Windows ja Intune Community and Troubleshooting Tools

Petri Paavola
Microsoft MVP - Windows and Intune

Petri Paavola

Microsoft MVP – Windows and Intune

Senior Modern Management Principal

Petri.Paavola@yodamiitti.fi

Microsoft® Most Valuable Professional

@petripaavola

https://github.com/petripaavola
Intune.ninja
Powershell.ninja

Skills

- Powershell / Graph API
- AI
- Windows Autopilot + Intune + Intune for Education
- Windows 10&11 Deployment and Management
- Traditional on-prem deployment and management
- Consulting &Training

Over 23 years of work experience

Current (10+ years):

- Yodamiitti Oy / Owner
  Consulting / Training

Past:

- Aalto university / IT-services
  Responsible for Workstation service

YODA MIITTI

Agenda

Key takeaways:

- Learn how community and troubleshooting tools will help your Intune and Windows management and troubleshooting
- World premiere - Introducing Get-WindowsTroubleShootingReportCommunity

Community Tools

Check these tools…

New features on Intune Community Tools

Quick overview of new updates and features released recently for community tools

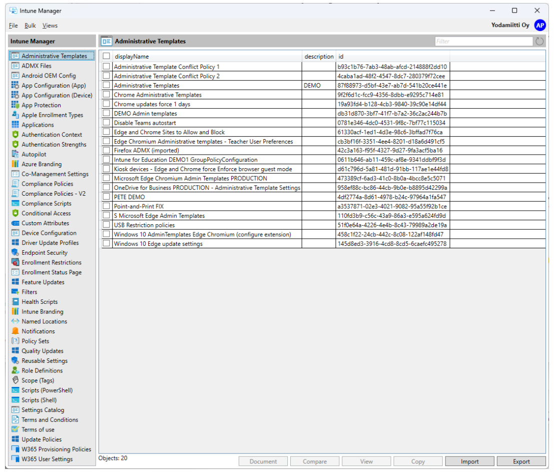
Intune log files troubleshooting helper tools

Updated tools for automatic and manual Intune log file analysis

World Premiere! Introducing Get-WindowsTroubleShootingReportCommunity

The Ultimate Intune and Windows Troubleshooting Tool
Something new, something unique(?), something for and from community

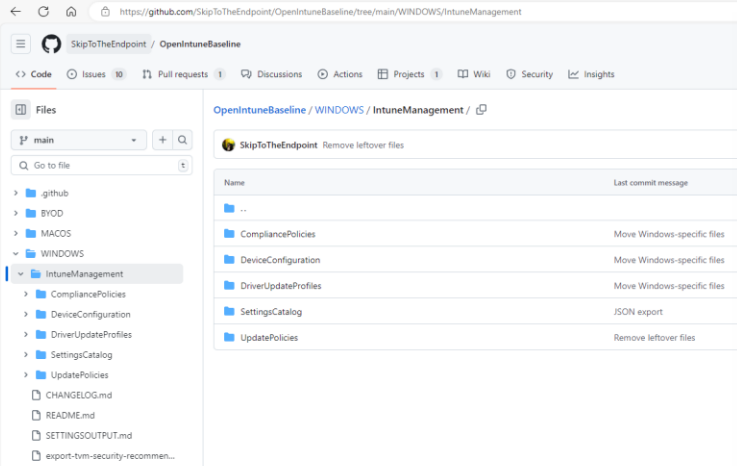
You can help making tools better! ☺



Administrative Templates

□	displayName	description	id
□	Administrative Template Conflict Policy 1		b93c1b76-7ab3-48ab-afcd-214888f2dd10
□	Administrative Template Conflict Policy 2		4caba1ad-48f2-4547-8dc7-280379f72cee
□	Administrative Templates	DEMO	87f88973-d5bf-43e7-ab7d-541b20ce441e
□	Chrome Administrative Templates		9f2f6d1c-fcc9-4356-8dbb-e9295c714e81
□	Chrome updates force 1 days		19a93fd4-b128-4cb3-9840-39c90e14df44
□	DEMO Admin templates		db31d870-3bf7-41f7-b7a2-36c2ac244b7b
□	Disable Teams autostart		0781e346-4dc0-4531-9f8c-7bf77c115034
□	Edge and Chrome Sites to Allow and Block		61330acf-1ed1-4d3e-98c6-3bffad7f76ca
□	Edge Chromium Administrative templates - Teacher User Preferences		cb3bf16f-3351-4ee4-8201-d18a6d491cf5
□	Firefox ADMX (imported)		42c3a163-f95f-4327-9d27-9fa3acf5ba16
□	Intune for Education DEMO1 GroupPolicyConfiguration		0611b646-ab11-459c-af8e-9341ddbf9f3d
□	Kiosk devices - Edge and Chrome force Enforce browser guest mode		d61c796d-5a81-481d-91bb-117ae1e44fd8
□	Microsoft Edge Chromium Admin Templates PRODUCTION		473389cf-6ad3-41c0-8b0a-4bcc8e5c5071
□	OneDrive for Business PRODUCTION - Administrative Template Settings		958ef88c-bc86-44cb-9b0e-b8895d42299a
□	PETE DEMO		4df2774a-8d61-4978-b24c-97964a1fa547
□	Point-and-Print FIX		a3537871-02e3-4021-9082-95a55f92b1ce
□	S Microsoft Edge Admin Templates		110fd3b9-c56c-43a9-86a3-e595a624fd9d
□	USB Restriction policies		51f0e64a-4226-4e4b-8c43-79989a2de19a
□	Windows 10 AdminTemplates Edge Chromium (configure extension)		458c1f22-24cb-442c-8c08-122af148fd47
□	Windows 10 Edge update settings		145d8ed3-3916-4cd8-8cd5-6caefc495278

Objects: 20



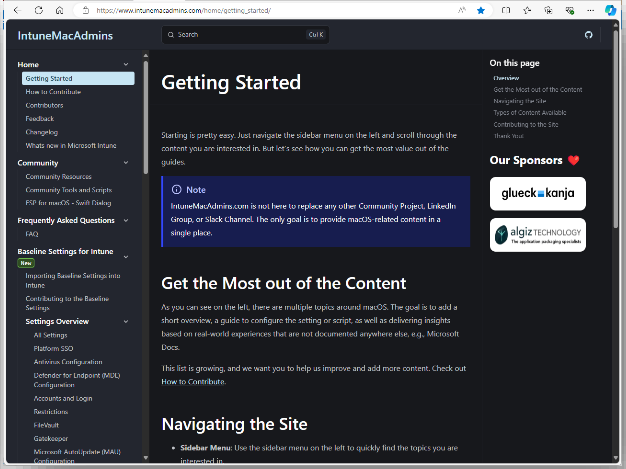
https://github.com/SkipToTheEndpoint/OpenIntuneBaseline/tree/main/WINDOWS/IntuneManagement

SkipToTheEndpoint / OpenIntuneBaseline

OpenIntuneBaseline / WINDOWS / IntuneManagement /

SkipToTheEndpoint Remove leftover files

Name	Last commit message
..	
CompliancePolicies	Move Windows-specific files
DeviceConfiguration	Move Windows-specific files
DriverUpdateProfiles	Move Windows-specific files
SettingsCatalog	JSON export
UpdatePolicies	Remove leftover files


Search
Ctrl K
Home
Getting Started
How to Contribute
Contributors
Feedback
Changelog
Whats new in Microsoft Intune
Community
Community Resources
Community Tools and Scripts
ESP for macOS - Swift Dialog
Frequently Asked Questions
FAQ
Baseline Settings for Intune
New
Importing Baseline Settings into Intune
Contributing to the Baseline Settings
Settings Overview
All Settings
Platform SSO
Antivirus Configuration
Defender for Endpoint (MDE) Configuration
Accounts and Login
Restrictions
FileVault
Gatekeeper
Microsoft AutoUpdate (MAU) Configuration
On this page
Overview
Get the Most out of the Content
Navigating the Site
Types of Content Available
Contributing to the Site
Thank You!
Our Sponsors
glueck kanja
algiz TECHNOLOGY
The application packaging specialists

https://www.intunemacadmins.com/home/getting_started/

IntuneMacAdmins

Getting Started

Starting is pretty easy. Just navigate the sidebar menu on the left and scroll through the content you are interested in. But let's see how you can get the most value out of the guides.

Note

IntuneMacAdmins.com is not here to replace any other Community Project, LinkedIn Group, or Slack Channel. The only goal is to provide macOS-related content in a single place.

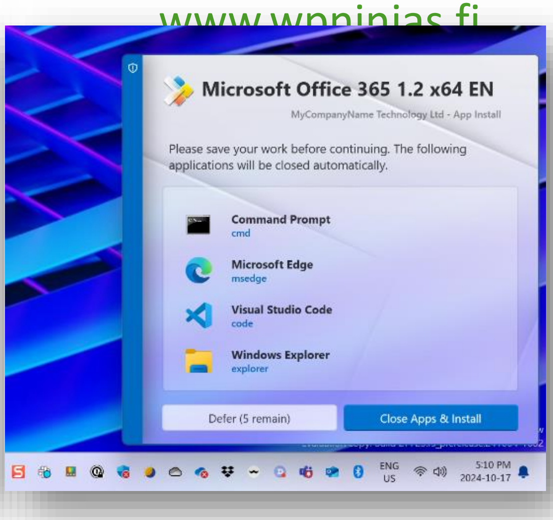
Get the Most out of the Content

As you can see on the left, there are multiple topics around macOS. The goal is to add a short overview, a guide to configure the setting or script, as well as delivering insights based on real-world experiences that are not documented anywhere else, e.g., Microsoft Docs.

This list is growing, and we want you to help us improve and add more content. Check out How to Contribute.

Navigating the Site

- **Sidebar Menu:** Use the sidebar menu on the left to quickly find the topics you are interested in.



Microsoft Office 365 1.2 x64 EN

MyCompanyName Technology Ltd - App Install

Please save your work before continuing. The following applications will be closed automatically.

Command Prompt
cmd

Microsoft Edge
msedge

Visual Studio Code
code

Windows Explorer
explorer

Community Tools

These will help your work day…

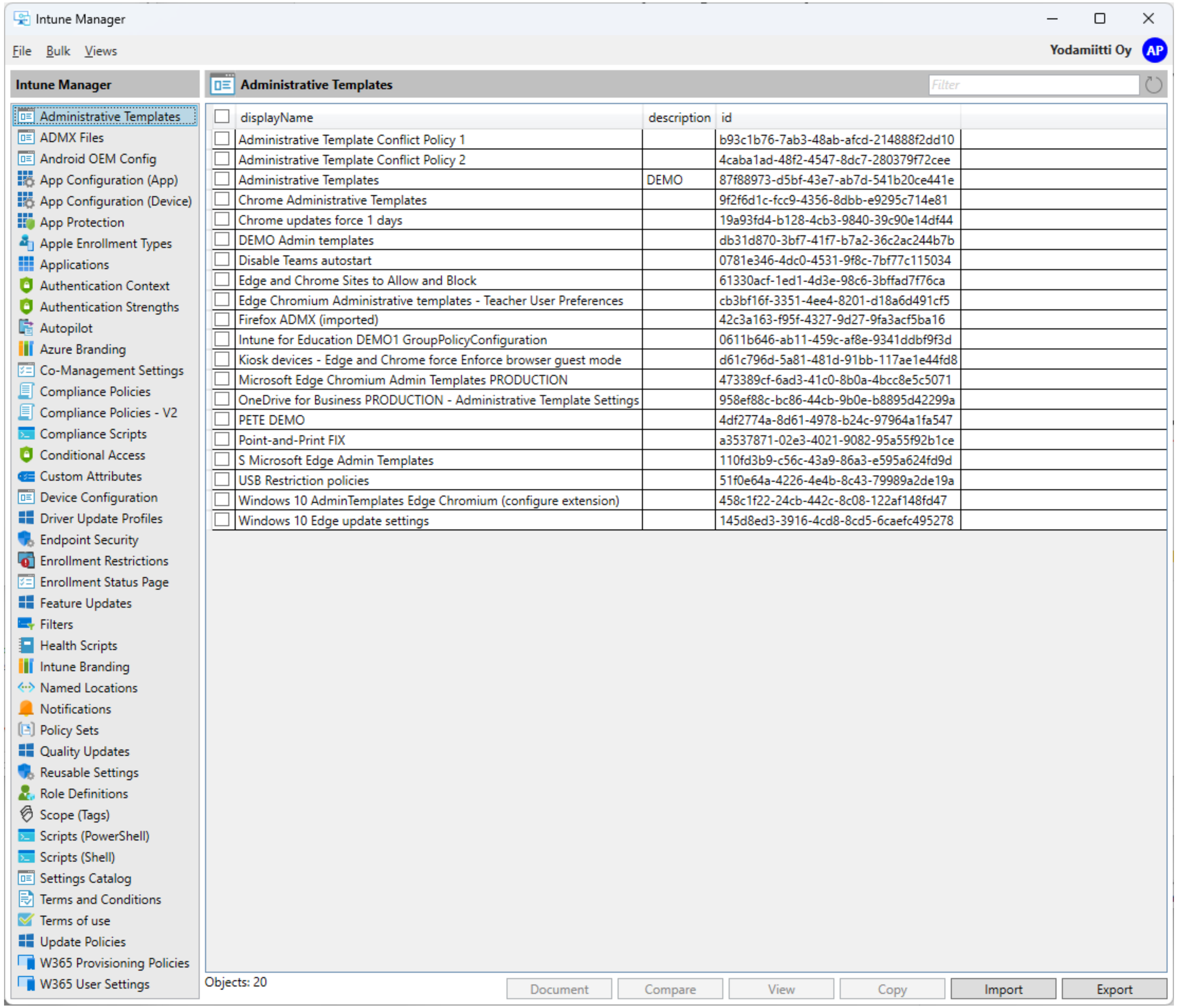
Intune Management - Micke Karlsson

www.wpninjas.fi

- Hyvin kattava työkalu
- Copy, export, import, backup
- Compare
- Edit (skriptit)
- Ja vaikka mitä

Tukee useita tenantteja
-> **Kopioi policyjä tenantista toiseen**

https://github.com/Micke-K/IntuneManagement

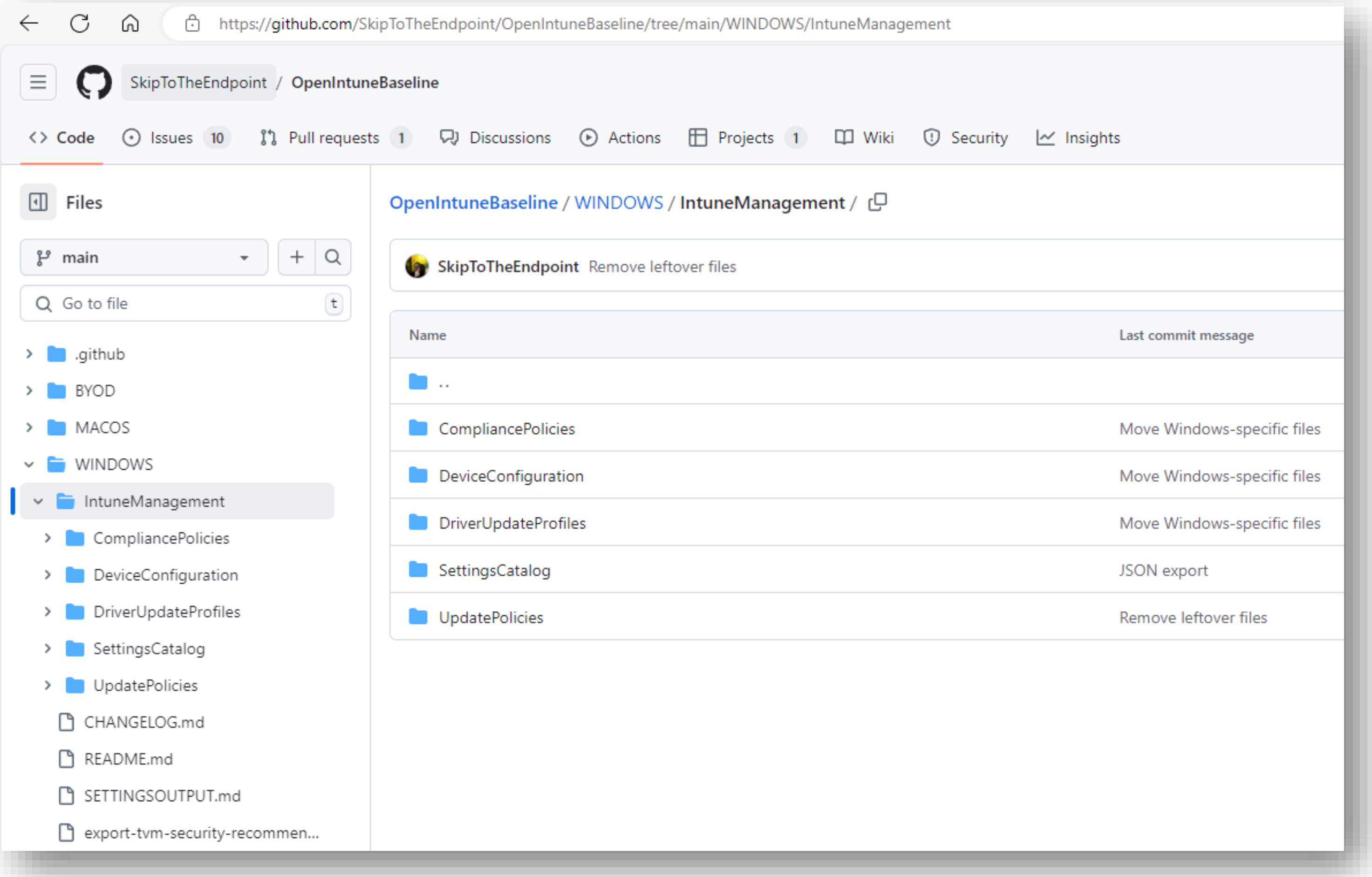


□	displayName	description	id
□	Administrative Template Conflict Policy 1		b93c1b76-7ab3-48ab-afcd-214888f2dd10
□	Administrative Template Conflict Policy 2		4caba1ad-48f2-4547-8dc7-280379f72cee
□	Administrative Templates	DEMO	87f88973-d5bf-43e7-ab7d-541b20ce441e
□	Chrome Administrative Templates		9f2f6d1c-fcc9-4356-8dbb-e9295c714e81
□	Chrome updates force 1 days		19a93fd4-b128-4cb3-9840-39c90e14df44
□	DEMO Admin templates		db31d870-3bf7-41f7-b7a2-36c2ac244b7b
□	Disable Teams autostart		0781e346-4dc0-4531-9f8c-7bf77c115034
□	Edge and Chrome Sites to Allow and Block		61330acf-1ed1-4d3e-98c6-3bffad7f76ca
□	Edge Chromium Administrative templates - Teacher User Preferences		cb3bf16f-3351-4ee4-8201-d18a6d491cf5
□	Firefox ADMX (imported)		42c3a163-f95f-4327-9d27-9fa3acf5ba16
□	Intune for Education DEMO1 GroupPolicyConfiguration		0611b646-ab11-459c-af8e-9341ddbf9f3d
□	Kiosk devices - Edge and Chrome force Enforce browser guest mode		d61c796d-5a81-481d-91bb-117ae1e44fd8
□	Microsoft Edge Chromium Admin Templates PRODUCTION		473389cf-6ad3-41c0-8b0a-4bcc8e5c5071
□	OneDrive for Business PRODUCTION - Administrative Template Settings		958ef88c-bc86-44cb-9b0e-b8895d42299a
□	PETE DEMO		4df2774a-8d61-4978-b24c-97964a1fa547
□	Point-and-Print FIX		a3537871-02e3-4021-9082-95a55f92b1ce
□	S Microsoft Edge Admin Templates		110fd3b9-c56c-43a9-86a3-e595a624fd9d
□	USB Restriction policies		51f0e64a-4226-4e4b-8c43-79989a2de19a
□	Windows 10 AdminTemplates Edge Chromium (configure extension)		458c1f22-24cb-442c-8c08-122af148fd47
□	Windows 10 Edge update settings		145d8ed3-3916-4cd8-8cd5-6caefc495278

Objects: 20

OpenIntuneBaseline - James Robinson

- Policyjä moniin eri käyttötarkoituksiin
- Aiemmalla Intune Management -työkalulla policyjä voi importoida omaan Intuneen
- Tai käsin Intune/Import tai skriptillä, jos ei voi käyttää ulkopuolisia työkaluja



https://github.com/SkipToTheEndpoint/OpenIntuneBaseline/tree/main/WINDOWS/IntuneManagement

SkipToTheEndpoint / OpenIntuneBaseline

- .github
- BYOD
- MACOS
- WINDOWS
  - IntuneManagement
    - CompliancePolicies
    - DeviceConfiguration
    - DriverUpdateProfiles
    - SettingsCatalog
    - UpdatePolicies
  - CHANGELOG.md
  - README.md
  - SETTINGSOUTPUT.md
  - export-tvm-security-recommen...

OpenIntuneBaseline / WINDOWS / IntuneManagement /

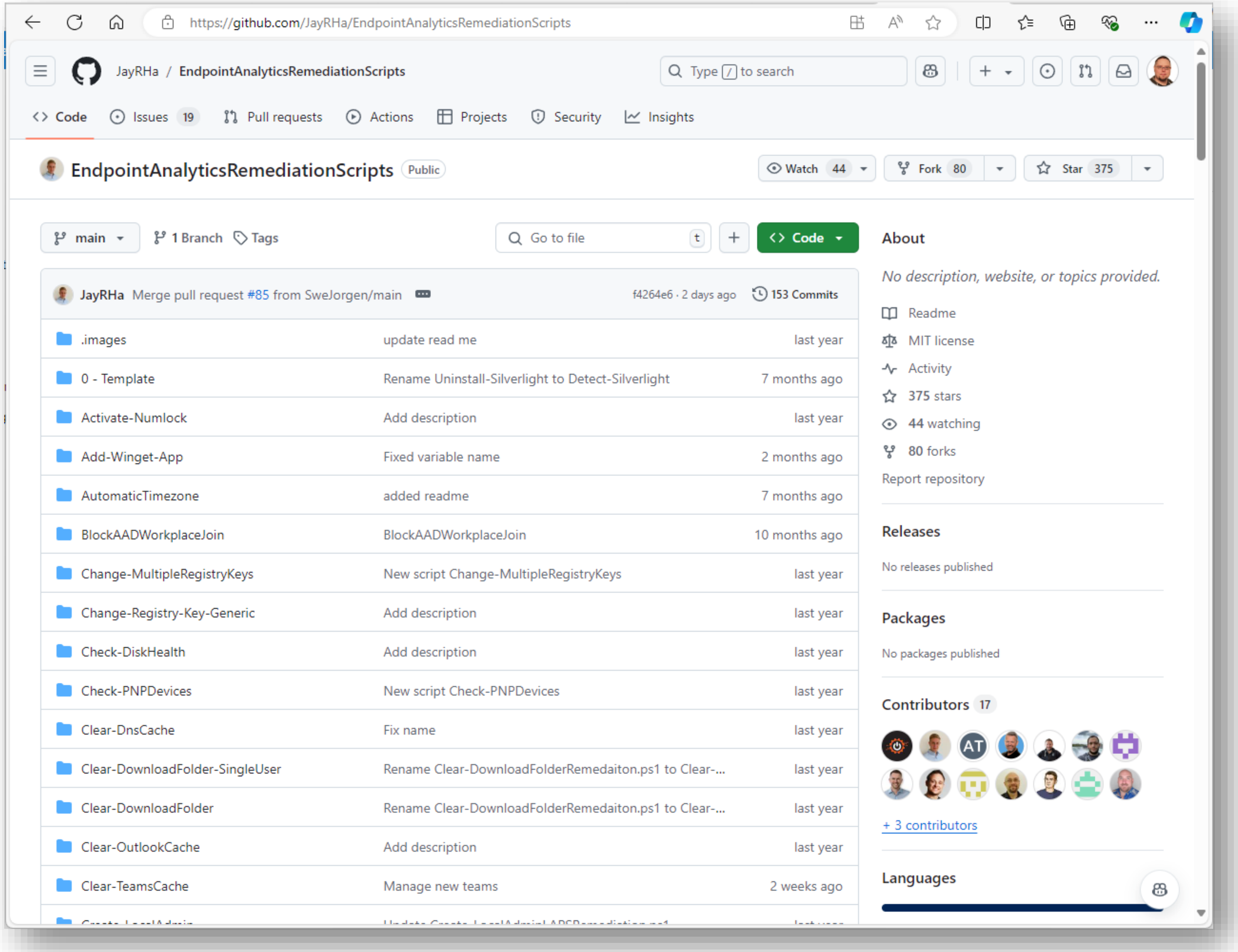
SkipToTheEndpoint Remove leftover files

Name	Last commit message
..	
CompliancePolicies	Move Windows-specific files
DeviceConfiguration	Move Windows-specific files
DriverUpdateProfiles	Move Windows-specific files
SettingsCatalog	JSON export
UpdatePolicies	Remove leftover files

https://openintunebaseline.com/

EndpointAnalyticsRemediationScripts - Jannik Reinhard

- Intune Remediations-skriptejä moniin eri käyttötarkoituksiin
- Kannattaa kahlata läpi



https://github.com/JayRHa/EndpointAnalyticsRemediationScripts

JayRHa / EndpointAnalyticsRemediationScripts

EndpointAnalyticsRemediationScripts

JayRHa Merge pull request #85 from SweJorgen/main ··· f4264e6 · 2 days ago 153 Commits

.images	update read me	last year
0 - Template	Rename Uninstall-Silverlight to Detect-Silverlight	7 months ago
Activate-Numlock	Add description	last year
Add-Winget-App	Fixed variable name	2 months ago
AutomaticTimezone	added readme	7 months ago
BlockAADWorkplaceJoin	BlockAADWorkplaceJoin	10 months ago
Change-MultipleRegistryKeys	New script Change-MultipleRegistryKeys	last year
Change-Registry-Key-Generic	Add description	last year
Check-DiskHealth	Add description	last year
Check-PNPDevices	New script Check-PNPDevices	last year
Clear-DnsCache	Fix name	last year
Clear-DownloadFolder-SingleUser	Rename Clear-DownloadFolderRemedaiton.ps1 to Clear-...	last year
Clear-DownloadFolder	Rename Clear-DownloadFolderRemedaiton.ps1 to Clear-...	last year
Clear-OutlookCache	Add description	last year
Clear-TeamsCache	Manage new teams	2 weeks ago

About

No description, website, or topics provided.

Readme
MIT license
Activity
375 stars
44 watching
80 forks
Report repository

Releases

No releases published

Packages

No packages published

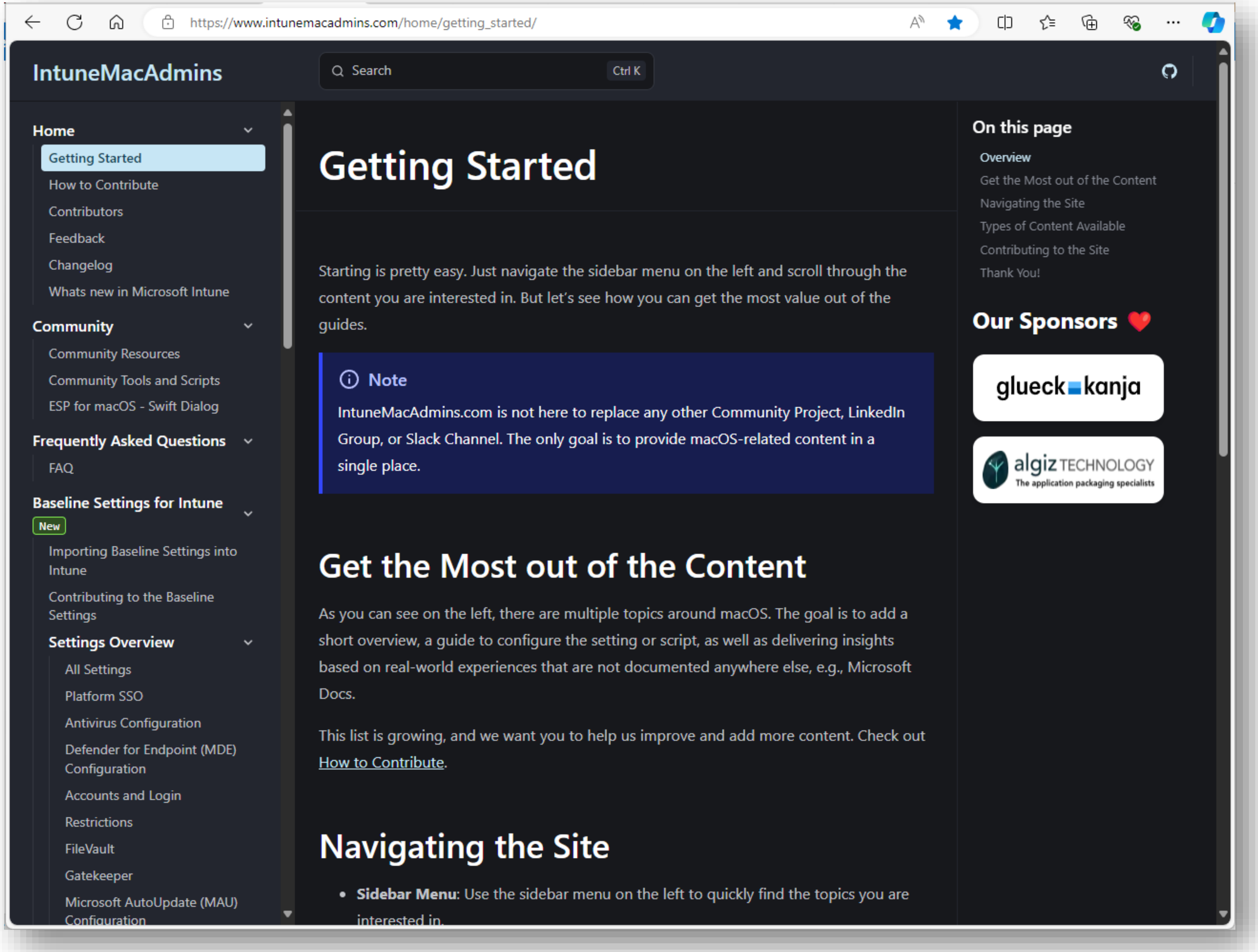
Contributors 17

+ 3 contributors

Languages

IntuneMacAdmins - Ugur Koc

- Paaaljon ohjeita ja vinkkejä **macOS Intune-hallintaan**
- Ei korvaa olemassa olevia foorumeita, mutta on oiva lisä



https://www.intunemacadmins.com/home/getting_started/
IntuneMacAdmins
Search
Ctrl K
Home
Getting Started
How to Contribute
Contributors
Feedback
Changelog
Whats new in Microsoft Intune
Community
Community Resources
Community Tools and Scripts
ESP for macOS - Swift Dialog
Frequently Asked Questions
FAQ
Baseline Settings for Intune
New
Importing Baseline Settings into Intune
Contributing to the Baseline Settings
Settings Overview
All Settings
Platform SSO
Antivirus Configuration
Defender for Endpoint (MDE) Configuration
Accounts and Login
Restrictions
FileVault
Gatekeeper
Microsoft AutoUpdate (MAU) Configuration
On this page
Overview
Get the Most out of the Content
Navigating the Site
Types of Content Available
Contributing to the Site
Thank You!
Our Sponsors
glueck kanja
algiz TECHNOLOGY
The application packaging specialists

Getting Started

Starting is pretty easy. Just navigate the sidebar menu on the left and scroll through the content you are interested in. But let's see how you can get the most value out of the guides.

Note

IntuneMacAdmins.com is not here to replace any other Community Project, LinkedIn Group, or Slack Channel. The only goal is to provide macOS-related content in a single place.

Get the Most out of the Content

As you can see on the left, there are multiple topics around macOS. The goal is to add a short overview, a guide to configure the setting or script, as well as delivering insights based on real-world experiences that are not documented anywhere else, e.g., Microsoft Docs.

This list is growing, and we want you to help us improve and add more content. Check out How to Contribute.

Navigating the Site

- **Sidebar Menu**: Use the sidebar menu on the left to quickly find the topics you are interested in.

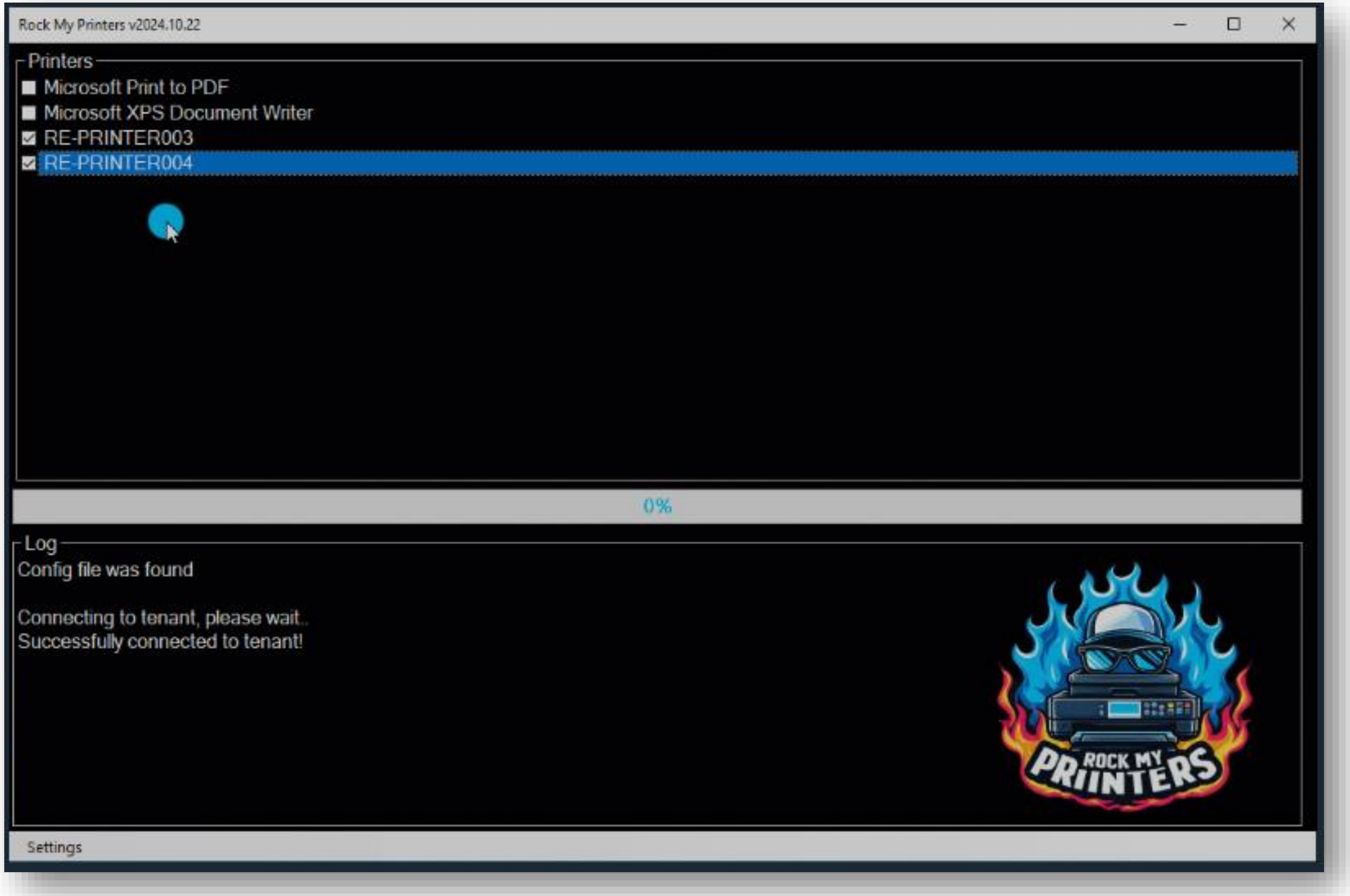
https://www.intunemacadmins.com/

Intune ja tulostimet

- Rock My Printers
  - Luo tulostinpaketteja automaattisesti
  - https://www.rockenroll.tech/2023/03/14/rock-my-printers/

- Teorian opiskelemiseksi kannattaa lukea läpi Rudyn blogi

https://call4cloud.nl/deploy-printer-drivers-intune-win32app/

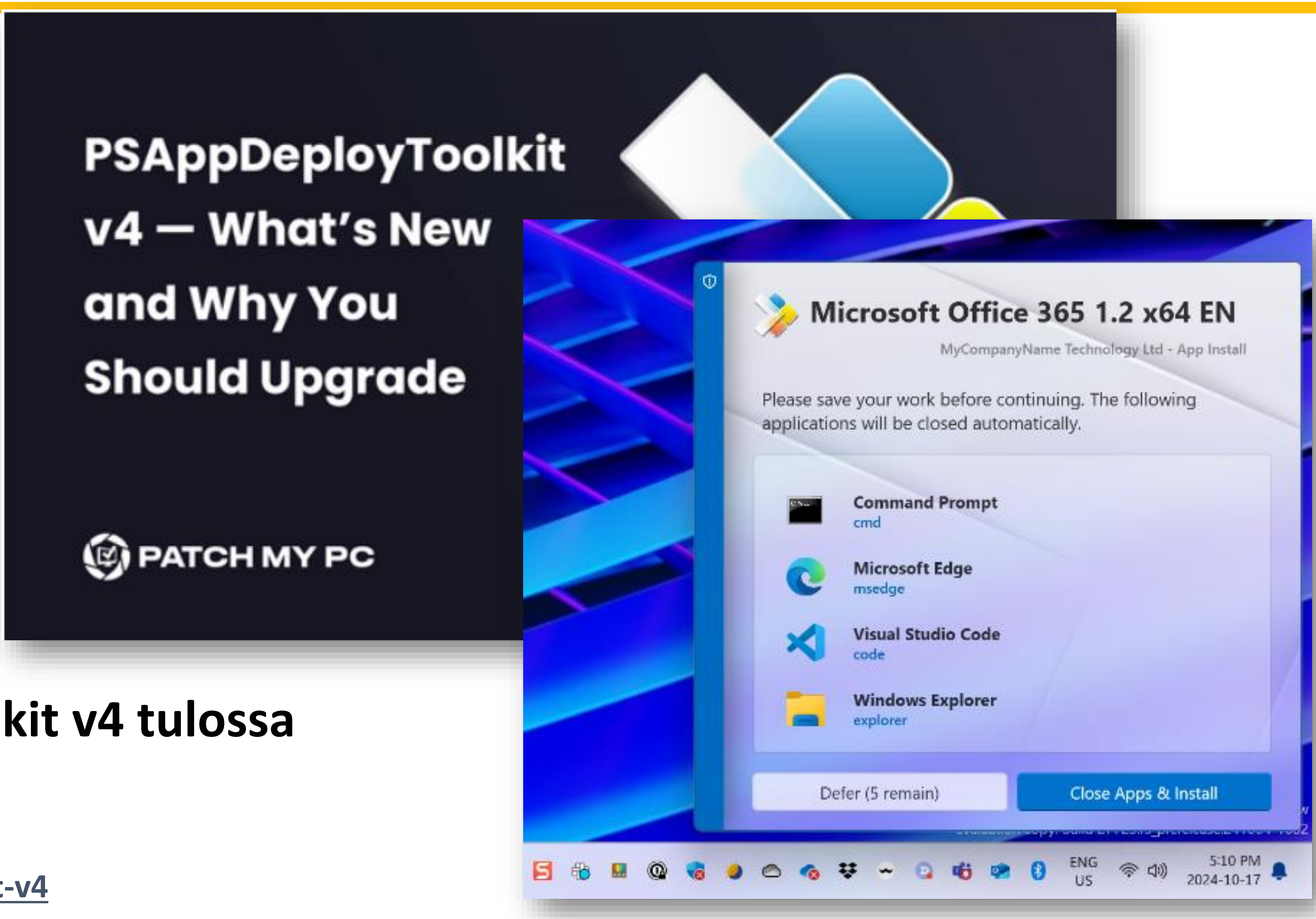


□ Microsoft Print to PDF
□ Microsoft XPS Document Writer
☑ RE-PRINTER003
☑ RE-PRINTER004

```
Config file was found

Connecting to tenant, please wait..
Successfully connected to tenant!
```

PSAppDeployToolkit v4



PSAppDeployToolkit v4 — What's New and Why You Should Upgrade

PATCH MY PC

Microsoft Office 365 1.2 x64 EN

MyCompanyName Technology Ltd - App Install

Please save your work before continuing. The following applications will be closed automatically.

- Command Prompt
  cmd
- Microsoft Edge
  msedge
- Visual Studio Code
  code
- Windows Explorer
  explorer

PSAppDeployToolkit v4 tulossa loppuvuodesta

https://patchmypc.com/psadt-v4

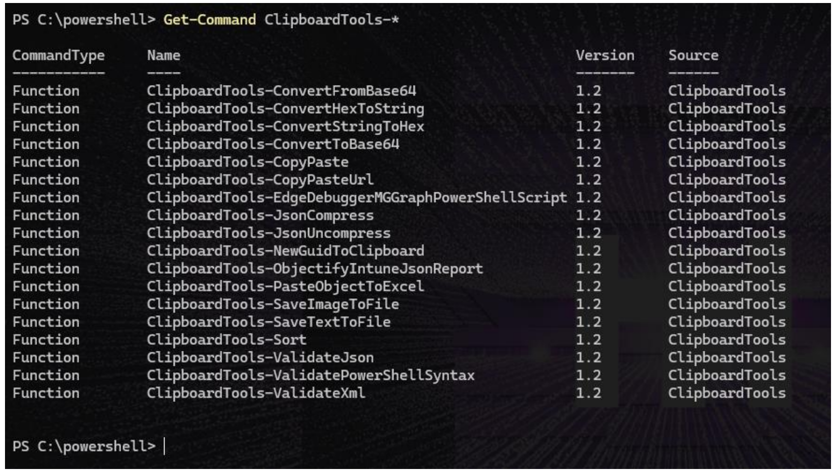
Intune Community Tools Updates

Quick overview of tools and new features

Intune Community Tools Updates

- Old/original Intune PowerShell SDK Graph API module stopped working earlier this year
  - This was anticipated and there was over a year or two to update scripts
  - Did we update scripts in time ?-) :D
- All Intune scripts using old PowerShell module or it's Enterprise Application ID in the world needed to be changed to use Microsoft Graph PowerShell module
  - or use custom Enterprise Application and not use PowerShell module at all

Let's look newest updates and new features in famous Troubleshooting Tools in next few DEMOs



```
PS C:\powershell> Get-Command ClipboardTools-*

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        ClipboardTools-ConvertFromBase64                   1.2        ClipboardTools
Function        ClipboardTools-ConvertHexToString                  1.2        ClipboardTools
Function        ClipboardTools-ConvertStringToHex                  1.2        ClipboardTools
Function        ClipboardTools-ConvertToBase64                     1.2        ClipboardTools
Function        ClipboardTools-CopyPaste                           1.2        ClipboardTools
Function        ClipboardTools-CopyPasteUrl                        1.2        ClipboardTools
Function        ClipboardTools-EdgeDebuggerMGGraphPowerShellScript 1.2        ClipboardTools
Function        ClipboardTools-JsonCompress                        1.2        ClipboardTools
Function        ClipboardTools-JsonUncompress                      1.2        ClipboardTools
Function        ClipboardTools-NewGuidToClipboard                  1.2        ClipboardTools
Function        ClipboardTools-ObjectifyIntuneJsonReport           1.2        ClipboardTools
Function        ClipboardTools-PasteObjectToExcel                  1.2        ClipboardTools
Function        ClipboardTools-SaveImageToFile                     1.2        ClipboardTools
Function        ClipboardTools-SaveTextToFile                      1.2        ClipboardTools
Function        ClipboardTools-Sort                                1.2        ClipboardTools
Function        ClipboardTools-ValidateJson                        1.2        ClipboardTools
Function        ClipboardTools-ValidatePowerShellSyntax            1.2        ClipboardTools
Function        ClipboardTools-ValidateXml                         1.2        ClipboardTools


PS C:\powershell> |
```

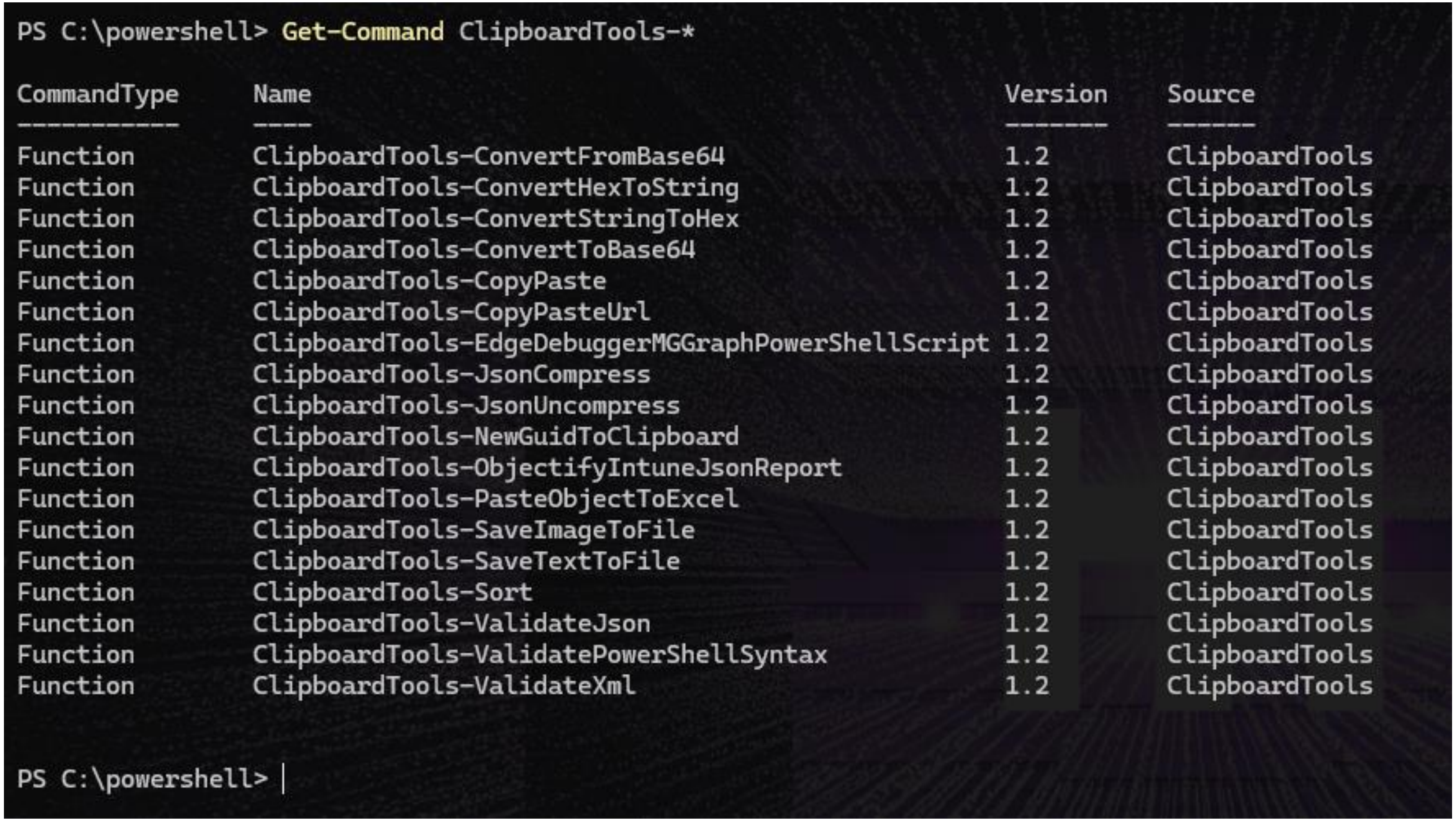
ClipboardTools-* PowerShell module updates

Toolset to help analyzing Intune log files manually and create your own Intune scripts easily

ClipboardTools

- ClipboardTools is set of tools which helps you to
  - Extract and convert log entries to human readable format
    - For example: json expansion and base64 conversions
- Updated: Create Intune/Graph API scripts without knowing Powershell or Graph API "at all"
  - DEMO on this later
  - All Petri's Intune related tools are made with this trick / tool
- Other useful little tools to help your every day life
- New tools to help some troublehooting tasks
- Easy install from Powershell Gallery:
  - **Install-Module -Name ClipboardTools -Scope CurrentUser**

ClipboardTools New Features DEMO

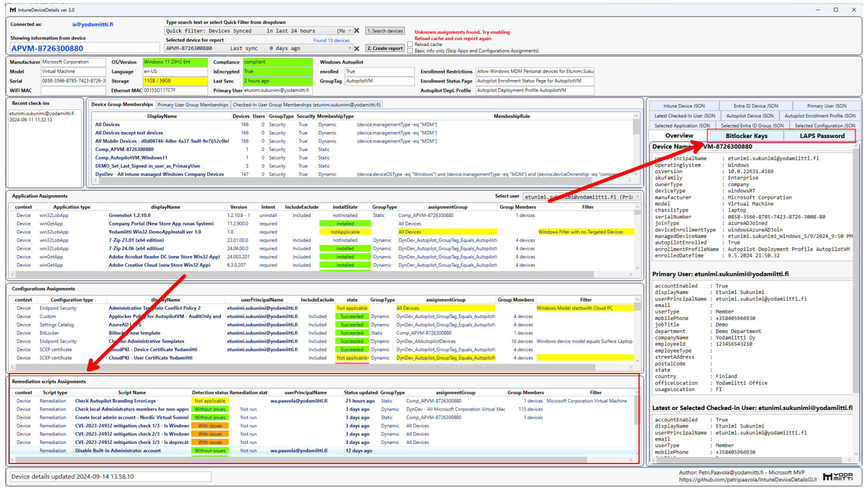


```
PS C:\powershell> Get-Command ClipboardTools-*

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        ClipboardTools-ConvertFromBase64                   1.2        ClipboardTools
Function        ClipboardTools-ConvertHexToString                  1.2        ClipboardTools
Function        ClipboardTools-ConvertStringToHex                  1.2        ClipboardTools
Function        ClipboardTools-ConvertToBase64                     1.2        ClipboardTools
Function        ClipboardTools-CopyPaste                           1.2        ClipboardTools
Function        ClipboardTools-CopyPasteUrl                        1.2        ClipboardTools
Function        ClipboardTools-EdgeDebuggerMGGraphPowerShellScript 1.2        ClipboardTools
Function        ClipboardTools-JsonCompress                        1.2        ClipboardTools
Function        ClipboardTools-JsonUncompress                      1.2        ClipboardTools
Function        ClipboardTools-NewGuidToClipboard                  1.2        ClipboardTools
Function        ClipboardTools-ObjectifyIntuneJsonReport           1.2        ClipboardTools
Function        ClipboardTools-PasteObjectToExcel                  1.2        ClipboardTools
Function        ClipboardTools-SaveImageToFile                     1.2        ClipboardTools
Function        ClipboardTools-SaveTextToFile                      1.2        ClipboardTools
Function        ClipboardTools-Sort                                1.2        ClipboardTools
Function        ClipboardTools-ValidateJson                        1.2        ClipboardTools
Function        ClipboardTools-ValidatePowerShellSyntax            1.2        ClipboardTools
Function        ClipboardTools-ValidateXml                         1.2        ClipboardTools


PS C:\powershell>
```

https://github.com/petripaavola/ClipboardTools



IntuneDeviceDetails ver 3.0

Connected as: la@yodamiitti.fi

Showing information from device: **APVM-8726300880**

Type search text or select Quick Filter from dropdown: `Quick filter: Devices Synced    in last 24 hours    (Ma`

Selected device for report: `APVM-8726300880    Last sync    0 days ago`

Found 13 devices

Unknown assignments found. Try enabling Reload cache and run report again

□ Reload cache
□ Basic info only (Skip Apps and Configurations Assignments)

Manufacturer	Microsoft Corporation	OS/Version	Windows 11 23H2 Ent	Compliance	compliant	Windows Autopilot			
Model	Virtual Machine	Language	en-US	isEncrypted	True	enrolled	True	Enrollment Restrictions	Allow Windows MDM Personal devices for Etunimi.Suku
Serial	0858-3566-8785-7423-8726-3	Storage	11GB / 59GB	Last Sync	2 hours ago	GroupTag	AutopilotVM	Enrollment Status Page	Autopilot Enrollment Status Page for AutopilotVM
WiFi MAC		Ethernet MAC	00155D117C7F	Primary User	etunimi.sukunimi@yodamiitti.fi			Autopilot Depl. Profile	Autopilot Deployment Profile AutopilotVM

Recent check-ins

etunimi.sukunimi@yodamiitti.fi
2024-09-11 11.32.13

Device Group Memberships | Primary User Group Memberships | Checked-In User Group Memberships (etunimi.sukunimi@yodamiitti.fi)

DisplayName	Devices	Users	GroupType	Security	MembeshipType	MembeshipRule
All Devices	166	0	Security	True	Dynamic	(device.managementType -eq "MDM")
All Devices except test devices	166	0	Security	True	Dynamic	(device.managementType -eq "MDM")
All Mobile Devices - d0d08746-4dbe-4a37-9adf-9e7652c0b4	166	0	Security	True	Dynamic	(device.managementType -eq "MDM")
Comp_APVM-8726300880	1	0	Security	True	Static	
Comp_AutopilotVM_Windows11	1	0	Security	True	Static	
DEMO_Set_Last_Signed-in_user_as_PrimaryUser	3	0	Security	True	Static	
DynDev - All Intune managed Windows Company Devices	147	0	Security	True	Dynamic	(device.deviceOSType -eq "Windows") and (device.managementType -eq "MDM") and (device.deviceOwnership -eq "compan

Application Assignments

Select user: `etunimi.sukunimi@yodamiitti.fi (Pri`

context	Application type	displayName	Version	Intent	IncludeExclude	installState	GroupType	assignmentGroup	Group Members	Filter
Device	win32LobApp	Greenshot 1.2.10.6	1.2.10.6 - 1	uninstall	Included	notInstalled	Static	Comp_APVM-8726300880	1 devices	
Device	winGetApp	Company Portal (New Store App runas System)	11.2.900.0	required		installed		All Devices		
Device	win32LobApp	Yodamiitti Win32 DemoAppInstall ver 1.0	1.0	required		notApplicable		All Devices		Windows Filter with no Targeted Devices
Device	win32LobApp	7-Zip 23.01 (x64 edition)	23.01.00.0	required	Included	notInstalled	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	
Device	win32LobApp	7-Zip 24.06 (x64 edition)	24.06.00.0	required	Included	installed	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	
Device	winGetApp	Adobe Acrobat Reader DC (new Store Win32 App)	24.003.201	required	Included	installed	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	
Device	winGetApp	Adobe Creative Cloud (new Store Win32 App)	6.3.0.207	required	Included	installed	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	

Configurations Assignments

context	Configuration type	displayName	userPrincipalName	IncludeExclude	state	GroupType	assignmentGroup	Group Members	Filter
Device	Endpoint Security	Administrative Template Conflict Policy 2	etunimi.sukunimi@yodamiitti.fi		Not applicable		All Devices		Windows Model startswith Cloud PC
Device	Custom	Applocker Policy for AutopilotVM - AuditOnly and	etunimi.sukunimi@yodamiitti.fi	Included	Succeeded	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	
Device	Settings Catalog	AzureAD LAPS	etunimi.sukunimi@yodamiitti.fi	Included	Succeeded	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	
Device	BitLocker	Bitlocker new template	etunimi.sukunimi@yodamiitti.fi	Included	Succeeded	Static	Comp_APVM-8726300880	1 devices	
Device	Endpoint Security	Chrome Administrative Templates	etunimi.sukunimi@yodamiitti.fi	Included	Succeeded	Dynamic	DynDev_AllAutopilotDevices	16 devices	Windows device model equals Surface Laptop
Device	SCEP certificate	CloudPKI - Device Certificate Yodamiitti	etunimi.sukunimi@yodamiitti.fi	Included	Succeeded	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	
Device	SCEP certificate	CloudPKI - User Certificate Yodamiitti		Included	Not applicable	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	

Remediation scripts Assignments

context	Script type	Script Name	Detection status	Remediation stat	userPrincipalName	Status updated	GroupType	assignmentGroup	Group Members	Filter
Device	Remediation	Check Autopilot Branding ErrorLogs	Not applicable		wa.paavola@yodamiitti.fi	21 hours ago	Static	Comp_APVM-8726300880	1 devices	Microsoft Corporation Virtual Machine
Device	Remediation	Check local Administrators members for non-appro	Without issues	Not run		3 days ago	Dynamic	DynDev - All Microsoft Corporation Virtual Mac	115 devices	
Device	Remediation	Create local admin account - Nordic Virtual Summi	Without issues	Not run		3 days ago	Static	Comp_APVM-8726300880	1 devices	
Device	Remediation	CVE-2023-24932 mitigation check 1/3 - Is Windows	With issues	Not run		3 days ago	Dynamic	All Devices		
Device	Remediation	CVE-2023-24932 mitigation check 2/3 - Is Windows	With issues	Not run		3 days ago	Dynamic	All Devices		
Device	Remediation	CVE-2023-24932 mitigation check 3/3 - Is deprecat	With issues	Not run		3 days ago	Dynamic	All Devices		
	Remediation	Disable Built-in Administrator account	Without issues	Not run	wa.paavola@yodamiitti.fi	12 days ago				

Intune Device JSON | Entra ID Device JSON | Primary User JSON
Latest Checked-In User JSON | Autopilot Device JSON | Autopilot Enrollment Profile JSON
Selected Application JSON | Selected Entra ID Group JSON | Selected Configuration JSON
Overview | **Bitlocker Keys** | **LAPS Password**

Device Name: APVM-8726300880

```
userPrincipalName     : etunimi.sukunimi@yodamiitti.fi
operatingSystem       : Windows
osVersion             : 10.0.22631.4169
skuFamily             : Enterprise
ownerType             : company
deviceType            : windowsRT
manufacturer          : Microsoft Corporation
model                 : Virtual Machine
chassisType           : laptop
serialNumber          : 0858-3566-8785-7423-8726-3008-80
joinType              : azureADJoined
deviceEnrollmentType  : windowsAzureADJoin
managedDeviceName     : etunimi.sukunimi_Windows_5/9/2024_9:50 PM
autopilotEnrolled     : True
enrollmentProfileName : Autopilot Deployment Profile AutopilotVM
enrolledDateTime      : 9.5.2024 21.50.32
```

Primary User: etunimi.sukunimi@yodamiitti.fi

```
accountEnabled    : True
displayName       : Etunimi Sukunimi
userPrincipalName : etunimi.sukunimi@yodamiitti.fi
email             :
userType          : Member
mobilePhone       : +358405966930
jobTitle          : Demo
department        : Demo Department
companyName       : Yodamiitti Oy
employeeId        : 123456543210
employeeType      :
streetAddress     :
postalCode        :
state             :
country           : Finland
officeLocation    : Yodamiitti Office
usageLocation     : FI
```

Latest or Selected Checked-in User: etunimi.sukunimi@yodamiitti.fi

```
accountEnabled    : True
displayName       : Etunimi Sukunimi
userPrincipalName : etunimi.sukunimi@yodamiitti.fi
email             :
userType          : Member
mobilePhone       : +358405966930
```

Device details updated 2024-09-14 13.58.10

Author: Petri.Paavola@yodamiitti.fi - Microsoft MVP
https://github.com/petripaavola/IntuneDeviceDetailsGUI

IntuneDeviceDetailsGUI updates

https://github.com/petripaavola/IntuneDeviceDetailsGUI

IntuneDeviceDetailsGUI

- Graphical Intune report which tells a LOT of information in one view

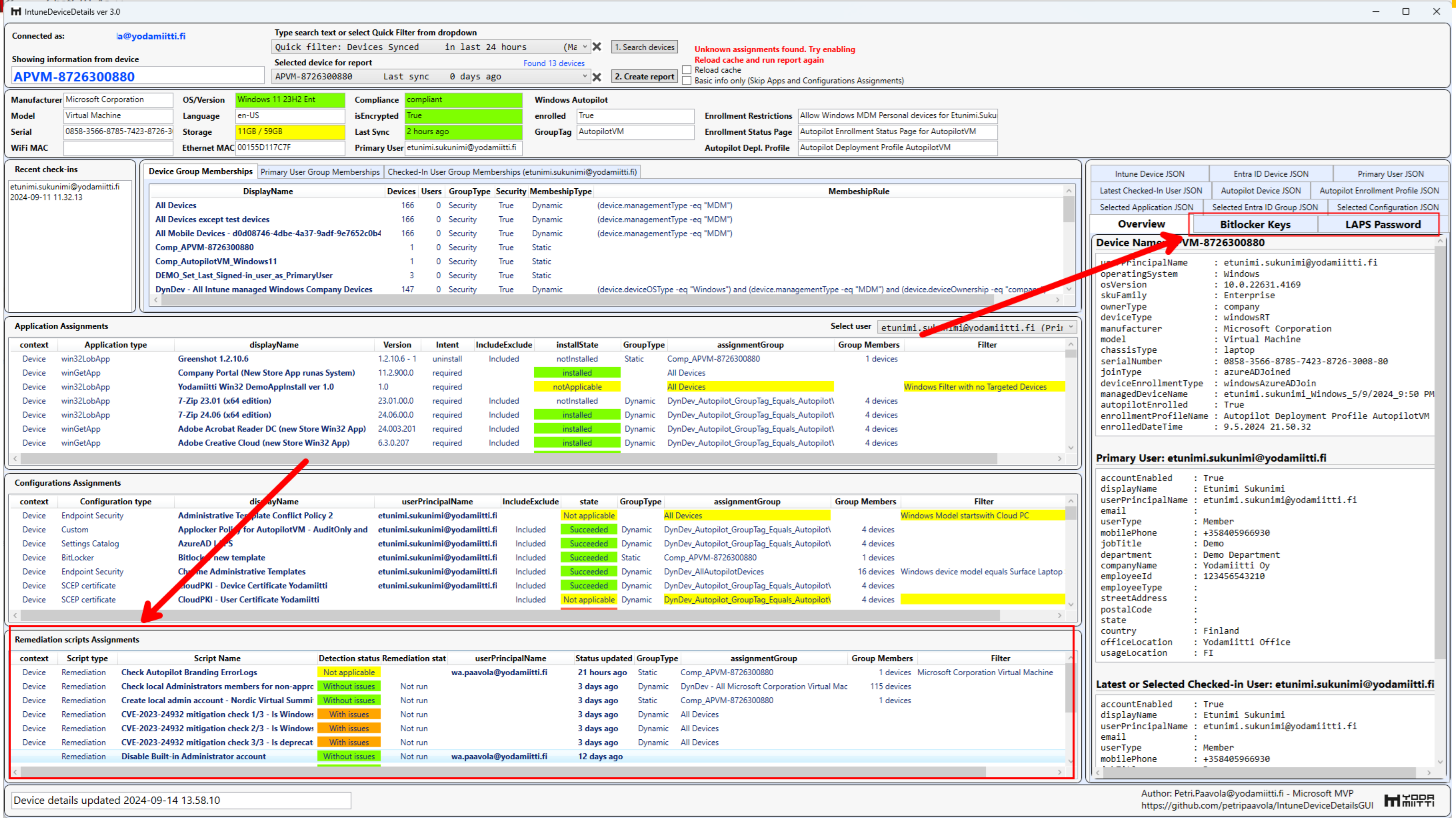
- This information is not easily available in Intune web console without doing tens of clicks to different pages and remembering everything you have seen in last few minutes of clicking

- DEMO Let's see new features for this tool
  - More information!

- Download from Petri's GitHub
  - https://github.com/petripaavola/IntuneDeviceDetailsGUI

IntuneDeviceDetailsGUI DEMO

www.wpninjas.fi



IntuneDeviceDetails ver 3.0

Connected as: la@yodamiitti.fi

Showing information from device
APVM-8726300880

Type search text or select Quick Filter from dropdown
Quick filter: Devices Synced in last 24 hours (Ma
1. Search devices

Selected device for report — Found 13 devices
APVM-8726300880 Last sync 0 days ago
2. Create report

Unknown assignments found. Try enabling
Reload cache and run report again

□ Reload cache
□ Basic info only (Skip Apps and Configurations Assignments)

Manufacturer	Microsoft Corporation	OS/Version	Windows 11 23H2 Ent	Compliance	compliant	Windows Autopilot	
Model	Virtual Machine	Language	en-US	isEncrypted	True	enrolled	True
Serial	0858-3566-8785-7423-8726-3	Storage	11GB / 59GB	Last Sync	2 hours ago	GroupTag	AutopilotVM
WiFi MAC		Ethernet MAC	00155D117C7F	Primary User	etunimi.sukunimi@yodamiitti.fi		

Enrollment Restrictions	Allow Windows MDM Personal devices for Etunimi.Suku
Enrollment Status Page	Autopilot Enrollment Status Page for AutopilotVM
Autopilot Depl. Profile	Autopilot Deployment Profile AutopilotVM

Recent check-ins

etunimi.sukunimi@yodamiitti.fi
2024-09-11 11.32.13

Device Group Memberships | Primary User Group Memberships | Checked-In User Group Memberships (etunimi.sukunimi@yodamiitti.fi)

DisplayName	Devices	Users	GroupType	Security	MembeshipType	MembeshipRule
All Devices	166	0	Security	True	Dynamic	(device.managementType -eq "MDM")
All Devices except test devices	166	0	Security	True	Dynamic	(device.managementType -eq "MDM")
All Mobile Devices - d0d08746-4dbe-4a37-9adf-9e7652c0b4	166	0	Security	True	Dynamic	(device.managementType -eq "MDM")
Comp_APVM-8726300880	1	0	Security	True	Static	
Comp_AutopilotVM_Windows11	1	0	Security	True	Static	
DEMO_Set_Last_Signed-in_user_as_PrimaryUser	3	0	Security	True	Static	
DynDev - All Intune managed Windows Company Devices	147	0	Security	True	Dynamic	(device.deviceOSType -eq "Windows") and (device.managementType -eq "MDM") and (device.deviceOwnership -eq "compa

Application Assignments

Select user: etunimi.sukunimi@yodamiitti.fi (Pri

context	Application type	displayName	Version	Intent	IncludeExclude	installState	GroupType	assignmentGroup	Group Members	Filter
Device	win32LobApp	Greenshot 1.2.10.6	1.2.10.6 - 1	uninstall	Included	notInstalled	Static	Comp_APVM-8726300880	1 devices	
Device	winGetApp	Company Portal (New Store App runas System)	11.2.900.0	required		installed		All Devices		
Device	win32LobApp	Yodamiitti Win32 DemoAppInstall ver 1.0	1.0	required		notApplicable		All Devices		Windows Filter with no Targeted Devices
Device	win32LobApp	7-Zip 23.01 (x64 edition)	23.01.00.0	required	Included	notInstalled	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	
Device	win32LobApp	7-Zip 24.06 (x64 edition)	24.06.00.0	required	Included	installed	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	
Device	winGetApp	Adobe Acrobat Reader DC (new Store Win32 App)	24.003.201	required	Included	installed	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	
Device	winGetApp	Adobe Creative Cloud (new Store Win32 App)	6.3.0.207	required	Included	installed	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	

Configurations Assignments

context	Configuration type	dis ayName	userPrincipalName	IncludeExclude	state	GroupType	assignmentGroup	Group Members	Filter
Device	Endpoint Security	Administrative Te plate Conflict Policy 2	etunimi.sukunimi@yodamiitti.fi		Not applicable		All Devices		Windows Model startswith Cloud PC
Device	Custom	Applocker Poli y for AutopilotVM - AuditOnly and	etunimi.sukunimi@yodamiitti.fi	Included	Succeeded	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	
Device	Settings Catalog	AzureAD L PS	etunimi.sukunimi@yodamiitti.fi	Included	Succeeded	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	
Device	BitLocker	Bitlock new template	etunimi.sukunimi@yodamiitti.fi	Included	Succeeded	Static	Comp_APVM-8726300880	1 devices	
Device	Endpoint Security	Ch me Administrative Templates	etunimi.sukunimi@yodamiitti.fi	Included	Succeeded	Dynamic	DynDev_AllAutopilotDevices	16 devices	Windows device model equals Surface Laptop
Device	SCEP certificate	loudPKI - Device Certificate Yodamiitti	etunimi.sukunimi@yodamiitti.fi	Included	Succeeded	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	
Device	SCEP certificate	CloudPKI - User Certificate Yodamiitti		Included	Not applicable	Dynamic	DynDev_Autopilot_GroupTag_Equals_Autopilot\	4 devices	

Remediation scripts Assignments

context	Script type	Script Name	Detection status	Remediation stat	userPrincipalName	Status updated	GroupType	assignmentGroup	Group Members	Filter
Device	Remediation	Check Autopilot Branding ErrorLogs	Not applicable		wa.paavola@yodamiitti.fi	21 hours ago	Static	Comp_APVM-8726300880	1 devices	Microsoft Corporation Virtual Machine
Device	Remediation	Check local Administrators members for non-appro	Without issues	Not run		3 days ago	Dynamic	DynDev - All Microsoft Corporation Virtual Mac	115 devices	
Device	Remediation	Create local admin account - Nordic Virtual Summi	Without issues	Not run		3 days ago	Static	Comp_APVM-8726300880	1 devices	
Device	Remediation	CVE-2023-24932 mitigation check 1/3 - Is Windows	With issues	Not run		3 days ago	Dynamic	All Devices		
Device	Remediation	CVE-2023-24932 mitigation check 2/3 - Is Windows	With issues	Not run		3 days ago	Dynamic	All Devices		
Device	Remediation	CVE-2023-24932 mitigation check 3/3 - Is deprecat	With issues	Not run		3 days ago	Dynamic	All Devices		
	Remediation	Disable Built-in Administrator account	Without issues	Not run	wa.paavola@yodamiitti.fi	12 days ago				

Device details updated 2024-09-14 13.58.10

Intune Device JSON | Entra ID Device JSON | Primary User JSON
Latest Checked-In User JSON | Autopilot Device JSON | Autopilot Enrollment Profile JSON
Selected Application JSON | Selected Entra ID Group JSON | Selected Configuration JSON

Overview | **Bitlocker Keys** | **LAPS Password**

Device Name VM-8726300880

```
us  PrincipalName     : etunimi.sukunimi@yodamiitti.fi
operatingSystem       : Windows
osVersion             : 10.0.22631.4169
skuFamily             : Enterprise
ownerType             : company
deviceType            : windowsRT
manufacturer          : Microsoft Corporation
model                 : Virtual Machine
chassisType           : laptop
serialNumber          : 0858-3566-8785-7423-8726-3008-80
joinType              : azureADJoined
deviceEnrollmentType  : windowsAzureADJoin
managedDeviceName     : etunimi.sukunimi_Windows_5/9/2024_9:50 PM
autopilotEnrolled     : True
enrollmentProfileName : Autopilot Deployment Profile AutopilotVM
enrolledDateTime      : 9.5.2024 21.50.32
```

Primary User: etunimi.sukunimi@yodamiitti.fi

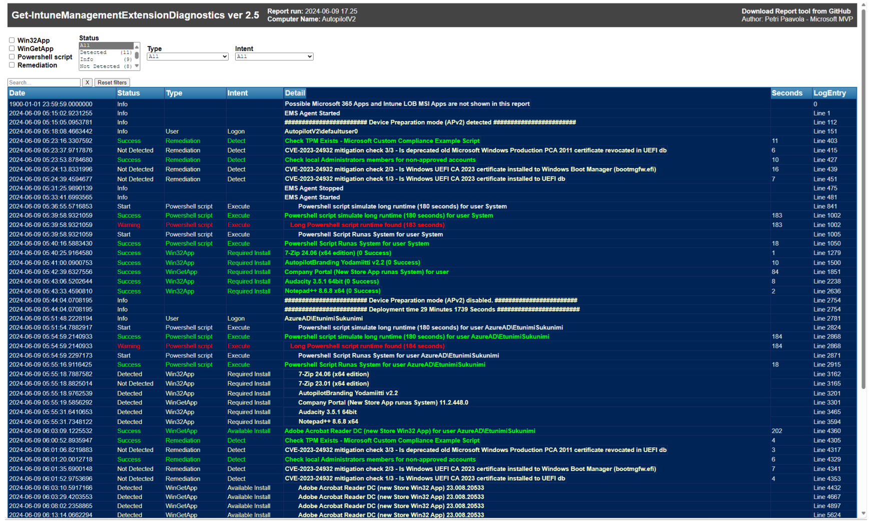
```
accountEnabled    : True
displayName       : Etunimi Sukunimi
userPrincipalName : etunimi.sukunimi@yodamiitti.fi
email             :
userType          : Member
mobilePhone       : +358405966930
jobTitle          : Demo
department        : Demo Department
companyName       : Yodamiitti Oy
employeeId        : 123456543210
employeeType      :
streetAddress     :
postalCode        :
state             :
country           : Finland
officeLocation    : Yodamiitti Office
usageLocation     : FI
```

Latest or Selected Checked-in User: etunimi.sukunimi@yodamiitti.fi

```
accountEnabled    : True
displayName       : Etunimi Sukunimi
userPrincipalName : etunimi.sukunimi@yodamiitti.fi
email             :
userType          : Member
mobilePhone       : +358405966930
```

Author: Petri.Paavola@yodamiitti.fi - Microsoft MVP
https://github.com/petripaavola/IntuneDeviceDetailsGUI

https://github.com/petripaavola/IntuneDeviceDetailsGUI



Get-IntuneManagementExtensionDiagnostics ver 2.5

Report run: 2024-06-09 17.25
Computer Name: AutopilotV2

Download Report tool from GitHub
Author: Petri Paavola - Microsoft MVP

□ Win32App
□ WinGetApp
□ Powershell script
□ Remediation

Status: All / Detected (11) / Info (9) / Not Detected (8)

Type: All

Intent: All

Date	Status	Type	Intent	Detail	Seconds	LogEntry
1900-01-01 23:59:59.0000000	Info			Possible Microsoft 365 Apps and Intune LOB MSI Apps are not shown in this report		0
2024-06-09 05:15:02.9231255	Info			EMS Agent Started		Line 1
2024-06-09 05:15:05.0953781	Info			######################## Device Preparation mode (APv2) detected ########################		Line 112
2024-06-09 05:18:08.4663442	Info	User	Logon	AutopilotV2\defaultuser0		Line 151
2024-06-09 05:23:16.3307592	Success	Remediation	Detect	Check TPM Exists - Microsoft Custom Compliance Example Script	11	Line 403
2024-06-09 05:23:37.9717876	Not Detected	Remediation	Detect	CVE-2023-24932 mitigation check 3/3 - Is deprecated old Microsoft Windows Production PCA 2011 certificate revocated in UEFI db	6	Line 415
2024-06-09 05:23:53.8784680	Success	Remediation	Detect	Check local Administrators members for non-approved accounts	10	Line 427
2024-06-09 05:24:13.8331996	Not Detected	Remediation	Detect	CVE-2023-24932 mitigation check 2/3 - Is Windows UEFI CA 2023 certificate installed to Windows Boot Manager (bootmgfw.efi)	16	Line 439
2024-06-09 05:24:39.4594677	Not Detected	Remediation	Detect	CVE-2023-24932 mitigation check 1/3 - Is Windows UEFI CA 2023 certificate installed to UEFI db	7	Line 451
2024-06-09 05:31:25.9890139	Info			EMS Agent Stopped		Line 475
2024-06-09 05:33:41.6993565	Info			EMS Agent Started		Line 481
2024-06-09 05:36:55.5716853	Start	Powershell script	Execute	Powershell script simulate long runtime (180 seconds) for user System		Line 841
2024-06-09 05:39:58.9321059	Success	Powershell script	Execute	Powershell script simulate long runtime (180 seconds) for user System	183	Line 1002
2024-06-09 05:39:58.9321059	Warning	Powershell script	Execute	Long Powershell script runtime found (183 seconds)	183	Line 1002
2024-06-09 05:39:58.9321059	Start	Powershell script	Execute	Powershell Script Runas System for user System		Line 1005
2024-06-09 05:40:16.5883430	Success	Powershell script	Execute	Powershell Script Runas System for user System	18	Line 1050
2024-06-09 05:40:25.9164580	Success	Win32App	Required Install	7-Zip 24.06 (x64 edition) (0 Success)	1	Line 1279
2024-06-09 05:41:00.0900753	Success	Win32App	Required Install	AutopilotBranding Yodamiitti v2.2 (0 Success)	10	Line 1500
2024-06-09 05:42:39.6327556	Success	WinGetApp	Required Install	Company Portal (New Store App runas System) for user	84	Line 1851
2024-06-09 05:43:06.5202644	Success	Win32App	Required Install	Audacity 3.5.1 64bit (0 Success)	8	Line 2238
2024-06-09 05:43:33.4590810	Success	Win32App	Required Install	Notepad++ 8.6.8 x64 (0 Success)	2	Line 2636
2024-06-09 05:44:04.0708195	Info			######################## Device Preparation mode (APv2) disabled. ########################		Line 2754
2024-06-09 05:44:04.0708195	Info			######################## Deployment time 29 Minutes 1739 Seconds ########################		Line 2754
2024-06-09 05:51:48.2228194	Info	User	Logon	AzureAD\EtunimiSukunimi		Line 2781
2024-06-09 05:51:54.7882917	Start	Powershell script	Execute	Powershell script simulate long runtime (180 seconds) for user AzureAD\EtunimiSukunimi		Line 2824
2024-06-09 05:54:59.2140933	Success	Powershell script	Execute	Powershell script simulate long runtime (180 seconds) for user AzureAD\EtunimiSukunimi	184	Line 2868
2024-06-09 05:54:59.2140933	Warning	Powershell script	Execute	Long Powershell script runtime found (184 seconds)	184	Line 2868
2024-06-09 05:54:59.2297173	Start	Powershell script	Execute	Powershell Script Runas System for user AzureAD\EtunimiSukunimi		Line 2871
2024-06-09 05:55:16.9116425	Success	Powershell script	Execute	Powershell Script Runas System for user AzureAD\EtunimiSukunimi	18	Line 2915
2024-06-09 05:55:18.7887582	Detected	Win32App	Required Install	7-Zip 24.06 (x64 edition)		Line 3162
2024-06-09 05:55:18.8825014	Not Detected	Win32App	Required Install	7-Zip 23.01 (x64 edition)		Line 3165
2024-06-09 05:55:18.9762539	Detected	Win32App	Required Install	AutopilotBranding Yodamiitti v2.2		Line 3201
2024-06-09 05:55:19.5856292	Detected	WinGetApp	Required Install	Company Portal (New Store App runas System) 11.2.448.0		Line 3301
2024-06-09 05:55:31.6410653	Detected	Win32App	Required Install	Audacity 3.5.1 64bit		Line 3465
2024-06-09 05:55:31.7348122	Detected	Win32App	Required Install	Notepad++ 8.6.8 x64		Line 3594
2024-06-09 06:03:09.1225532	Success	WinGetApp	Available Install	Adobe Acrobat Reader DC (new Store Win32 App) for user AzureAD\EtunimiSukunimi	202	Line 4360
2024-06-09 06:00:52.8935947	Success	Remediation	Detect	Check TPM Exists - Microsoft Custom Compliance Example Script	4	Line 4305
2024-06-09 06:01:06.8219883	Not Detected	Remediation	Detect	CVE-2023-24932 mitigation check 3/3 - Is deprecated old Microsoft Windows Production PCA 2011 certificate revocated in UEFI db	3	Line 4317
2024-06-09 06:01:20.0012718	Success	Remediation	Detect	Check local Administrators members for non-approved accounts	6	Line 4329
2024-06-09 06:01:35.6900148	Not Detected	Remediation	Detect	CVE-2023-24932 mitigation check 2/3 - Is Windows UEFI CA 2023 certificate installed to Windows Boot Manager (bootmgfw.efi)	7	Line 4341
2024-06-09 06:01:52.9753696	Not Detected	Remediation	Detect	CVE-2023-24932 mitigation check 1/3 - Is Windows UEFI CA 2023 certificate installed to UEFI db	4	Line 4353
2024-06-09 06:03:10.5917166	Detected	WinGetApp	Available Install	Adobe Acrobat Reader DC (new Store Win32 App) 23.008.20533		Line 4432
2024-06-09 06:03:29.4203553	Detected	WinGetApp	Available Install	Adobe Acrobat Reader DC (new Store Win32 App) 23.008.20533		Line 4667
2024-06-09 06:08:02.2358865	Detected	WinGetApp	Available Install	Adobe Acrobat Reader DC (new Store Win32 App) 23.008.20533		Line 4897
2024-06-09 06:13:14.0662294	Detected	WinGetApp	Available Install	Adobe Acrobat Reader DC (new Store Win32 App) 23.008.20533		Line 5624

Get-IntuneManagementExtensionDiagnostics updates

Famous Intune log events analysis report tool

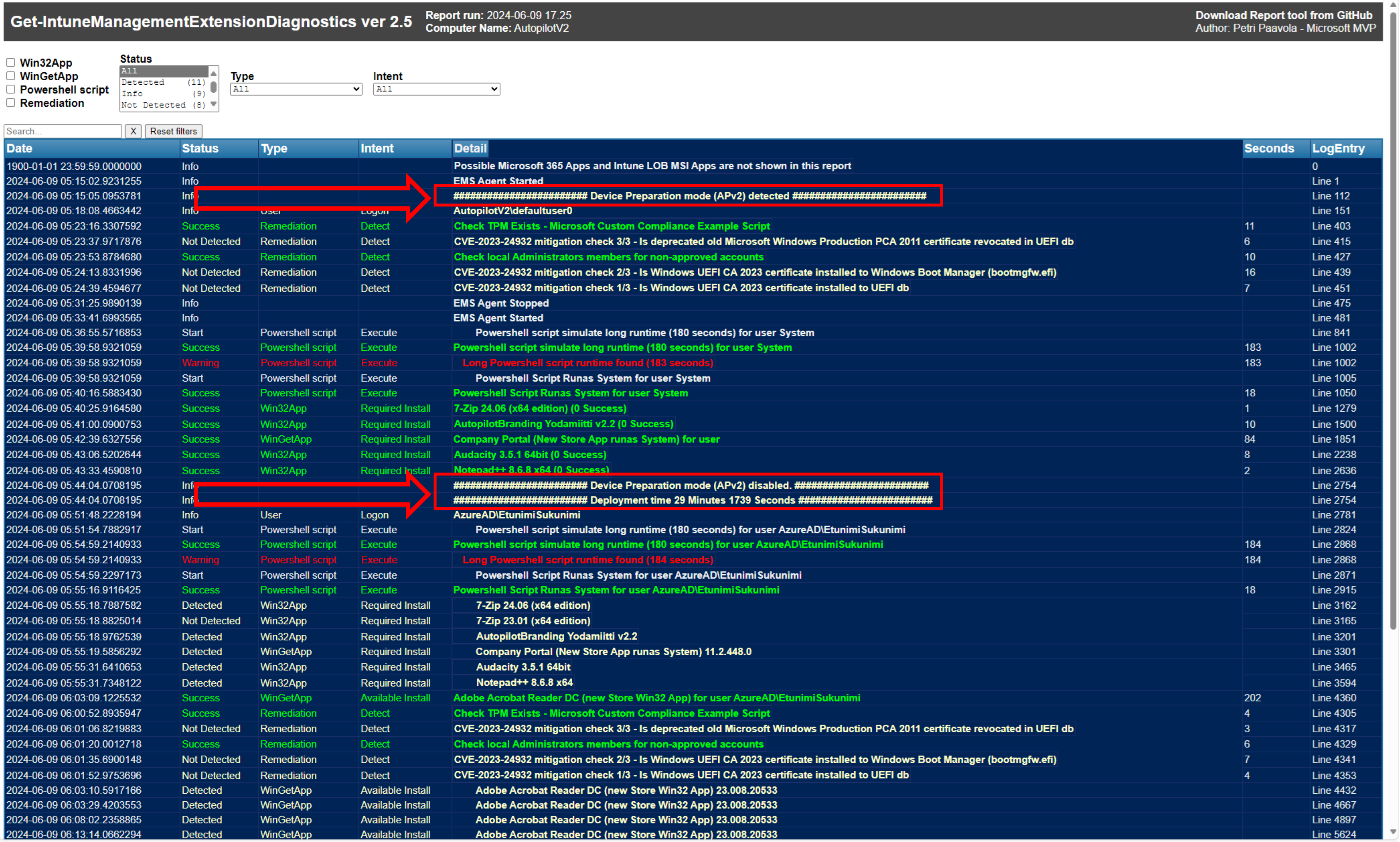
Get-IntuneManagementExtensionDiagnostics

- **Get-IntuneManagementExtensionDiagnostics** creates report of Intune Management Extension agent events from Intune log files
- Output is easy to read HTML report
- Shows information what happened and why

- Let's look for new features in this tool
  - More information, more details, Device preparation, PowerShell and Remediation script content and output, …

- Easy download from Powershell Gallery:
  - **Save-Script Get-IntuneManagementExtensionDiagnostics -Path ./**

Get-IntuneManagementExtensionDiagnostics DEMO



Get-IntuneManagementExtensionDiagnostics ver 2.5

Report run: 2024-06-09 17.25
Computer Name: AutopilotV2

Download Report tool from GitHub
Author: Petri Paavola - Microsoft MVP

- ☐ Win32App
- ☐ WinGetApp
- ☐ Powershell script
- ☐ Remediation

Status

```
All
Detected     (11)
Info          (9)
Not Detected  (8)
```

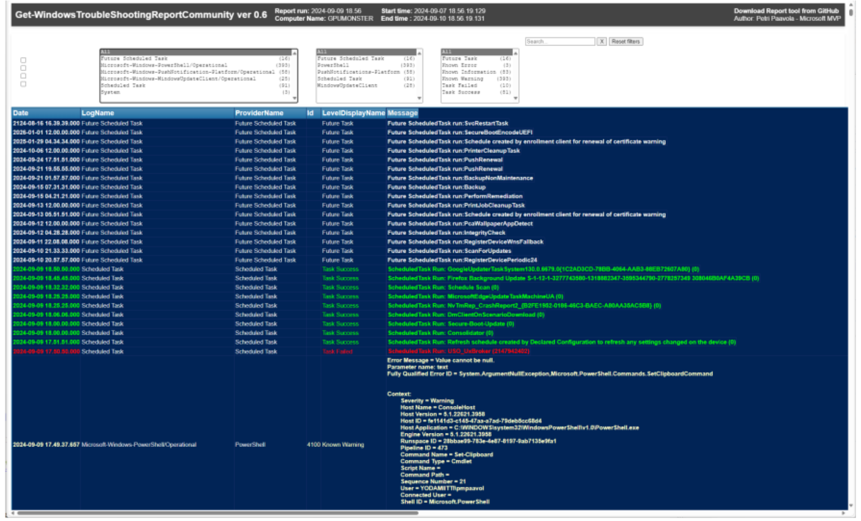
Type All

Intent All

Search... X Reset filters

Date	Status	Type	Intent	Detail	Seconds	LogEntry
1900-01-01 23:59:59.0000000	Info			Possible Microsoft 365 Apps and Intune LOB MSI Apps are not shown in this report		0
2024-06-09 05:15:02.9231255	Info			EMS Agent Started		Line 1
2024-06-09 05:15:05.0953781	Inf			######################## Device Preparation mode (APv2) detected ########################		Line 112
2024-06-09 05:18:08.4663442	Info	User	Logon	AutopilotV2\defaultuser0		Line 151
2024-06-09 05:23:16.3307592	Success	Remediation	Detect	Check TPM Exists - Microsoft Custom Compliance Example Script	11	Line 403
2024-06-09 05:23:37.9717876	Not Detected	Remediation	Detect	CVE-2023-24932 mitigation check 3/3 - Is deprecated old Microsoft Windows Production PCA 2011 certificate revocated in UEFI db	6	Line 415
2024-06-09 05:23:53.8784680	Success	Remediation	Detect	Check local Administrators members for non-approved accounts	10	Line 427
2024-06-09 05:24:13.8331996	Not Detected	Remediation	Detect	CVE-2023-24932 mitigation check 2/3 - Is Windows UEFI CA 2023 certificate installed to Windows Boot Manager (bootmgfw.efi)	16	Line 439
2024-06-09 05:24:39.4594677	Not Detected	Remediation	Detect	CVE-2023-24932 mitigation check 1/3 - Is Windows UEFI CA 2023 certificate installed to UEFI db	7	Line 451
2024-06-09 05:31:25.9890139	Info			EMS Agent Stopped		Line 475
2024-06-09 05:33:41.6993565	Info			EMS Agent Started		Line 481
2024-06-09 05:36:55.5716853	Start	Powershell script	Execute	Powershell script simulate long runtime (180 seconds) for user System		Line 841
2024-06-09 05:39:58.9321059	Success	Powershell script	Execute	Powershell script simulate long runtime (180 seconds) for user System	183	Line 1002
2024-06-09 05:39:58.9321059	Warning	Powershell script	Execute	Long Powershell script runtime found (183 seconds)	183	Line 1002
2024-06-09 05:39:58.9321059	Start	Powershell script	Execute	Powershell Script Runas System for user System		Line 1005
2024-06-09 05:40:16.5883430	Success	Powershell script	Execute	Powershell Script Runas System for user System	18	Line 1050
2024-06-09 05:40:25.9164580	Success	Win32App	Required Install	7-Zip 24.06 (x64 edition) (0 Success)	1	Line 1279
2024-06-09 05:41:00.0900753	Success	Win32App	Required Install	AutopilotBranding Yodamiitti v2.2 (0 Success)	10	Line 1500
2024-06-09 05:42:39.6327556	Success	WinGetApp	Required Install	Company Portal (New Store App runas System) for user	84	Line 1851
2024-06-09 05:43:06.5202644	Success	Win32App	Required Install	Audacity 3.5.1 64bit (0 Success)	8	Line 2238
2024-06-09 05:43:33.4590810	Success	Win32App	Required Install	Notepad++ 8.6.8 x64 (0 Success)	2	Line 2636
2024-06-09 05:44:04.0708195	Inf			######################## Device Preparation mode (APv2) disabled. ########################		Line 2754
2024-06-09 05:44:04.0708195	Inf			######################## Deployment time 29 Minutes 1739 Seconds ########################		Line 2754
2024-06-09 05:51:48.2228194	Info	User	Logon	AzureAD\EtunimiSukunimi		Line 2781
2024-06-09 05:51:54.7882917	Start	Powershell script	Execute	Powershell script simulate long runtime (180 seconds) for user AzureAD\EtunimiSukunimi		Line 2824
2024-06-09 05:54:59.2140933	Success	Powershell script	Execute	Powershell script simulate long runtime (180 seconds) for user AzureAD\EtunimiSukunimi	184	Line 2868
2024-06-09 05:54:59.2140933	Warning	Powershell script	Execute	Long Powershell script runtime found (184 seconds)	184	Line 2868
2024-06-09 05:54:59.2297173	Start	Powershell script	Execute	Powershell Script Runas System for user AzureAD\EtunimiSukunimi		Line 2871
2024-06-09 05:55:16.9116425	Success	Powershell script	Execute	Powershell Script Runas System for user AzureAD\EtunimiSukunimi	18	Line 2915
2024-06-09 05:55:18.7887582	Detected	Win32App	Required Install	7-Zip 24.06 (x64 edition)		Line 3162
2024-06-09 05:55:18.8825014	Not Detected	Win32App	Required Install	7-Zip 23.01 (x64 edition)		Line 3165
2024-06-09 05:55:18.9762539	Detected	Win32App	Required Install	AutopilotBranding Yodamiitti v2.2		Line 3201
2024-06-09 05:55:19.5856292	Detected	WinGetApp	Required Install	Company Portal (New Store App runas System) 11.2.448.0		Line 3301
2024-06-09 05:55:31.6410653	Detected	Win32App	Required Install	Audacity 3.5.1 64bit		Line 3465
2024-06-09 05:55:31.7348122	Detected	Win32App	Required Install	Notepad++ 8.6.8 x64		Line 3594
2024-06-09 06:03:09.1225532	Success	WinGetApp	Available Install	Adobe Acrobat Reader DC (new Store Win32 App) for user AzureAD\EtunimiSukunimi	202	Line 4360
2024-06-09 06:00:52.8935947	Success	Remediation	Detect	Check TPM Exists - Microsoft Custom Compliance Example Script	4	Line 4305
2024-06-09 06:01:06.8219883	Not Detected	Remediation	Detect	CVE-2023-24932 mitigation check 3/3 - Is deprecated old Microsoft Windows Production PCA 2011 certificate revocated in UEFI db	3	Line 4317
2024-06-09 06:01:20.0012718	Success	Remediation	Detect	Check local Administrators members for non-approved accounts	6	Line 4329
2024-06-09 06:01:35.6900148	Not Detected	Remediation	Detect	CVE-2023-24932 mitigation check 2/3 - Is Windows UEFI CA 2023 certificate installed to Windows Boot Manager (bootmgfw.efi)	7	Line 4341
2024-06-09 06:01:52.9753696	Not Detected	Remediation	Detect	CVE-2023-24932 mitigation check 1/3 - Is Windows UEFI CA 2023 certificate installed to UEFI db	4	Line 4353
2024-06-09 06:03:10.5917166	Detected	WinGetApp	Available Install	Adobe Acrobat Reader DC (new Store Win32 App) 23.008.20533		Line 4432
2024-06-09 06:03:29.4203553	Detected	WinGetApp	Available Install	Adobe Acrobat Reader DC (new Store Win32 App) 23.008.20533		Line 4667
2024-06-09 06:08:02.2358865	Detected	WinGetApp	Available Install	Adobe Acrobat Reader DC (new Store Win32 App) 23.008.20533		Line 4897
2024-06-09 06:13:14.0662294	Detected	WinGetApp	Available Install	Adobe Acrobat Reader DC (new Store Win32 App) 23.008.20533		Line 5624

https://github.com/petripaavola/Get-IntuneManagementExtensionDiagnostics



Get-WindowsTroubleShootingReportCommunity ver 0.6 **Report run:** 2024-09-09 18.56 **Computer Name:** GPUMONSTER **Start time:** 2024-09-07 18.56.19.129 **End time :** 2024-09-10 18.56.19.131

Download Report tool from GitHub
Author: Petri Paavola - Microsoft MVP

□
□
□
□

```
All
Future Scheduled Task                                      (16)
Microsoft-Windows-PowerShell/Operational                  (393)
Microsoft-Windows-PushNotification-Platform/Operational    (58)
Microsoft-Windows-WindowsUpdateClient/Operational          (28)
Scheduled Task                                             (91)
System                                                      (3)
```

```
All
Future Scheduled Task       (16)
PowerShell                 (393)
PushNotifications-Platform  (58)
Scheduled Task              (91)
WindowsUpdateClient         (28)
```

```
All
Future Task           (16)
Known Error            (3)
Known Information     (83)
Known Warning        (393)
Task Failed           (10)
Task Success          (81)
```

Date	LogName	ProviderName	Id	LevelDisplayName	Message
2124-08-16 16.39.39.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:SvcRestartTask
2026-01-01 12.00.00.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:SecureBootEncodeUEFI
2025-01-29 04.34.34.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:Schedule created by enrollment client for renewal of certificate warning
2024-10-06 12.00.00.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PrinterCleanupTask
2024-09-24 17.51.51.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PushRenewal
2024-09-21 19.55.55.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PushRenewal
2024-09-21 01.57.57.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:BackupNonMaintenance
2024-09-15 07.31.31.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:Backup
2024-09-15 04.21.21.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PerformRemediation
2024-09-13 12.00.00.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PrintJobCleanupTask
2024-09-13 05.51.51.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:Schedule created by enrollment client for renewal of certificate warning
2024-09-12 12.00.00.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PcaWallpaperAppDetect
2024-09-12 04.28.28.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:IntegrityCheck
2024-09-11 22.08.08.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:RegisterDeviceWnsFallback
2024-09-10 21.33.33.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:ScanForUpdates
2024-09-10 20.57.57.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:RegisterDevicePeriodic24
2024-09-09 18.50.50.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: GoogleUpdaterTaskSystem130.0.6679.0{1C2AD3CD-78BB-4064-AAB3-88EB72607A80} (0)
2024-09-09 18.45.45.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Firefox Background Update S-1-12-1-3277743580-1318882347-3595344790-2778257349 308046B0AF4A39CB (0)
2024-09-09 18.32.32.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Schedule Scan (0)
2024-09-09 18.25.25.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: MicrosoftEdgeUpdateTaskMachineUA (0)
2024-09-09 18.25.25.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: NvTmRep_CrashReport2_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} (0)
2024-09-09 18.06.06.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: DmClientOnScenarioDownload (0)
2024-09-09 18.00.00.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Secure-Boot-Update (0)
2024-09-09 18.00.00.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Consolidator (0)
2024-09-09 17.51.51.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Refresh schedule created by Declared Configuration to refresh any settings changed on the device (0)
2024-09-09 17.50.50.000	Scheduled Task	Scheduled Task		Task Failed	ScheduledTask Run: USO_UxBroker (2147942402)
2024-09-09 17.49.37.657	Microsoft-Windows-PowerShell/Operational	PowerShell	4100	Known Warning	Error Message = Value cannot be null. Parameter name: text Fully Qualified Error ID = System.ArgumentNullException,Microsoft.PowerShell.Commands.SetClipboardCommand Context: Severity = Warning Host Name = ConsoleHost Host Version = 5.1.22621.3958 Host ID = fe1141d3-c145-47aa-a7ad-79deb8cc68d4 Host Application = C:\WINDOWS\system32\WindowsPowerShell\v1.0\PowerShell.exe Engine Version = 5.1.22621.3958 Runspace ID = 28bbae99-783e-4e87-8197-9ab7135e9fa1 Pipeline ID = 473 Command Name = Set-Clipboard Command Type = Cmdlet Script Name = Command Path = Sequence Number = 21 User = YODAMIITT\pmpaavol Connected User = Shell ID = Microsoft.PowerShell

Introducing -

Get-WindowsTroubleShootingReportCommunity

The Ultimate Windows and Intune Troubleshooting Tool to troubleshoot anything and you can be part of the Contributing Community!

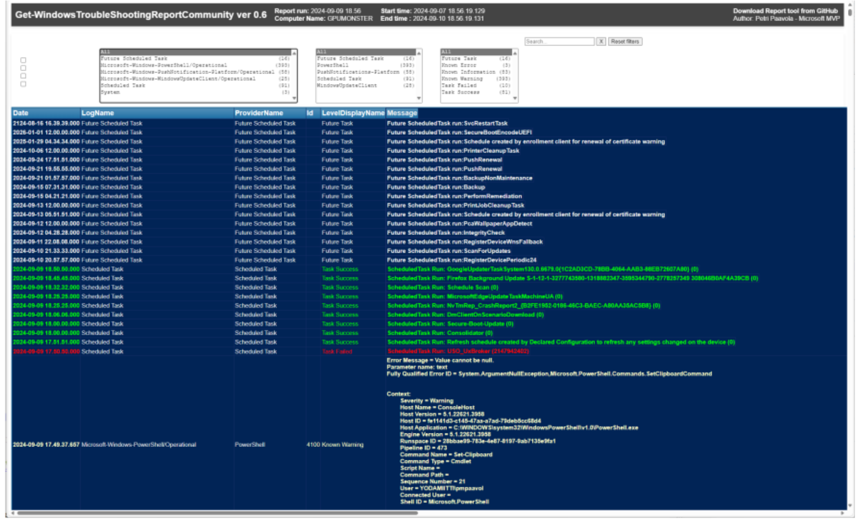
Get-WindowsTroubleShootingReportCommunity

- With PowerShell we can
  - get information very easily from Windows Events and from any log file
  - **objectify** data
  - sort and filter data(=objects) really easily
  - And we can show information in human readable format
- It all started with 2 commands (maybe don't run these commands ☺)
  - **Get-WinEvent * | Out-GridView**
  - **Get-Content -Path C:\Programdata\Microsoft\IntuneManagementExtension\logs\*.log | Out-GridView**
- That got me thinking about creating something new and unique
- Something where anyone can contribute the troubleshooting features
- Is this **THE** Troubleshooting Tool to analyze and report any events and log files?

Get-WindowsTroubleShootingReportCommunity

www.wpninjas.fi

- **Read Windows Event logs**
  - Online or from saved files (downloaded Diagnostics package)
- **Read any .log file format**
  - No restrictions for log file format as long as there is dateTime and message information in structured format
  - Intune/ConfigMgr CMTrace the most important ones but others too
- **Show events and logs sorted by dateTime**
  - This gives **timeline** what happened
  - For troubleshooting specific case you can show **ALL** events and logs
- **Detect Known Events and log messages**
  - Create easy to read report with only Known Events and log entries
  - Run report for extended long period (easily 30-365 days)
- **Realtime filtering and search by many ways in HTML report**
  - Scenario-based troubleshooting, for example Updates troubleshooting
- **Create your own Event Rules easily for detection**
- **Share you Event Rules to the rest of the world! ☺**



Get-WindowsTroubleShootingReportCommunity ver 0.6 **Report run:** 2024-09-09 18.56 **Computer Name:** GPUMONSTER **Start time:** 2024-09-07 18.56.19.129 **End time :** 2024-09-10 18.56.19.131 **Download Report tool from GitHub** Author: Petri Paavola - Microsoft MVP

Search... X Reset filters

□ □ □ □

```
All
Future Scheduled Task                                      (16)
Microsoft-Windows-PowerShell/Operational                   (393)
Microsoft-Windows-PushNotification-Platform/Operational    (58)
Microsoft-Windows-WindowsUpdateClient/Operational          (25)
Scheduled Task                                             (91)
System                                                     (3)
```

```
All
Future Scheduled Task         (16)
PowerShell                    (393)
PushNotifications-Platform    (58)
Scheduled Task                (91)
WindowsUpdateClient           (25)
```

```
All
Future Task           (16)
Known Error           (3)
Known Information     (83)
Known Warning         (393)
Task Failed           (10)
Task Success          (81)
```

Date	LogName	ProviderName	Id	LevelDisplayName	Message
2124-08-16 16.39.39.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:SvcRestartTask
2026-01-01 12.00.00.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:SecureBootEncodeUEFI
2025-01-29 04.34.34.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:Schedule created by enrollment client for renewal of certificate warning
2024-10-06 12.00.00.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PrinterCleanupTask
2024-09-24 17.51.51.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PushRenewal
2024-09-21 19.55.55.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PushRenewal
2024-09-21 01.57.57.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:BackupNonMaintenance
2024-09-15 07.31.31.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:Backup
2024-09-15 04.21.21.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PerformRemediation
2024-09-13 12.00.00.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PrintJobCleanupTask
2024-09-13 05.51.51.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:Schedule created by enrollment client for renewal of certificate warning
2024-09-12 12.00.00.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PcaWallpaperAppDetect
2024-09-12 04.28.28.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:IntegrityCheck
2024-09-11 22.08.08.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:RegisterDeviceWnsFallback
2024-09-10 21.33.33.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:ScanForUpdates
2024-09-10 20.57.57.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:RegisterDevicePeriodic24
2024-09-09 18.50.50.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: GoogleUpdaterTaskSystem130.0.6679.0{1C2AD3CD-78BB-4064-AAB3-88EB72607A80} (0)
2024-09-09 18.45.45.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Firefox Background Update S-1-12-1-3277743580-1318882347-3595344790-2778257349 308046B0AF4A39CB (0)
2024-09-09 18.32.32.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Schedule Scan (0)
2024-09-09 18.25.25.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: MicrosoftEdgeUpdateTaskMachineUA (0)
2024-09-09 18.25.25.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: NvTmRep_CrashReport2_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} (0)
2024-09-09 18.06.06.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: DmClientOnScenarioDownload (0)
2024-09-09 18.00.00.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Secure-Boot-Update (0)
2024-09-09 18.00.00.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Consolidator (0)
2024-09-09 17.51.51.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Refresh schedule created by Declared Configuration to refresh any settings changed on the device (0)
2024-09-09 17.50.50.000	Scheduled Task	Scheduled Task		Task Failed	ScheduledTask Run: USO_UxBroker (2147942402)
2024-09-09 17.49.37.657	Microsoft-Windows-PowerShell/Operational	PowerShell	4100	Known Warning	Error Message = Value cannot be null. Parameter name: text Fully Qualified Error ID = System.ArgumentNullException,Microsoft.PowerShell.Commands.SetClipboardCommand Context: Severity = Warning Host Name = ConsoleHost Host Version = 5.1.22621.3958 Host ID = fe1141d3-c145-47aa-a7ad-79deb8cc68d4 Host Application = C:\WINDOWS\system32\WindowsPowerShell\v1.0\PowerShell.exe Engine Version = 5.1.22621.3958 Runspace ID = 28bbae99-783e-4e87-8197-9ab7135e9fa1 Pipeline ID = 473 Command Name = Set-Clipboard Command Type = Cmdlet Script Name = Command Path = Sequence Number = 21 User = YODAMITT\pmpaavol Connected User = Shell ID = Microsoft.PowerShell

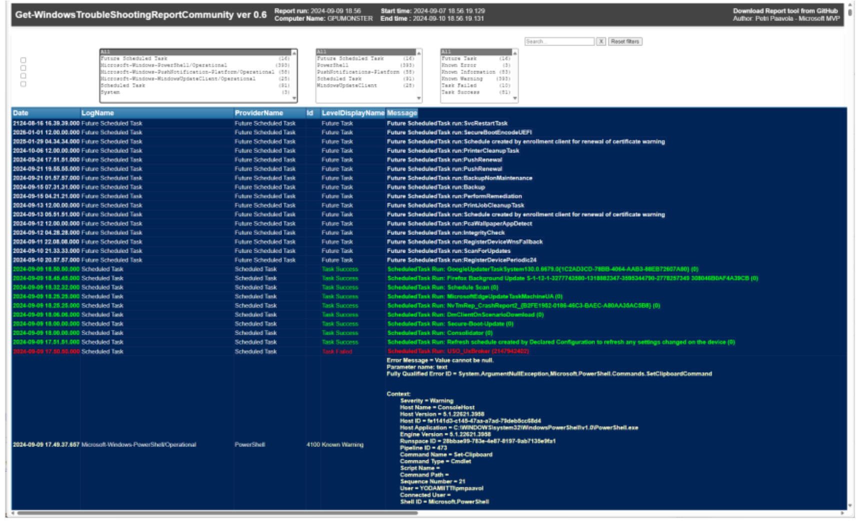
More details are revealed in Ninja Summit Session.

You will be the first one to see this new tool ☺

Get-WindowsTroubleShootingReportCommunity

www.wpninjas.fi

- **Scenario based views. For example do you really know exactly**
  - When Windows Updates installed in last 30 days, or not installed
    - When updates where actually installed after restart
    - What Firmware updates have been installed during last 365 days
  - Has Defender for Endpoint updated AV signatures and how often it runs
  - When computer restarted and changed to different power modes
  - What and when MSI applications installed and if they succeeded
  - When Store apps updated or failed
  - What PowerShell scripts ran in computer
  - Intune related events (enrollment, sync, MDM setting, app and scripts run)
  - ConfigMgr related events
  - What Errors there are in Event logs for last x minutes/hours/days
  - Did your Intune MDM policies succeeded or failed
  - and much more …
- **This list is just the beginning**
- **You can help by creating and sharing more Known Event rules!**



Get-WindowsTroubleShootingReportCommunity ver 0.6 **Report run:** 2024-09-09 18.56 **Computer Name:** GPUMONSTER **Start time:** 2024-09-07 18.56.19.129 **End time :** 2024-09-10 18.56.19.131 **Download Report tool from GitHub** Author: Petri Paavola - Microsoft MVP

```
All
Future Scheduled Task                                     (16)
Microsoft-Windows-PowerShell/Operational                 (393)
Microsoft-Windows-PushNotification-Platform/Operational   (58)
Microsoft-Windows-WindowsUpdateClient/Operational         (25)
Scheduled Task                                            (91)
System                                                     (3)
```

```
All
Future Scheduled Task       (16)
PowerShell                 (393)
PushNotifications-Platform  (58)
Scheduled Task              (91)
WindowsUpdateClient         (28)
```

```
All
Future Task          (16)
Known Error           (3)
Known Information    (83)
Known Warning       (393)
Task Failed          (10)
Task Success         (81)
```

Date	LogName	ProviderName	Id	LevelDisplayName	Message
2124-08-16 16.39.39.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:SvcRestartTask
2026-01-01 12.00.00.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:SecureBootEncodeUEFI
2025-01-29 04.34.34.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:Schedule created by enrollment client for renewal of certificate warning
2024-10-06 12.00.00.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PrinterCleanupTask
2024-09-24 17.51.51.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PushRenewal
2024-09-21 19.55.55.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PushRenewal
2024-09-21 01.57.57.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:BackupNonMaintenance
2024-09-15 07.31.31.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:Backup
2024-09-15 04.21.21.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PerformRemediation
2024-09-13 12.00.00.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PrintJobCleanupTask
2024-09-13 05.51.51.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:Schedule created by enrollment client for renewal of certificate warning
2024-09-12 12.00.00.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:PcaWallpaperAppDetect
2024-09-12 04.28.28.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:IntegrityCheck
2024-09-11 22.08.08.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:RegisterDeviceWnsFallback
2024-09-10 21.33.33.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:ScanForUpdates
2024-09-10 20.57.57.000	Future Scheduled Task	Future Scheduled Task		Future Task	Future ScheduledTask run:RegisterDevicePeriodic24
2024-09-09 18.50.50.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: GoogleUpdaterTaskSystem130.0.6679.0{1C2AD3CD-78BB-4064-AAB3-88EB72607A80} (0)
2024-09-09 18.45.45.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Firefox Background Update S-1-12-1-3277743580-1318882347-3595344790-2778257349 308046B0AF4A39CB (0)
2024-09-09 18.32.32.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Schedule Scan (0)
2024-09-09 18.25.25.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: MicrosoftEdgeUpdateTaskMachineUA (0)
2024-09-09 18.25.25.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: NvTmRep_CrashReport2_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} (0)
2024-09-09 18.06.06.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: DmClientOnScenarioDownload (0)
2024-09-09 18.00.00.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Secure-Boot-Update (0)
2024-09-09 18.00.00.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Consolidator (0)
2024-09-09 17.51.51.000	Scheduled Task	Scheduled Task		Task Success	ScheduledTask Run: Refresh schedule created by Declared Configuration to refresh any settings changed on the device (0)
2024-09-09 17.50.50.000	Scheduled Task	Scheduled Task		Task Failed	ScheduledTask Run: USO_UxBroker (2147942402)
2024-09-09 17.49.37.657	Microsoft-Windows-PowerShell/Operational	PowerShell	4100	Known Warning	Error Message = Value cannot be null. Parameter name: text Fully Qualified Error ID = System.ArgumentNullException,Microsoft.PowerShell.Commands.SetClipboardCommand Context: Severity = Warning Host Name = ConsoleHost Host Version = 5.1.22621.3958 Host ID = fe1141d3-c145-47aa-a7ad-79deb5cc68d4 Host Application = C:\WINDOWS\system32\WindowsPowerShell\v1.0\PowerShell.exe Engine Version = 5.1.22621.3958 Runspace ID = 28bbae99-783e-4e87-8197-9ab7135e9fa1 Pipeline ID = 473 Command Name = Set-Clipboard Command Type = Cmdlet Script Name = Command Path = Sequence Number = 21 User = YODAMIITTI\pmpaavol Connected User = Shell ID = Microsoft.PowerShell

More details are revealed in Ninja Summit Session.

You will be the first one to see this new tool ☺

Showcase and DEMO
of the new
troubleshoot anything in the world -tool

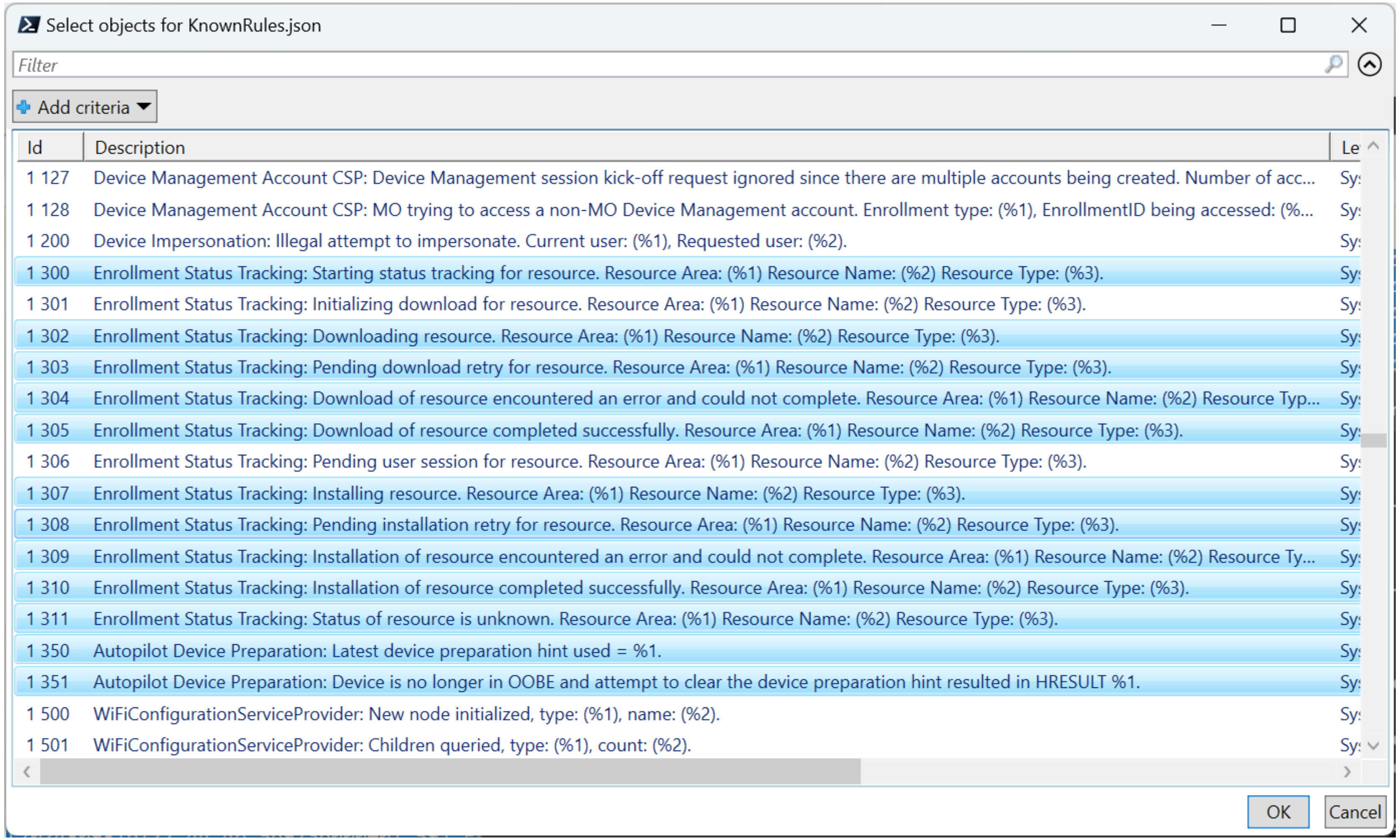
Get-WindowsTroubleShootingReportCommunity

Create Known Events rules easily

- **I created a helper tool which helps you to create Scenarios from Event log events**

.\Create-EventRules-GUI-HelperTool.ps1

- **Hard part is to figure out Categories and what events we are interested on**
- **Something completed -> Green**
- **Something failed -> Red**
- **Do not add everything?**
- **Or create 2 sets?**
  - **Limited (success and fails)**
  - **Full (all events)**



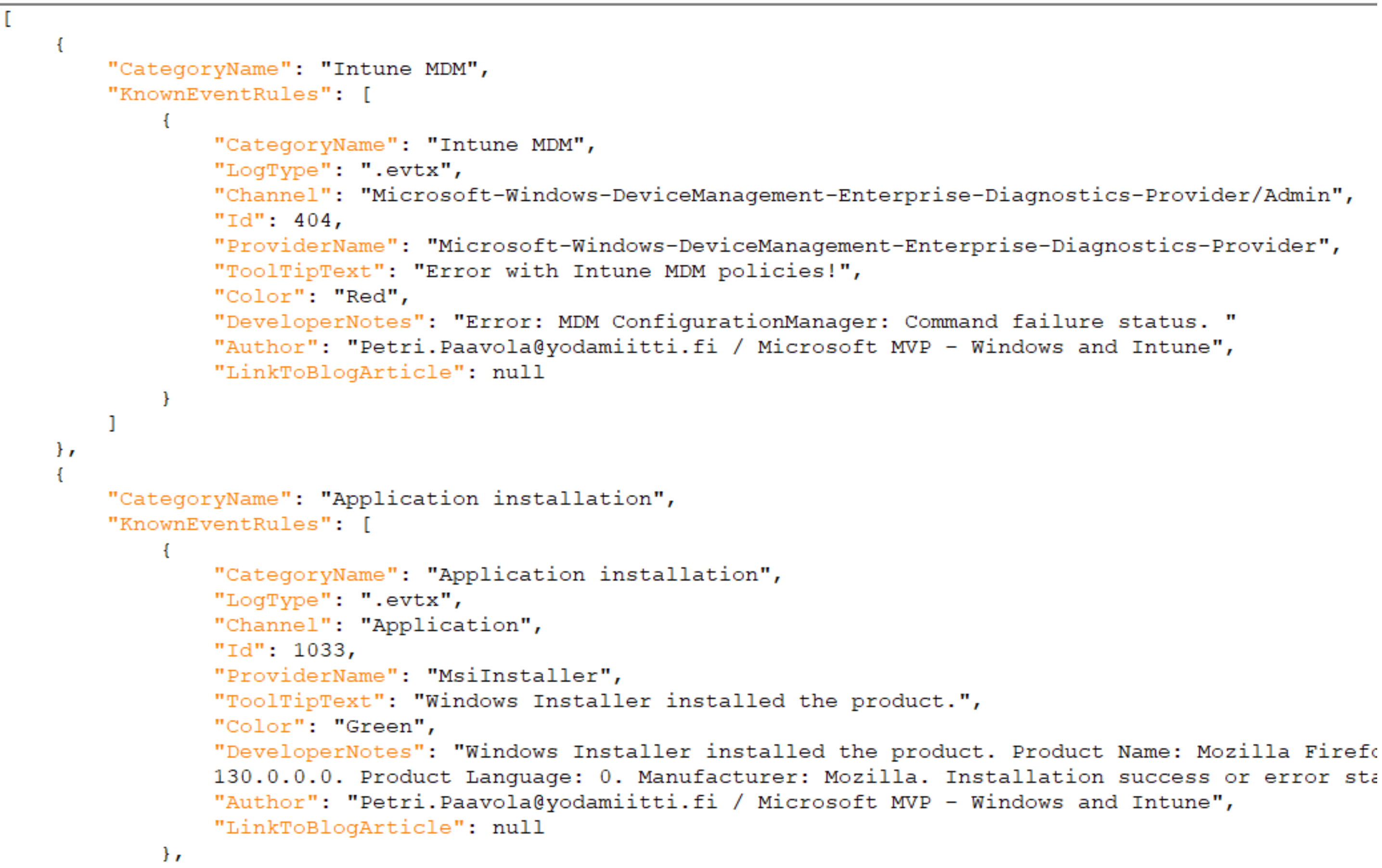
Id	Description	Le
1 127	Device Management Account CSP: Device Management session kick-off request ignored since there are multiple accounts being created. Number of acc...	Sy
1 128	Device Management Account CSP: MO trying to access a non-MO Device Management account. Enrollment type: (%1), EnrollmentID being accessed: (%...	Sy
1 200	Device Impersonation: Illegal attempt to impersonate. Current user: (%1), Requested user: (%2).	Sy
1 300	Enrollment Status Tracking: Starting status tracking for resource. Resource Area: (%1) Resource Name: (%2) Resource Type: (%3).	Sy
1 301	Enrollment Status Tracking: Initializing download for resource. Resource Area: (%1) Resource Name: (%2) Resource Type: (%3).	Sy
1 302	Enrollment Status Tracking: Downloading resource. Resource Area: (%1) Resource Name: (%2) Resource Type: (%3).	Sy
1 303	Enrollment Status Tracking: Pending download retry for resource. Resource Area: (%1) Resource Name: (%2) Resource Type: (%3).	Sy
1 304	Enrollment Status Tracking: Download of resource encountered an error and could not complete. Resource Area: (%1) Resource Name: (%2) Resource Typ...	Sy
1 305	Enrollment Status Tracking: Download of resource completed successfully. Resource Area: (%1) Resource Name: (%2) Resource Type: (%3).	Sy
1 306	Enrollment Status Tracking: Pending user session for resource. Resource Area: (%1) Resource Name: (%2) Resource Type: (%3).	Sy
1 307	Enrollment Status Tracking: Installing resource. Resource Area: (%1) Resource Name: (%2) Resource Type: (%3).	Sy
1 308	Enrollment Status Tracking: Pending installation retry for resource. Resource Area: (%1) Resource Name: (%2) Resource Type: (%3).	Sy
1 309	Enrollment Status Tracking: Installation of resource encountered an error and could not complete. Resource Area: (%1) Resource Name: (%2) Resource Ty...	Sy
1 310	Enrollment Status Tracking: Installation of resource completed successfully. Resource Area: (%1) Resource Name: (%2) Resource Type: (%3).	Sy
1 311	Enrollment Status Tracking: Status of resource is unknown. Resource Area: (%1) Resource Name: (%2) Resource Type: (%3).	Sy
1 350	Autopilot Device Preparation: Latest device preparation hint used = %1.	Sy
1 351	Autopilot Device Preparation: Device is no longer in OOBE and attempt to clear the device preparation hint resulted in HRESULT %1.	Sy
1 500	WiFiConfigurationServiceProvider: New node initialized, type: (%1), name: (%2).	Sy
1 501	WiFiConfigurationServiceProvider: Children queried, type: (%1), count: (%2).	Sy

More details are revealed in Ninja Summit Session.

You will be the first one to see this new tool ☺

Get-WindowsTroubleShootingReportCommunity

www.wpninjas.fi



```
[
    {
        "CategoryName": "Intune MDM",
        "KnownEventRules": [
            {
                "CategoryName": "Intune MDM",
                "LogType": ".evtx",
                "Channel": "Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Admin",
                "Id": 404,
                "ProviderName": "Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider",
                "ToolTipText": "Error with Intune MDM policies!",
                "Color": "Red",
                "DeveloperNotes": "Error: MDM ConfigurationManager: Command failure status. "
                "Author": "Petri.Paavola@yodamiitti.fi / Microsoft MVP - Windows and Intune",
                "LinkToBlogArticle": null
            }
        ]
    },
    {
        "CategoryName": "Application installation",
        "KnownEventRules": [
            {
                "CategoryName": "Application installation",
                "LogType": ".evtx",
                "Channel": "Application",
                "Id": 1033,
                "ProviderName": "MsiInstaller",
                "ToolTipText": "Windows Installer installed the product.",
                "Color": "Green",
                "DeveloperNotes": "Windows Installer installed the product. Product Name: Mozilla Firef
                130.0.0.0. Product Language: 0. Manufacturer: Mozilla. Installation success or error sta
                "Author": "Petri.Paavola@yodamiitti.fi / Microsoft MVP - Windows and Intune",
                "LinkToBlogArticle": null
            },
```

Create and Share your Known Event Rules

Download tools from GitHub and Powershell Gallery

Työkalu vielä "hiljaisessa" jakelussa, joten se on saatavilla, mutta sitä ei ole julkisesti julkaistu vielä. Kokeile ja laita palautetta miltä näyttää.

https://github.com/petripaavola/Get-WindowsTroubleshootingReportCommunity

Check out my GitHub for Community Tools downloads and documentation

Powershell.ninja

https://github.com/petripaavola

Thank You