

Workplace Ninja User Group Finland

29.11.2024



Workplace Ninja
User Group Finland



29.11.2024 Ohjelma

www.wpninjas.fi

- **09.00 - 09.10 Avaus & Uutiset & Discord**
Workplace Ninja User Group Finland
- **09.10 - 09.55 Ignite-uutiset**
WPNinjas ja Mikko Lindström (Microsoft) ja kaikki muutkin
- **09.55 - 10.05 Tauko**
- **10.05 - 11.00 Kuinka PAW tehdään kunnollisesti -
myös cloud-only ympäristössä**
Sami Laiho - WPNinja ja Microsoft MVP
- **11.00 - 11.15 Ask The Ninjas!**
Kysy mitä mieleen juolahtaa



Syksyn in-person-tapaamisen palautteet

www.wpninjas.fi

Posia

- Sisällöstä tuli paljon kiitosta
 - Niin Petrin kuin Pavelin puheenvuorot koettiin mielenkiintoisiksi
- Rento ilmapiiri
- Yhteisöllisyyden tunne 🤪
- Hyvät tilat
- Verkostoituminen tärkeää
- Hyviä keskusteluja
- Osallistujat aktiivisia
- Sponsoripuheetkin oli ok

Kehitettävää

- Tarjoilut monipuolisemmaksi
- Tauot pidemmiksi
- Monipuolisemmat aiheet

"Hyvää keskustelua koko päivän ajan ja pystyi tutustumaan uusiin ihmisiin eli verkostoitumaan!"

"Rento ilmapiiri, hyvät aiheet, safkat ja juomat asialliset."

"Todella helposti saavutettava sijainti ja tilat."

"Nörttihenki, positiivisuus ja avoimuus. Seurustelu samanhenkisten kanssa oli mahtavaa."

"Tykkäsin kovasti live-tapaamisesta, toivottavasti järjestätte lisää."

"Ehkä ne patongit ois voinu korvata jollain toisella ruoalla."

"Aikataulu oli aika tiukka – tauot olisivat voineet olla hieman pidempiä."

"Security-puolen asioita voisi olla enemmän seuraavaan sessioon."

"Monipuolisemmin esityksiä, mutta ymmärrän, että esiintyjäpulaa on ilmassa."



Syksyn in-person-tapaamisen palautteet

www.wpninjas.fi

9. Arvosana muille järjestelyille

[More details](#)

4.72

Average Rating



Level 5  23

Level 4  4

Level 3  2

Level 2

Level 1



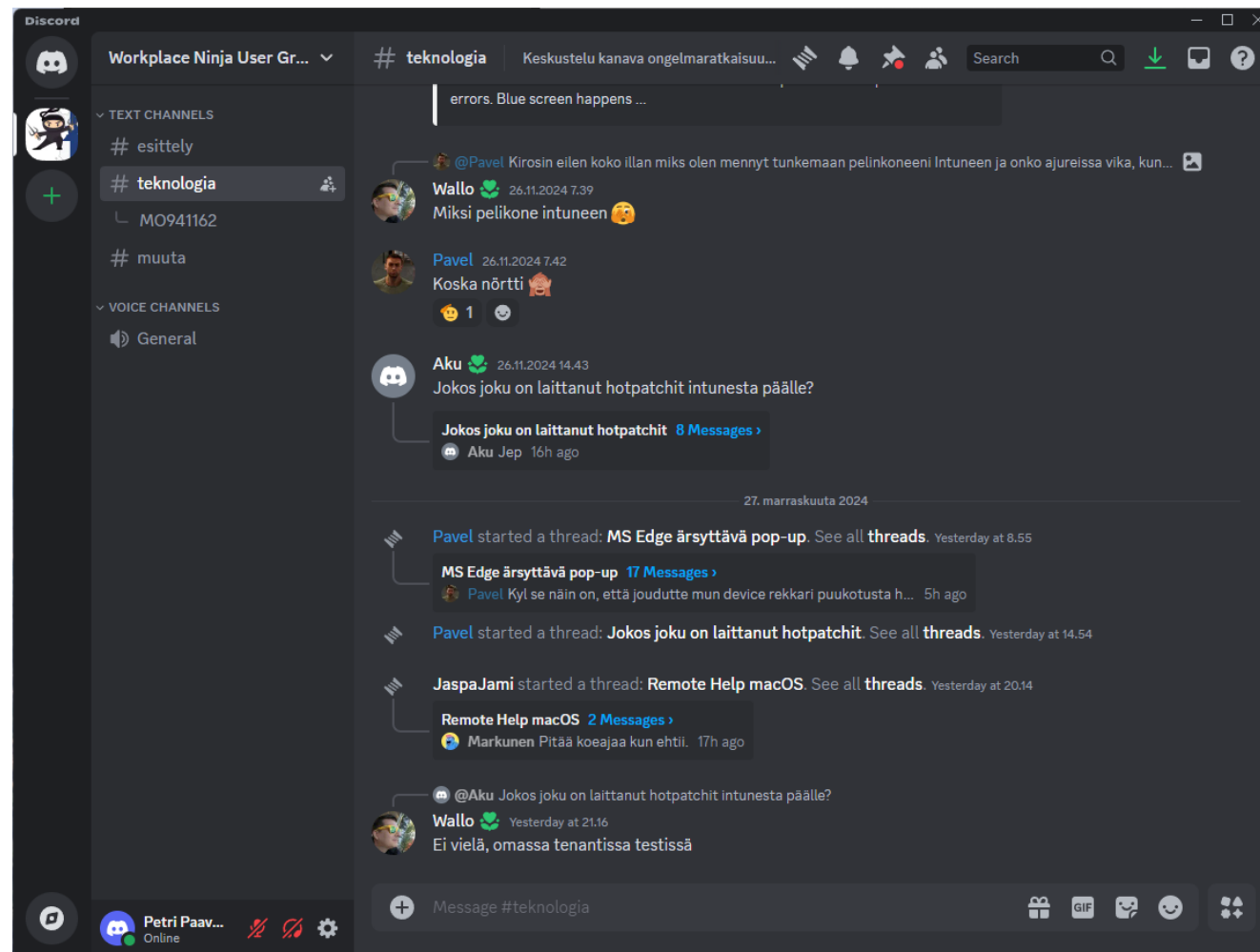
Discord-kanava avattu!

www.wpninjas.fi

- Kyselyssä Discord voitti kanavaksi reaaliaika-chattiin
- Discord-kanava on nyt luotu
- Discordille annetaan **2 kuukauden koeaika** ja sen jälkeen katsotaan mikä tilanne on

Liity mukaan!

<https://discord.gg/9pAAAVJv7N>



Mitä uutta Ignite 2024 työasemahallinnassa?



Workplace Ninja
User Group Finland

Windows 365/AVD uudistukset

Mikko Lindström/Microsoft Oy



Ignite 2024 eli Perämiehen syttyminen





- Microsoftin pääseminaari
- Vihdoin taas isompana live-seminaarina Chicagossa
 - Ilmainen virtuaalitapahtuma
- Pääpaino markkinointiviestillä
 - Julkistetaan eri tuotteita
 - Tekninen sisältö vähissä
 - [Book of News](https://news.microsoft.com/ignite-2024-book-of-news/) sisältää kaikki julkistukset
<https://news.microsoft.com/ignite-2024-book-of-news/>
- Työasemapuolella ollut teknisempi virtuaalikonffa Technical Takeoff Igniten jälkeen
 - Ollut paljon teknisiä nauhoitettuja esityksiä
 - Tänä vuonna ei tullut Igniten jälkeen syksyllä → kalenteriongelma



Intune Device inventory

www.wpninjas.fi

- Julkistettiin
 - Aluksi Windows-laitteet
- Ei vielä ulkona ☹️
 - Joulukuussa?
- Luvattiin myös iOS, Android, macOS ja Linux laitteille



Intune Device query

Usean koneen Device query julkistettiin.
Mahdollisuus ajaa toimintoja koneille, myös remediation scripts!
(Ei vielä ulkona)

Properties

Search

▼ BiosInfo

▼ Certificate

▼ Cpu

▲ DiskDrive

Description

DiskName

Driveld

DriveIndex

InterfaceType

Manufacturer

Model

PartitionCount

PnpDeviceId

▶ Run ✕ Clear input ✕ Cancel 🔗 Query with Copilot

1 DiskDrive

Get started

Results

Columns ▼

Device Actions ▼

Driveld

\\.\PHYSICALD...

Delete

Retire

Wipe

Collect diagnostics

Autopilot Reset

Fresh Start

Pause config refresh

Restart

PnpDeviceId	SizeBytes	Manufacturer	Model
SCSI\DISK&VE...	256052966400	(Standard disk ...	SAMSUNG MZ...

es/DeviceSettingsMenuBlade/~/compliance...



Copilot ja Device query

- Mahdollisuus luoda Device query:n KQL kyselyjä Copilotin avulla

The screenshot displays the Microsoft Intune admin center interface. On the left is a navigation pane with options like Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area is titled 'Devices | Device query (preview)'. It includes a search bar and a list of properties for device queries, such as Battery, BiosInfo, Cpu, DiskDrive, EncryptableVolume, LogicalDrive, MemoryInfo, NetworkAdapter, OsVersion, SystemEnclosure, Time, Tpm, and VideoController. On the right, the 'Copilot (preview)' panel is open, showing a prompt to improve the experience by sharing feedback. Below this, a text box contains a request: 'Generate a report of my devices' specification, list their CPU model, type, and core count, OS name and version, bios name and version, and disk size, and memory size. Also include the manufacturer if available'. The Copilot panel then displays a generated KQL query:

```
Cpu | join (OsVersion) | join (BiosInfo) | join (DiskDrive) | join (MemoryInfo) | project Device, Model, ProcessorType, CoreCount, OsName, OsVersion, BiosName,
```

 with buttons for 'Add to editor' and 'Add and run'. Below the query, it says 'How was this query generated?' and 'AI generated content may be incorrect. Check it for accuracy.' At the bottom of the Copilot panel, there is a text input field labeled 'Request device data or enter your question' and a 'View prompts' link. The footer of the Copilot panel reads 'Generated by Copilot for Security' with a 'Learn more' link.



Copilot ja Enterprise Privilege Management

Tarkistaa elevointia pyydettävän ohjelman hyvyys (Microsoft Defender Threat Intelligence)

Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Endpoint security

Endpoint security | Endpoint Privilege Management

Search

Reports Policies Reusable settings Elevation requests

Refresh

Status == all

File	Publisher	Username
InstallPrinter.msi	UnknownPublisher	User1@contoso
Procmon.exe	UnknownPublisher	User1@contoso
MusicSoftware.exe	Microsoft Windows	User2@contoso
regedit.exe	Microsoft Windows	User3@contoso
rdpinput.exe	Microsoft Windows	User1@contoso
splwow64.exe	Microsoft Windows	User3@contoso

Overview

All devices

Security baselines

Security tasks

Manage

Antivirus

Disk encryption

Firewall

Endpoint Privilege Management

Endpoint detection and response

App Control for Business (Preview)

Attack surface reduction

Account protection

Device compliance

Conditional access

Monitor

Assignment failures

Setup

Microsoft Defender for Endpoint

Help and support

Help and support

Copilot (preview)

The reputation details for the indicator of compromise "94795fd89366e01bd6ce6471ff27c3782e2e16377a848426cf0b2e6baee9449b" are as follows:

Score: 100

Classification: MALICIOUS

Last seen: 2024-10-17T13:37:58Z

Rules:

- Name: Indicator related to a known Malware campaign
- Description: This file has traits consistent with hacking tool.
- Name: Indicator related to a known Malware campaign
- Description: This file has traits based from Microsoft Windows Defender engine.

MITRE Techniques: T1106

References:
MDTI: 94795fd89366e01bd6ce6471ff27c3782e2e16377a848426cf0b2e6baee9449b
T1106

AI generated content may be incorrect. Check it for accuracy.

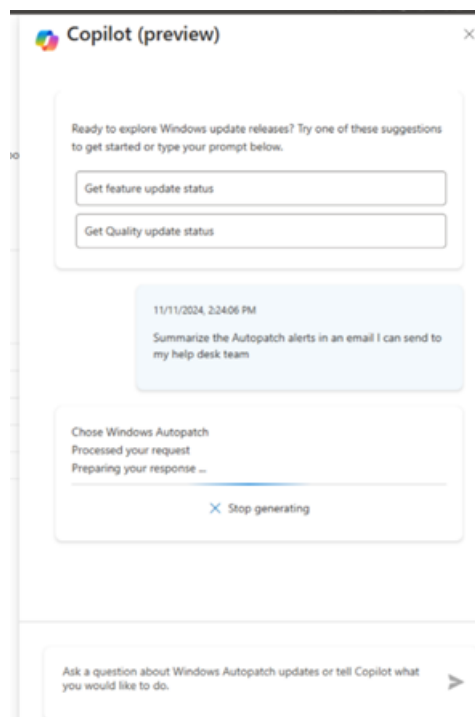
View prompts
Generated by Copilot for Security Learn more



Copilot lisäjuttuja

www.wpninjas.fi

- Configurations
 - Yhteenvedo asetuksista
 - Tulossa vapaampi kyselymahdollisuus
- Autopatch
 - Päivitysten vaikutus
 - Ongelmat päivityksissä





Intune policyt

www.wpninjas.fi

- Intune device configuration näyttää nyt myös Endpoint Security -policyt samassa näkymässä
- Huom! Uusia Administrative Templateja ei voi kohta enää tehdä (2412 eteenpäin)
- Custom OMA-URI:n voi jatkossa luoda vain, jos asetusta ei ole Settings Catalogissa
- Olemassa olevat Administrative Templatet migroidaan Settings Catalog -tyyppisiksi

<https://techcommunity.microsoft.com/blog/intunecustomersuccess/support-tip-windows-device-configuration-policies-migrating-to-unified-settings-/4189665>



(Enterprise?) App management

- Pre/post actions
 - Toivottavasti kaikille Intune-asiakkaille
 - Vielä vähän tietoa

Program Edit	
Pre-install script	No Pre-install script
Post-install script	No Post-install script

- Tämä toiminto on ollut jo pidempään macOS PKG-sovellusjakelussa ja toive on ollut suuri saada sama toiminnallisuus myös Windows-sovellusjakeluihin



Modern MAM

www.wpninjas.fi

- Voit liittää puhelimen tai siis sovellukset hallintaan useampaan tenanttiin

Coming Soon...

Multi Account MAM

Enable multiple
MAM policies,
federate device
compliance state

Managed Browser

Managed and
secured browser
configuration for
Corp Owned &
BYOD devices

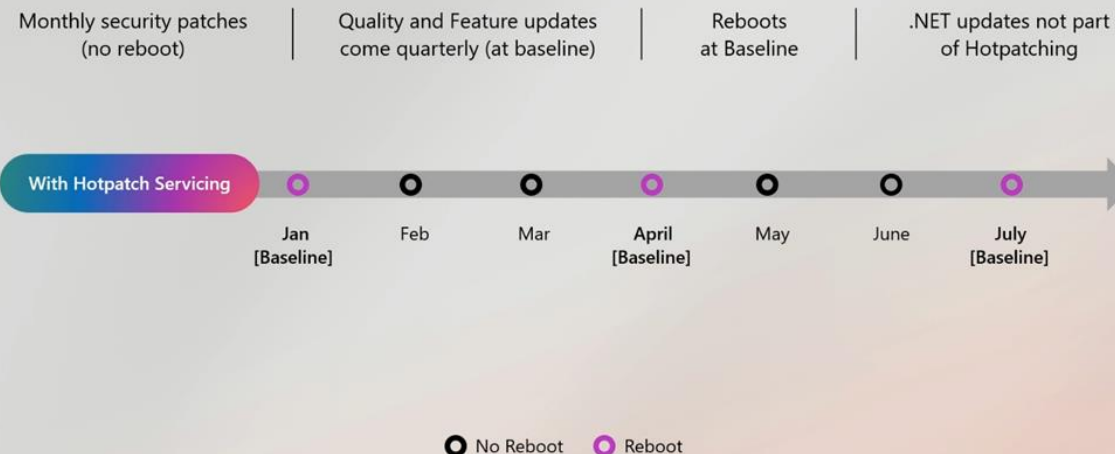


Windows - Hotpatch

www.wpninjas.fi

- Windows 11 24H2
- Neljä kertaa vuodessa tavallinen buuttia vaativa CU
 - Tammikuu/Huhtikuu/Heinäkuu/Lokakuu
- Seuraava 2 kuukautta hotpatch-päivitys
- Vaatimukset
 - Windows Enterprise E3/E5, A3/A5, F3 tai Windows 365 Enterprise
 - Windows 11 24H2 (26100.2033 tai uudempi)
 - Intune
- Ei koske
 - Ajuripäivityksiä
 - .NET Framework-päivitykset

How it works



1 Settings 2 Review + save

Define the quality update policy settings below. Devices assigned to this policy must meet prerequisites. [prerequisites.](#)

Automatic update deployment settings *

Apply the latest cumulative quality updates for security ☐ Allow

When available, apply without restarting the device ("hotpatch"). ☒ Allow

[Learn more about updating without restarts.](#)



- **Turvallisempi Recall**

- <https://blogs.windows.com/windows-insider/2024/11/22/previewing-recall-with-click-to-do-on-copilot-pcs-with-windows-insiders-in-the-dev-channel/>
 - Windows Insider Program
 - Copilot+PC:eille
- Oletuksena pois päältä!
- Vaatimukset Bitlocker/Secure Boot/Windows Hello
- Recall:n käyttö vaatii Hello todennuksen
- Myös Personal Data Encryption vaatii vahvan Hello-todennuksen
- Windows Search with AI tulossa

<https://blogs.windows.com/windows-insider/2024/11/22/previewing-recall-with-click-to-do-on-copilot-pcs-with-windows-insiders-in-the-dev-channel/>



Windows - Security

www.wpninjas.fi

The close Microsoft collaboration with MVI partners also includes working on new Windows platform capabilities to enable running anti-virus processing outside kernel mode. This will enable anti-virus products on Windows to provide a high level of security while minimizing reliability risks, as crashes outside kernel mode will only affect the anti-virus application, and not all of Windows. A private preview of these new Windows security platform capabilities will be made available to partners in July 2025.

<https://blogs.windows.com/windowsexperience/2024/11/19/microsoft-ignite-2024-embracing-the-future-of-windows-at-work/>
<https://learn.microsoft.com/en-us/windows/security/book/>



Windows - Quick Machine Recovery

www.wpninjas.fi

Empowering IT administrators with great tools during critical times is a top priority. Our first step is born out of the learnings from the July incident with the announcement of **Quick Machine Recovery**. This feature will enable IT administrators to execute targeted fixes from Windows Update on PCs, even when machines are unable to boot, without needing physical access to the PC. This remote recovery will unblock your employees from broad issues much faster than what has been possible in the past. Quick Machine Recovery will be available to the Windows Insider Program community in early 2025.

<https://blogs.windows.com/windowsexperience/2024/11/19/microsoft-ignite-2024-embracing-the-future-of-windows-at-work/>



Windows - Security

www.wpninjas.fi

Administrator protection is a new solution that will have the security of Standard user permissions by default, where users can still easily make Windows system changes when needed. With administrator protection, if a system change requires admin rights, the user is prompted to securely authorize the change using Windows Hello. Once authorized, Windows creates a temporary isolated admin token to get the job done. This temporary token is immediately destroyed once the job is complete. This means admin privileges do not persist. Administrator protection is new to Windows and in preview.

Tauko klo 09.55 - 10.05



Kuinka PAW tehdään kunnollisesti - myös cloud-only ympäristössä

Sami Laiho, Adminize

WPNinja ja Microsoft MVP – Windows and Security



Ask The Ninjas!

Kaikki





Kiitos

