for this driver. Save any changes to apply them to the driver.

Current status: Needs review

Devices installed: N/A

Additional details

Actions: Decline, Decline, Approve



Windows LAPS



Wieso ?

-Legacy LAPS unterstützt kein Entra Join

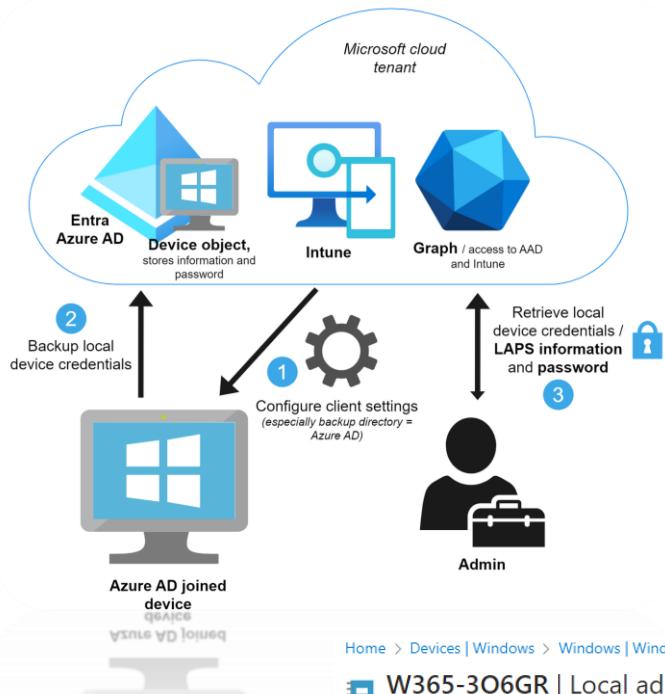
Wie

-Intune policy/GPO

Benefit

-Schutz vor

lateral-traversal attacks



Home > Devices | Windows > Windows | Windows devices > W365-30

W365-306GR | Local admin password

Search Refresh Got feed Learn more about Local Adi Local administrator pass... Show local administrator pass...

Overview Properties Monitor Performance (preview) Hardware Discovered apps Device compliance Device configuration App configuration Local admin password

Local administrator password

Account name	ladmin
Security ID	S-1-5-21-200505706-3673728020-2588066601-1000
Local administrator password	27Xe85ww@b pA7
Last password rotation	11/12/2023, 5:40:42 PM
Next password rotation	12/12/2023, 5:40:41 PM



macOS management



→ Wieso sollte man Macs verwalten?

- 🚀 Microsoft investiert in eine **zero-day support** Strategie für macOS
- 💡 **Feature Gleichheit**, Intune + Defender + Entra = Feature Gleichheit für alle OS
- 🏆 Motivator für «**Modern Workplace**» und Motivatoren für IT & End user



Windows 365

Ein Cloud PC ist eine virtuelle Windows Instanz, mit monatlicher Abrechnung, integriert in das Microsoft Ökosystem.



- **Verwaltet aus Intune** > Single-pane of glass experience 😎
 - Content übernehmen (Policies, Apps)
 - Wissen übernehmen
 - Kosten reduzieren
- **Nativ integriert mit Windows** 
 - Windows 365 Boot & Switch
 - Windows App
- **Workloads zu Microsoft verlagert**
 - “VDI” Plattform Betrieb & Wartung
 - Image Bereitstellung & Pflege





How to stay up to date



Community!

Events, Twitter, LinkedIn, Blogs (oceanleaf.ch 😊)

Offizielle Seiten

Tech Community, aka.ms/IntunelD

Message Center

Störungen / Ankündigungen

CCP

<https://aka.ms/joinccp> - NDA = Voraussetzung



Ask me Anything

Eure Erfahrungen?



Tipps & Tricks?

Was plant ihr?