



November 13-15, Oslo Spektrum

# Ronni Pedersen & Jörgen Nilsson

10 Intune tips that will make your admin life easier

# About me..



## Jörgen Nilsson

- Principal Consultant, Onevinn
- Microsoft MVP: Security
- Microsoft Certified Trainer (MCT)

## Contact Info

- Mail: [Jorgen.nilsson@onevinn.se](mailto:Jorgen.nilsson@onevinn.se)
- X: @ccmexec

# About me...



## Ronni Pedersen

- Cloud Architect, APENTO
- Microsoft MVP: Security + Windows
- ITIL Certified
- Microsoft Certified Trainer (MCT)

## Contact Info

- Mail: [rop@apento.com](mailto:rop@apento.com)
- Twitter (X): [@ronnipedersen](https://twitter.com/ronnipedersen)

Cloud Native...

# Aim for 100% Cloud Native

## Security & Compliance

- AI and Automation
- Zero Trust
- Secure Device (No identity)

## Performance / End User Experience

- Fast boot and logon time
- Provision and policy update from anywhere

## Simple Management

- Cross-platform
- No infrastructure
- Reduced complexity (Conflicts)



Licensing...

# Licensing

- Let's be honest... You need to buy more than just Intune P1
  - 90% of you needs the full EMS E5 suite if you want to stay secure...
  - And/or buy 3<sup>rd</sup>. party solutions (add-ons)
- Microsoft E5 Security
  - Insights on vulnerabilities
- Microsoft Intune Suite
  - Advanced Insight Analytics
  - Device Query
  - Remote Help
  - New features...





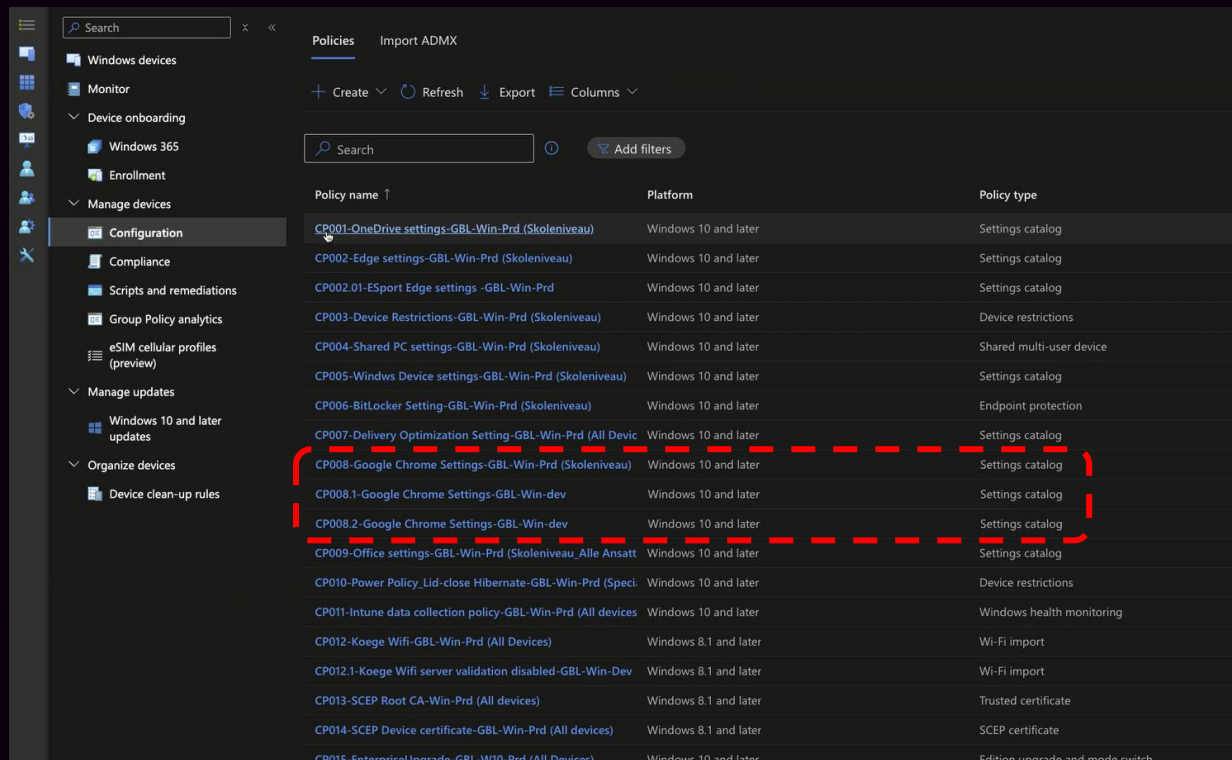
# Governance, Standards, Documentation, Process

# Microsoft Intune and Governance

- Well documented processes and standards
- Naming convention/version management
  - Whatever works for you are great!
  - Just make sure everyone is following the same standard!
- Change Management
  - Documentation is key...
  - The “Why” is important



# Naming Standards (examples)



The screenshot shows the Microsoft Intune console with the 'Policies' tab selected. The left sidebar shows the navigation menu with 'Configuration' highlighted. The main area displays a table of policies. A red dashed box highlights the policy 'CP008-Google Chrome Settings-GBL-Win-Prd (Skoleniveau)'.

Policy name ↑	Platform	Policy type
CP001-OneDrive settings-GBL-Win-Prd (Skoleniveau)	Windows 10 and later	Settings catalog
CP002-Edge settings-GBL-Win-Prd (Skoleniveau)	Windows 10 and later	Settings catalog
CP002.01-ESport Edge settings -GBL-Win-Prd	Windows 10 and later	Settings catalog
CP003-Device Restrictions-GBL-Win-Prd (Skoleniveau)	Windows 10 and later	Device restrictions
CP004-Shared PC settings-GBL-Win-Prd (Skoleniveau)	Windows 10 and later	Shared multi-user device
CP005-Windows Device settings-GBL-Win-Prd (Skoleniveau)	Windows 10 and later	Settings catalog
CP006-BitLocker Setting-GBL-Win-Prd (Skoleniveau)	Windows 10 and later	Endpoint protection
CP007-Delivery Optimization Setting-GBL-Win-Prd (All Devices)	Windows 10 and later	Settings catalog
CP008-Google Chrome Settings-GBL-Win-Prd (Skoleniveau)	Windows 10 and later	Settings catalog
CP008.1-Google Chrome Settings-GBL-Win-dev	Windows 10 and later	Settings catalog
CP008.2-Google Chrome Settings-GBL-Win-dev	Windows 10 and later	Settings catalog
CP009-Office settings-GBL-Win-Prd (Skoleniveau, Alle Ansatt)	Windows 10 and later	Settings catalog
CP010-Power Policy Lid-close Hibernate-GBL-Win-Prd (Speci)	Windows 10 and later	Device restrictions
CP011-Intune data collection policy-GBL-Win-Prd (All devices)	Windows 10 and later	Windows health monitoring
CP012-Koege Wifi-GBL-Win-Prd (All Devices)	Windows 8.1 and later	Wi-Fi import
CP012.1-Koege Wifi server validation disabled-GBL-Win-Dev	Windows 8.1 and later	Wi-Fi import
CP013-SCEP Root CA-Win-Prd (All devices)	Windows 8.1 and later	Trusted certificate
CP014-SCEP Device certificate-GBL-Win-Prd (All devices)	Windows 8.1 and later	SCEP certificate
CP015-EnterprisseUpgrade-GBL-W10-Prd (All Devices)	Windows 10 and later	Edition upgrade and mode switch

Win - OIB - Credential Management - D - Passwordless - v3.1

Win - OIB - Defender Antivirus - D - Additional Configuration - v3.1

Win - OIB - Device Security - D - Audit and Event Logging - v3.1

Win - OIB - Device Security - D - Enhanced Phishing Protection - v3.0

Win - OIB - Device Security - D - Local Security Policies - v3.0

Win - OIB - Device Security - D - Login and Lock Screen - v3.1

Win - OIB - Device Security - D - Remote Desktop Services and RPC - v3.0

Win - OIB - Device Security - D - Security Hardening - v3.1

Win - OIB - Device Security - D - Timezone - v3.1

Win - OIB - Device Security - D - User Rights - v3.1

Win - OIB - Device Security - D - Windows Subsystem for Linux - v3.1

Win - OIB - Device Security - U - Device Guard, Credential Guard and HVCI - v3.1

Win - OIB - Device Security - U - Power and Device Lock - v3.0

Win - OIB - Device Security - U - Windows Spotlight and Org Messages - v3.0

Win - OIB - Google Chrome - D - Security - v3.0

Win - OIB - Google Chrome - U - Experience and Extensions - v3.0

Win - OIB - Google Chrome - U - Profiles, Sign-In and Sync - v3.0

Win - OIB - Health Monitoring - D - Endpoint Analytics and Windows Updates - v3.0

Win - OIB - Internet Explorer (Legacy) - D - Security - v3.1.1

Win - OIB - Microsoft Accounts - U - Configuration - v3.0

Win - OIB - Microsoft Edge - D - Security - v3.0

# Policy Grouping

Policy name ↑	Platform	Policy type
CP001-Windows OS Hardening-Win-GBL-Prd	Windows 10 and later	Settings catalog
CP002-Personal Data Encryption-W11-GBL-Prd	Windows 10 and later	Custom
CP002.1-Disable kernel-mode crash dumps and live dumps-W11-GBL-Prd	Windows 10 and later	Settings catalog
CP002.2-Disable Winlogon automatic restart sign-on-W11-GBL-Prd	Windows 10 and later	Administrative templates
CP002.3-Disable Windows Error Reporting (WER)/Disable user-mode crash dumps-Win-GBL-Prd	Windows 10 and later	Settings catalog
CP002.4-Disable hibernation-W11-GBL-Prd	Windows 10 and later	Settings catalog
CP002.5-Disable password when resuming from connected standby-W11-GBL-Prd	Windows 10 and later	Settings catalog
CP003-Intune data collection policy-Win-GBL-Prd	Windows 10 and later	Windows health monitoring
CP004-Win11 Start Menu customization-W11-GBL-Prd	Windows 10 and later	Custom
CP005-SmartScreen Enhanced Phishing Protection-Win11-GBL-Prd	Windows 10 and later	Settings catalog
CP006-Windows Hello for Business cloud Kerberos trust-W11-GBL-Prd	Windows 10 and later	Settings catalog
CP007-Credentials Delegation, Remote Credential Guard-W11-GBL-Prd	Windows 10 and later	Settings catalog
CP007.1-DISABLE Credentials Delegation, Remote Credential Guard-W11-GBL-Prd	Windows 10 and later	Settings catalog
CP008-Remove Chat Icon-W11-GBL-Prd	Windows 10 and later	Settings catalog
CP009-Onedrive Sign-in and move known folders-W11-GBL-Prd	Windows 10 and later	Settings catalog
CP009.1-Onedrive SharePoint IT-og-Digitaliseringsafdelingen-AFD-W11-GBL-Prd	Windows 10 and later	Settings catalog
CP010-Edge settings-GBL-Win-Prd	Windows 10 and later	Settings catalog

# Intune Naming Convention (Example)

## 9.1 Intune Naming Convention

To ensure structure in Intune the following Naming Convention will be used for all Profiles.

{TYPExxx.y}-{USE}-{Platform}-{Ownership}-{RING}

(Ownership)

- GBL: Global
- KOL: Kolding
- DK: Denmark

{Platform}

- Win: Windows 10/11
- W10: Windows 10
- W11: Windows 11
- iOS
- Android
- 

{TYPExxx(y)}

- Xxx: is a consecutive number for each Type. **Numbers can be reused when an old rule is deleted**
- (y) is only added if a given profile is duplicated then.
- AC: Application Control
- AP: Account Protection
- ASR: Attack Surface Reduction
- CA: Conditional Access
- CP: Configuration Profile
- DS:Device Script
- DCP: Device Compliance Policy
- DE: Disk Encryption
- EDR: Endpoint Detection and Response
- ESP: Enrolment Status Page
- FW: Firewall
- PR: Proactive Remediation

Ownership is important when customers are using RBAC

{USE}

Description of the policy i.e (shown with Type)

- DE - Default Bitlocker with TPM
- ASR-Block abuse of exploited vulnerable signed drivers (Device)

{RING}

- PRD
- DEV

Examples:

{TYPExxx.y}-{USE}-{Platform}-{Ownership}-{RING}

- ASR001-Block abuse of exploited vulnerable signed drivers (Device)-GBL-Win-Prd
- ASR001.1-Block abuse of exploited vulnerable signed drivers (Device)-GBL-Win-DEV
- DP001-Default Compliance-GBL-W11-PRD



## ID Design Decisions

#	Decision Point	Decision	Justification
ID1	<a href="#">Enabling Passwordless sign-in</a>	All Win11 users will be enabled for Password less sign-in, and Hello for Business will be used to facilitate password less sign-in on Win11 devices. The end-goal is to completely eliminate passwords from the Identity directories.	Passwords are a primary attack vector. Bad actors use social engineering, phishing, and spray attacks to compromise passwords. A <a href="#">passwordless</a> authentication strategy mitigates the risk of these attacks.
ID2	<a href="#">Windows Hello for Business</a>	Windows Hello for Business will be required on all Win11 endpoints. Device compliance policies will be used to check that Windows Hello is enabled on all Win11 endpoints.	Windows Hello for Business will ensure that a PIN/biometric is used to log-in to all Win11 devices instead of a Password. As the PIN/Biometric is device specific it can't be used without the specific device that it was created for
ID3	<a href="#">Temporary access pass</a>	Temporary access pass will be used to provide a temporary password that can be used to enabled <a href="#">passwordless</a> phone sign-in.	
ID4	<a href="#">Cloud Trust</a>	Cloud Kerberos trust will be enabled in	The sur... all Active A... joined devices

# Policy Design

	A	B	C	F	G
1	Policy	Setting name	Default setting	Customer Implemented Setting	Design Decision / Justification
2	DCP001-Default Compliance Policy immediately				
3				<a href="https://www.imab.dk/use-custom-compliance-settings-in-microsoft-intune-to-require-windows-hello-enrollment/Hello-for-Business">https://www.imab.dk/use-custom-compliance-settings-in-microsoft-intune-to-require-windows-hello-enrollment/Hello-for-Business</a>	ID2
4		Custom Compliance	Not Configured	Require	OS7
5		Require BitLocker:	Not Configured	Not Configured	HS3,HS4,OS1
6		Require Secure Boot to be enabled on the device:	Not Configured	Not Configured	HS3
6		Require code integrity:	Not Configured	Require	HS3

# Policy Deployment

Home > Devices | Windows > Windows

## Windows | Compliance

Search

Windows devices

Monitor

Device onboarding

- Windows 365
- Enrollment

Manage devices

- Configuration
- Compliance**
- Scripts and remediations
- Compliance analytics

December 31st, 2024 marks the end of Microsoft Intune support for Android devices. [Learn more about ending support for Android device administrator.](#)

+ Create policy Refresh Export Columns

Search

Platform or OS: Windows

Policy name	Platform or OS
DCP001.1-Default Compliance Policy-W11-GBL-DEV	Windows 10 and later
DCP002.1-Default Compliance Policy 1 day	Windows 10 and later
W10-D-Version Compliance	Windows 10 and later

Home > Windows | Compliance > DCP001.1-Default Compliance Policy-W11-GBL-DEV >

## Windows 10/11 compliance policy

Windows 10 and later

1 Compliance settings 2 Review + save

Custom Compliance

Custom compliance **Require** Not configured

Select your discovery script [Get-WindowsHelloStatus](#)

Upload and validate the JSON file with your custom compliance settings

Setting name	Operator	Value
WHFBEnrollmentStatus	isEquals	ENROLLED

```
1 {
2   "Rules": [
3     {
4       "SettingName": "WHFBEnrollmentStatus",
5       "Operator": "IsEquals",
6       "DataType": "String",
7       "Operand": "ENROLLED",
8       "MoreInfoUrl": "https://imab.dk",
9       "RemediationStrings": [
10        {
11          "Language": "en-US",
12          "Title": "Windows Hello for Business must be enrolled",
13          "Description": "Windows Hello for Business must be enrolled"
14        }
15      ]
16     }
17   ]
18 }
```

Device Health





# DESKTOP-9SECHR9 | Device configuration ...

Overview

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Local admin password

Recovery keys

User experience

Device diagnostics

Group membership

Managed Apps

Filter evaluation

Enrollment

Remediations (preview)

Device query

Recently updated information can take up to 20 minutes to be available in this report.

Refresh Export Columns

Policy ↑

Logged in user

Policy type

State

Windows - Disable CoPilot

Settings Catalog

✓ Succeeded

Windows - Disable CoPilot

Settings Catalog

✓ Succeeded

Windows - Disable CoPilot

Settings Catalog

✓ Succeeded

Windows - EPM - Default Allow Elevation - U - V1.0

Settings Catalog

✓ Succeeded

Windows - EPM - Elevate 7zip - U - V1.0

Settings Catalog

✓ Succeeded

Windows - EPM - Elevate VSCode - U - V1.0

Settings Catalog

✓ Succeeded

Windows - ESP - SkipUserStatusPage

Device configuration

✓ Succeeded

Windows - ESP - SkipUserStatusPage

Device configuration

✓ Succeeded

Windows - ESP - SkipUserStatusPage

Device configuration

✓ Succeeded

Windows - Edge v125 Sec Baseline Plus Meny - D -V1

Settings Catalog

✓ Succeeded

Windows - Edge v125 Sec Baseline Plus Meny - D -V1

Settings Catalog

✓ Succeeded

Windows - Enable RDP

Settings Catalog

✓ Succeeded

Windows - Enable RDP

Microsoft Defender Firewall Rules

✓ Succeeded

Windows - Enable SSPR

Device configuration

✓ Succeeded

Windows - Enable SSPR

Device configuration

✓ Succeeded

Windows - Enable SSPR

Device configuration

✓ Succeeded

# Adopt Security baselines

# Security Baselines

- Security Baseline for Windows 10 and later
- Security Baseline for Microsoft Edge
- Windows 365 Security Baseline
- Microsoft Defender for Endpoint Security Baseline
- Microsoft 365 Apps for Enterprise Security Baseline

Intune policies are the way to go as we get status back for each setting.

- The security baselines have been around for many many years....

# Adopting baselines

- Recommendation: Move settings to dedicated security policies under Endpoint Security
  - BitLocker
  - Defender
  - Firewall
  - ASR rules
- Unexpected reboot during Autopilot
  - Target User or Devices?
  - Move the settings that cause the issue to user targeting:
    - Credential guard
    - Device Lock
    - DMA Guard
    - Lock screen

## Configuration settings [Edit](#)

✓ Administrative Templates

✓ Device Guard

✓ Device Lock

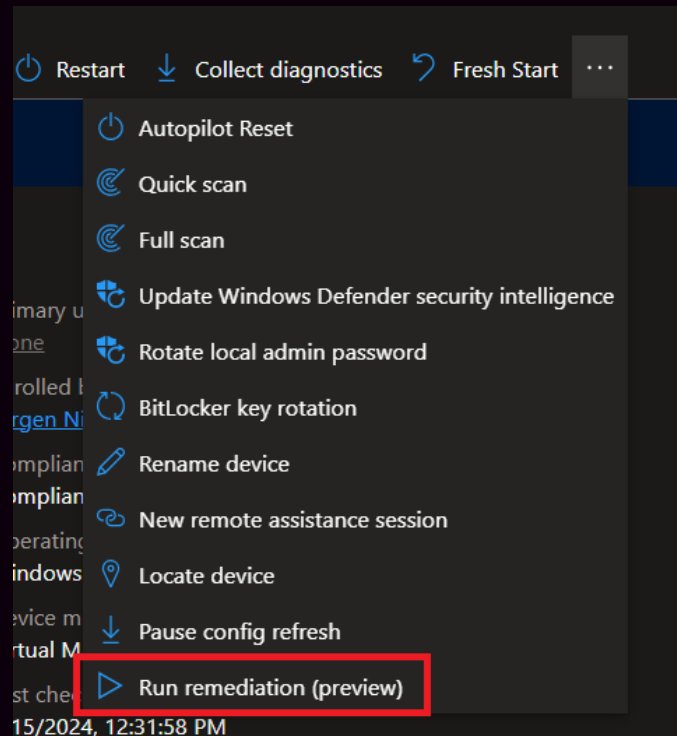
✓ Dma Guard

✓ Virtualization Based Technology

Remediations on demand...

# Remediations on demand

- Troubleshooting a device in a Zero-trust design is something totally different than traditional support.
- Remediations = modern way of troubleshooting in a Zero-Trust world
- Build your own library of scripts
- Inform/train ServiceDesk
- Naming convention + RBAC
- Community repo:  
<https://github.com/JayRHa/EndpointAnalyticsRemediationScripts>



# RBAC

Built-in roles are too powerful!

## Help Desk Operator

Help Desk Operators perform remote tasks on users and devices and can assign applications or policies to users or devices.

- Roles = What a member of the role can do
- Scope Groups = targeting, which groups including virtual groups
- Scope Tags = Which devices are in scope for each role

**You must do RBAC!**



# 3rd Party Patch Management



# Challenges

- Outdated Third-Party Software is leaving you vulnerable
- Defending Against Software Supply Chain Attacks
  - The United States Cybersecurity and Infrastructure Security Agency recommends applying patches to protect against supply chain attacks and compromises, including in third-party software.



# Patch My PC (The Marketing Slide)

- Automate third-party updates in Intune and ConfigMgr
- Automate packaging of third-party applications
- Advanced customization options
  - 3rd.party updates
  - 3rd. application
- Basic SSRS Reports for ConfigMgr software updates compliance
- Advanced Intune deployment features with filters and dynamic assignments

# “Just 4 Clicks” or “Flip the Switch” 🤪

**PATCH MY PC**

You currently have only one user with Access Management privileges. To prevent access issues please add a second user with Access Management privileges. [Fix Access](#)

Ronni Pedersen  
APERTO

**App Catalog**

Search

**Add App**

App Name	Vendor	Version	Language	Architecture	Last Updated
1Password	AgileBits Inc.	8.10.36	English	64-bit, Any	Jul 10, 2024 6:52 AM
3CX Call Flow Designer	3CX Ltd.				
3CX Desktop App	3CX Ltd.				
3CXPhone for Windows	3CX Ltd.				
3Dconnexion 3DxWare 10	3Dconnexion				
4K Video Downloader	Open Media				
7-Zip	Igor Pavlov				

**Connection**  
**Intune**

Display Name \*

GitHub CLI

Language \*

English

Architecture \*

64-bit

Installer Type \*

.msi

Install Context \*

System

**Add Assignment**

Add Available


Add Required

**Add Update Only**

Add Uninstall


# Notifications (Webhook / Email)

Ronni Pedersen via Workflows 02:03


 Deployment update Success  
**Zoom Workplace**

Version:	6.1.43767
Classification:	Updates
Size:	127.04 MB
Severity:	Moderate
Time:	7/31/24 12:03:21 AM UTC
Release Notes:	Zoom Workplace 6.1.6.43767: Minor bug fixes. <a href="https://support.zoom.us/hc/en-us/articles/201361953">https://support.zoom.us/hc/en-us/articles/201361953</a>

Ronni Pedersen used a Workflow template to send this card. [Get template](#)

 Reply


Ronni Pedersen via Workflows 02:03 New

 Deployment update Success  
**Microsoft PowerToys**


Version:	0.83.0
Classification:	Updates
Size:	257.65 MB
Severity:	Moderate
Time:	7/31/24 12:03:50 AM UTC
Release Notes:	Microsoft PowerToys 0.83.0: This release contains bug fixes and enhancements. <a href="https://github.com/microsoft/PowerToys/releases/tag/v0.83.0">https://github.com/microsoft/PowerToys/releases/tag/v0.83.0</a>

Ronni Pedersen used a Workflow template to send this card. [Get template](#)


Deployments from APENTO

 Git Success


Version:	2.46.0.0	Classification:	Updates
Time:	7/31/24 12:00:51 AM UTC	Severity:	Moderate
Size:	60.46 MB		
Release Notes:	Git 2.46.0: This release contains new features, bug fixes and enhancements. <a href="https://github.com/git/git/releases/tag/v2.46.0">https://github.com/git/git/releases/tag/v2.46.0</a>		

 Zoom Workplace Success

Version:	6.1.43767	Classification:	Updates
Time:	7/31/24 12:03:21 AM UTC	Severity:	Moderate
Size:	127.04 MB		
Release Notes:	Zoom Workplace 6.1.6.43767: Minor bug fixes. <a href="https://support.zoom.us/hc/en-us/articles/201361953">https://support.zoom.us/hc/en-us/articles/201361953</a>		

 Microsoft PowerToys Success

Version:	0.83.0	Classification:	Updates
Time:	7/31/24 12:03:50 AM UTC	Severity:	Moderate
Size:	257.65 MB		
Release Notes:	Microsoft PowerToys 0.83.0: This release contains bug fixes and enhancements. <a href="https://github.com/microsoft/PowerToys/releases/tag/v0.83.0">https://github.com/microsoft/PowerToys/releases/tag/v0.83.0</a>		

 Google Chrome Success

Version:	127.0.6533.89	Classification:	SecurityUpdates
Time:	7/31/24 12:04:52 AM UTC	Severity:	Critical
Size:	100.73 MB		
Release Notes:	Google Chrome 127.0.6533.89: This update includes 3 security fixes: Critical CVE-2024-6990: Uninitialized Use in Dawn. High CVE-2024-7255: Out of bounds read in WebTransport. High CVE-2024-7256: Insufficient data validation in Dawn.		

# Risk based deployments... (Rings)

# Risk based deployments

## Options

- Don't use rings... (aka The CrowdStrike model 🤖).
- Built your own model
- Built on top of Windows Autopatch Groups



# Windows Autopatch Groups

**Deployment rings and distribution** [Edit](#)

Dynamic group distribution ⓘ Windows Autopatch Device Registration

Deployment ring	Assigned group ⓘ	Dynamic group distribution ⓘ	Approx. device count ⓘ
Windows Autopatch - Test	None	Not applicable	0
Windows Autopatch - Ring1	None	<input checked="" type="checkbox"/> 1 %	about 5
Windows Autopatch - Ring2	None	<input checked="" type="checkbox"/> 9 %	about 45
Windows Autopatch - Ring3	None	<input checked="" type="checkbox"/> 90 %	about 443
Windows Autopatch - Last	None	Not applicable	0

**Deployment rings and distribution** [Edit](#)

Dynamic group distribution ⓘ All Cloud PCs

Deployment ring	Assigned group ⓘ	Dynamic group distribution ⓘ	Approx. device count ⓘ
Cloud PC - Test	None	Not applicable	0
Cloud PC - Ring1	None	<input checked="" type="checkbox"/> 5 %	about 1
Cloud PC - Ring2	None	<input checked="" type="checkbox"/> 20 %	about 3
Cloud PC - Ring3	None	<input checked="" type="checkbox"/> 75 %	about 10
Cloud PC - Last	None	Not applicable	0



# Diagnostics settings



# Intune Tenant Diagnostics settings

- Event Hub = Automation, Send to third party
- Log analytic = Reporting, Alerting
- Azure Storage = Archive
- Send to partner solution

## Logs:

- AuditLogs
- OperationalLogs
- DeviceComplianceOrg
- Devices
- Windows365AuditLogs

Diagnostic settings			
Name	Storage account	Event hub	Log Analytics workspace
Events	-	CcmexeclIntuneEvents/int...	
Intune	-	-	ccmintunelogs
<a href="#">+ Add diagnostic setting</a>			
Click 'Add Diagnostic setting' above to configure the collection of the following data:			
<ul style="list-style-type: none"><li>• AuditLogs</li><li>• OperationalLogs</li><li>• DeviceComplianceOrg</li><li>• Devices</li><li>• Windows365AuditLogs</li></ul>			

# Event hub cost – Audit Logs

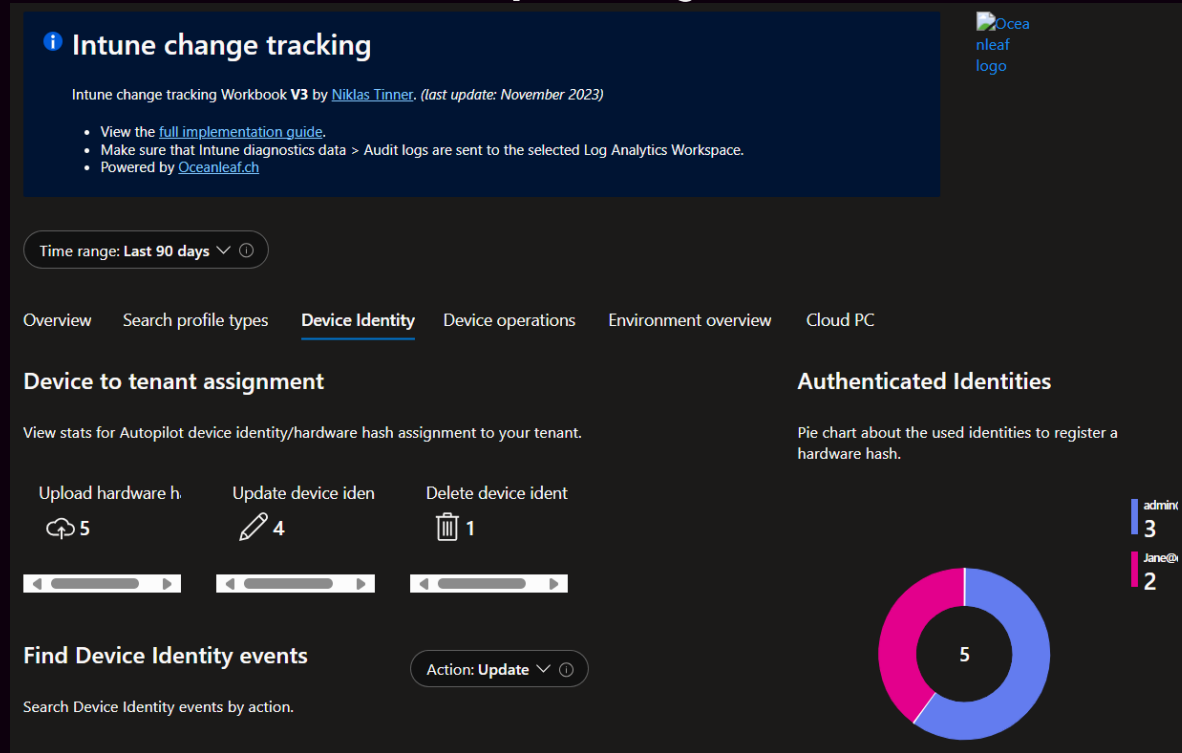
## 100'000 Users

Category	Value
Events per second	18
Events per five-minute interval	5,400
Volume per interval	10.8 MB
Messages per interval	43
Messages per month	371,520
Estimated cost per month (USD)	\$10.83

## 1'000 Users

Category	Value
Events per second	0.1
Events per five-minute interval	52
Volume per interval	104 KB
Messages per interval	1
Messages per month	8,640
Estimated cost per month (USD)	\$10.80

# Workbook sample by Niklas Tinner



Monitor your connectors

# Certificates and Connectors

- Monitoring APN certificates and Tokens used is important
- We see way to often that these are expired....

Tenant details

Connector status

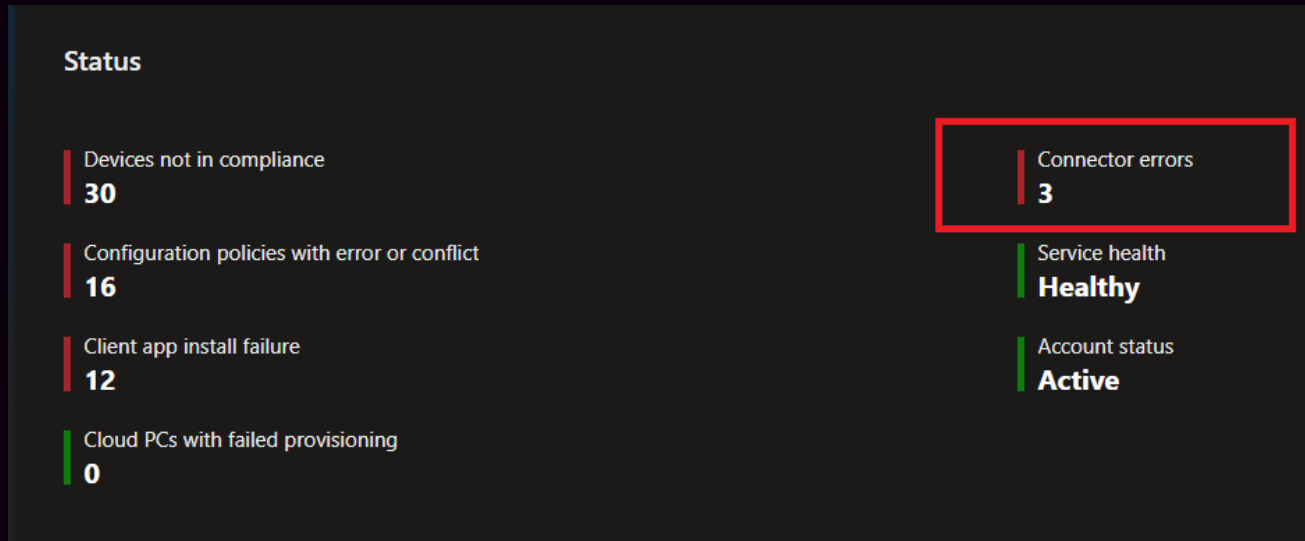
Service health and message center

3 UNHEALTHY

Status	↑↓	Connector	↑↓	Time stamp
! Unhealthy		DEP last sync date		8/8/2024, 11:58:03 AM
! Unhealthy		VPP expiry date		8/8/2024, 1:32:40 PM
! Unhealthy		DEP expiry date		8/8/2024, 1:33:52 PM
✓ Healthy		Windows 365 Azure network connection		9/15/2024, 4:44:54 PM

# Intune Home blade

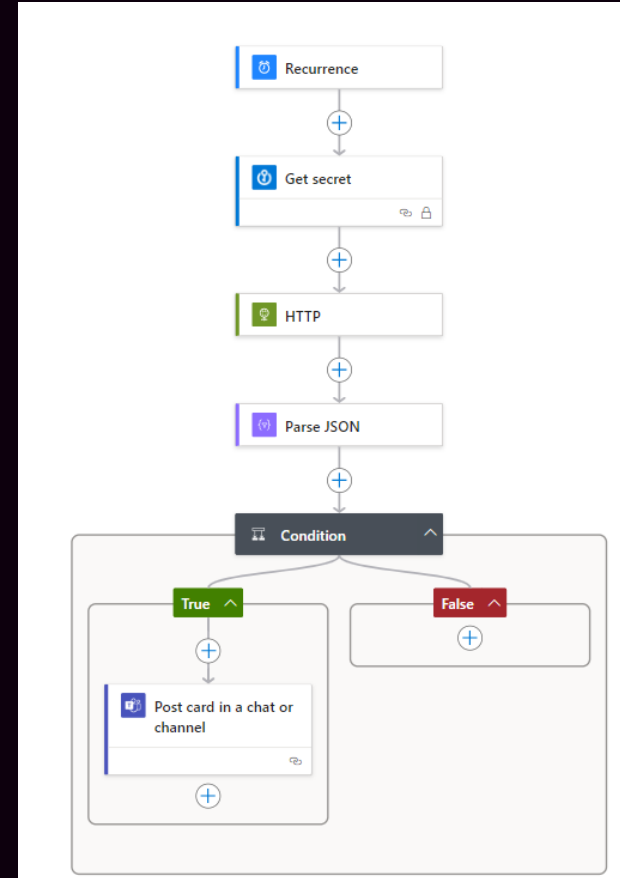
- Shows only errors not warnings...



# Logic app

- We can easily monitor this using a logic app!
- A great guide to get you started by Peter van der Woude

[Monitoring Apple MDM push certificate with Azure Logic Apps and Adaptive Cards for Teams – All about Microsoft Intune \(petervanderwoude.nl\)](#)



# Advanced Endpoint Analytics...



# Advanced Endpoint Analytics

## Features

- Anomaly detection
- Device Scopes
- Enhanced device timeline
- Battery health
- Device query
- Resource Performance Report

# Advanced Endpoint Analytics (Anomalies)

Endpoint analytics | Overview

OverviewAnomaliesModel scoresDevice scores

Anomalies monitors the health of devices in your organization for user experience and productivity regressions followed by deployment objectives.

Anomalies by severity

High0Medium1

Refresh

Search by anomaly

Showing 1 to 1 of 1 devices

Add filter

Severity ↑↓Medium

RefreshExportColumns

Search

Add filters

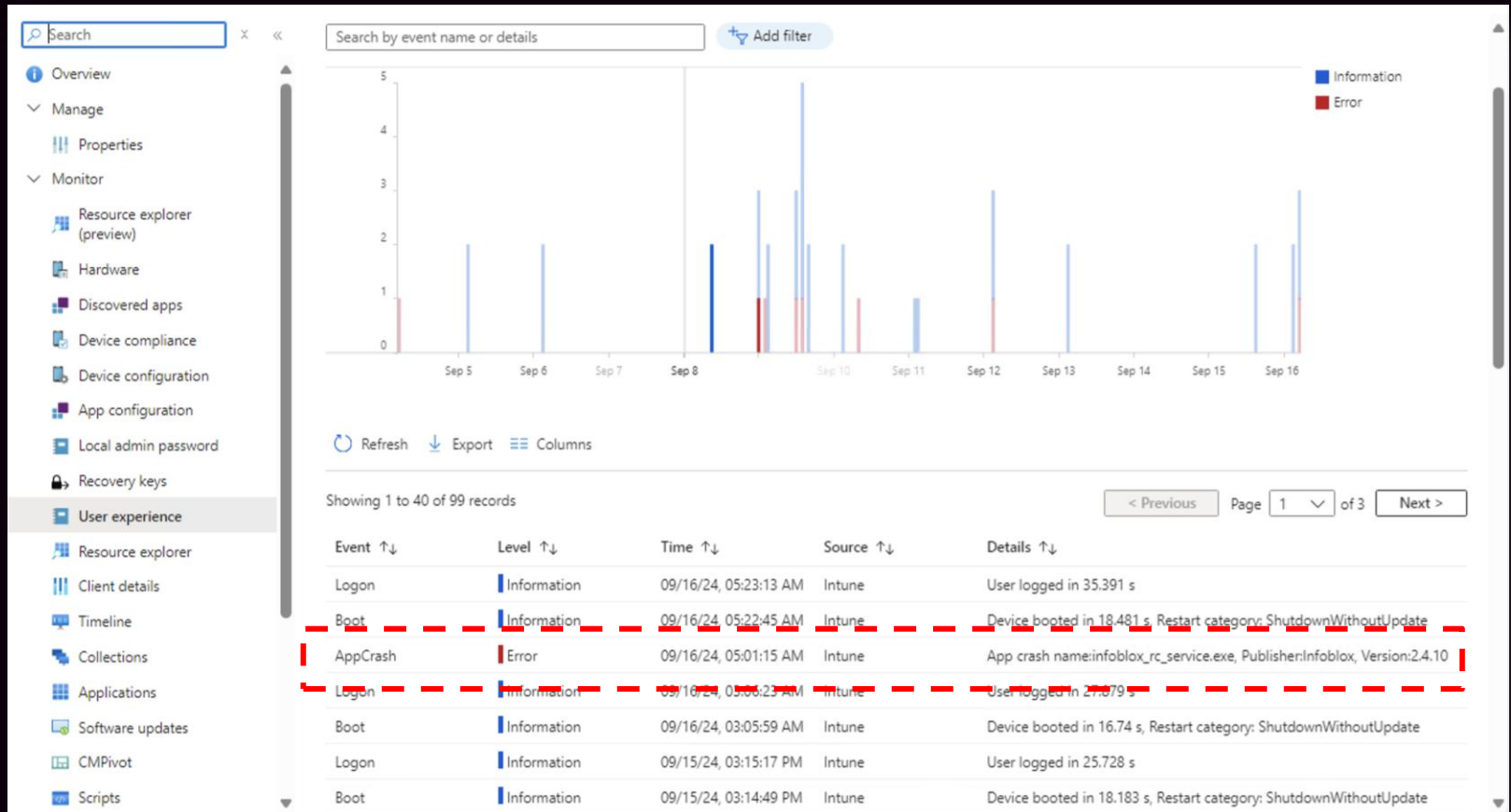
Showing 1 devices out of 1 devices

Device Name	Manufacturer	Model	OS version	First occurrence (UTC)	Latest occurrence (UTC)
DESKTOP-LKLEGPU	Intel(R) Client Systems	NUC12SNKi72	10.0.22621.2283	09/17/2023	09/20/2023

View all affected devices

Title ↑↓	Status ↑↓	Count	First occurrence (UTC)	Latest occurrence (UTC)
Devices experiencing multiple stop error restarts in a 48 hour window	Active	1	09/17/2023	09/20/2023

# Enhanced Device Timeline



# Battery Health Score

## Overview

[Device performance](#)[Model performance](#)[OS performance](#)[App impact](#)

This report offers insights on the battery health for the devices in your organization. Review your score and see how it compares to the selected baseline. Refer to the insights and recommendations to learn how to improve your score.

[Learn more about battery health.](#)

Device scope : **All Devices**

Baseline ⓘ

All organizations (median) ▼

Battery health score ⓘ

✓ Meeting goals

Score  
**85**

Baseline ⓘ  
**50**

## Score categories

Factor	Score
Battery capacity score ⓘ	99
Battery runtime score ⓘ	72

ⓘ Baselines aren't available for battery health scores when the *All organizations (median)* baseline is selected. [Learn more.](#)

# Device Query

▶ Run ✕ Clear input ✕ Cancel

```
1 WindowsEvent('System', 7d)
2 | where tostring(EventId) == '19'
3 | project EventId, LoggedDateTime, LogName, Message, ProviderName, WindowsUserAccount
4
```

Get started **Results**

Columns ▾

59 items

EventId	Message
19	Installation Successful: Windows successfully installed the following update: 9NDMT2VKSNL1-Microsoft.LanguageExperiencePackda-DK
19	Installation Successful: Windows successfully installed the following update: Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1....
19	Installation Successful: Windows successfully installed the following update: Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1....
19	Installation Successful: Windows successfully installed the following update: Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1....
19	Installation Successful: Windows successfully installed the following update: Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1....

# Resource Performance Report

Home > Reports | Endpoint analytics > Endpoint analytics

## Endpoint analytics | Resource performance ...

### Resource performance score

Model performance

Device performance

Resource performance helps you optimize hardware resource utilization on the devices in your organization. Review your current resource performance score and see how it compares to the selected baseline. Refer to the insights and recommendations to learn how to improve your score. [Learn more about resource performance.](#)

Device scope : All Devices

### Resource performance score

Meeting goals

Resource performance sc...

79

Baseline

50

### Score breakdown

Metric	Score/Baseline
CPU spike time score	88
RAM spike time score	70

▲ = Baseline

Baseline

All organizations (median)

### Insights and recommendations

You have 3855 physical devices with high RAM usage. On average, these devices have a RAM spike of 60% compared to an average of 1% for your other devices.

Getting these devices to normal RAM usage range will boost your score by 17 points. [Learn more about optimizing RAM performance](#)

You have 34 physical device models with high RAM usage. On average, these device models have a RAM spike of 54% compared to an average of 4% for your other devices.

Getting these models to normal RAM usage range will boost your score by 14 points. [Learn more about optimizing RAM performance](#)

You have 192 cloud PC devices with above average spike time % on RAM.

Upgrading these devices to a higher configuration of Cloud PCs will improve user performance and RAM score.

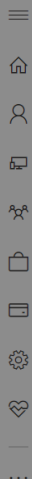
Keep up with what is going on

# Keep up with what is going on

- Message center
- Service Health
- Join the Microsoft Management CCP Program  
<https://aka.ms/JoinMMCCP>
- X (formerly Twitter)  
Intune Support team  
<https://x.com/IntuneSuppTeam>







Home &gt; Message center

## Message center

Each message gives you a high-level overview of a planned change and how it may affect your users, and links out to more detailed information to help you prepare. [Learn more about managing changes](#)

Inbox Archive

Preferences Planner syncing

Filters: Service Tag Message state Relevance Status for your org Platform

<input type="checkbox"/>	Message title	☆	Service
<input type="checkbox"/>	(Updated) Microsoft Outlook for iOS and Android: The Dictation feature will retire in September 2024	:	Microsoft 365 Apps
<input type="checkbox"/>	Microsoft 365 Backup is now generally available	:	Microsoft 365 suite
<input type="checkbox"/>	Rewrite in Microsoft Edge	:	Microsoft 365 suite
<input type="checkbox"/>	Classic Microsoft Outlook for Windows: New reporting buttons integrated with Microsoft Defender for Office 365	:	Exchange Online  Microsoft Defender XDR
<input type="checkbox"/>	Microsoft 365 admin center: Admins can no longer receive user passwords in email as of August 30, 2024	:	Microsoft 365 suite
<input type="checkbox"/>	Microsoft Purview   Information Protection: Default sensitivity labels and policies enhancements	:	Microsoft Purview

## Preferences

Custom View Email

Receive email notifications from message center

- ☐ Primary e-mail address:
- ☒ Other e-mail addresses

Enter up to two email addresses, separated by a semicolon.

### Choose which emails you want to get

We may occasionally notify you about important updates that aren't covered by these settings.

- ☒ Send me emails for major updates
- ☒ Send me emails for data privacy messages
- ☒ Send me a weekly digest about services I select
- ☒ Azure Information Protection
- ☒ Basic Mobility & Security
- ☒ Dynamics 365 Apps
- ☒ Exchange Online
- ☒ General announcement
- ☒ Microsoft 365 Apps

Save



Home &gt; Service health



# Service health

[Overview](#)[Issue history](#)[Reported issues](#)

View the issues and health status of all services that are available with your current subscriptions. [Learn more about Service Health](#)

[Report an issue](#)[Customize](#)

## Active issues Microsoft is working on

Issue title

Issue type

Users may experience delays with multiple alerts and queries in the Microsoft Defender for Cloud Apps service

Advisories

Users may be unable to create connectors in Microsoft Teams

Advisories

Users may be unable to view data for multiple features in Microsoft 365 Defender for Endpoint

Advisories

Users may be unable to import PST files using Drive Shipping in any Microsoft 365 service

Advisories

Some users may see their auto recorded Microsoft Teams meetings spoken languages set incorrectly

Advisories

Admins may be unable to retrieve case details for support tickets within the Microsoft 365 Admin center

Advisories

Some users may be able to access the Bookings with Me feature even though it has been blocked for the organization

Advisories

Admins are unable to add a specific security group to the people insights field in the Microsoft 365 admin center

Advisories

Some users are incorrectly able to approve user email purge actions in Microsoft Defender for Office 365

Advisories

## Customize

[Page view](#)[Email](#)☒ Send me email notifications about service health

Enter up to 2 email addresses, separated by a semicolon

Include these issue types \*

- ☒ Incidents
- ☒ Advisories
- ☒ Issues in your environment that require action

Include these services \*

- ☒ Azure Information Protection
- ☒ Dynamics 365 Apps
- ☒ Exchange Online
- ☒ Microsoft 365 apps
- ☒ Microsoft 365 for the web
- ☒ Microsoft 365 suite
- ☒ Microsoft Bookings
- ☒ Microsoft Defender for Cloud Apps

[Save](#)

# Community Tools

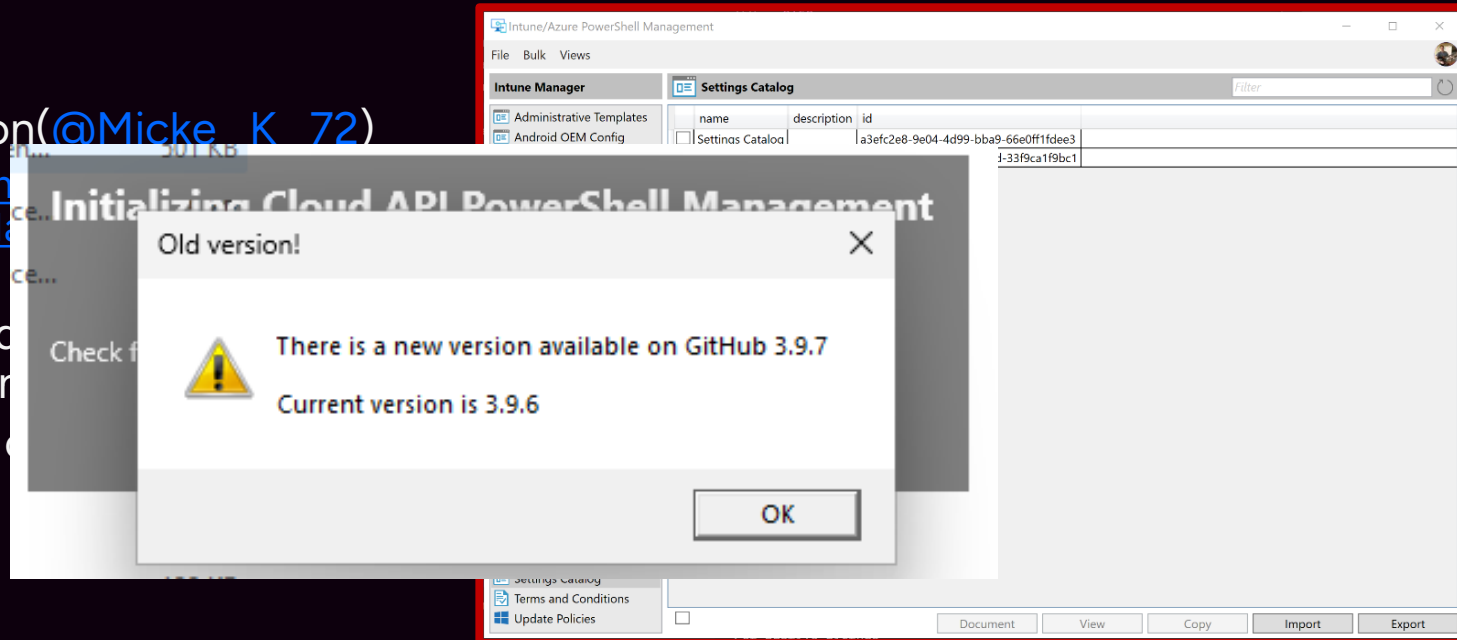
# Use Community Tools

- The Intune community is simply amazing!
- Community tools fills gaps in the product
- Follow community tools creators on X, LinkedIn...
- Give them praise for the work they do
- Let them know you are using their tool
- Keep the tools updated



# Intune Manager

- Tool Author:  
Mikael Karlsson (@Micke\_K\_72)
  - [https://github.com/Micke\\_K\\_72/IntuneManager](https://github.com/Micke_K_72/IntuneManager)
- Copy, export, document and profiles are
- “THE” Intune Manager







Thank you!