



Workplace Ninja
User Group Finland



Windows työasemien tietoturva ja
kovennukset 31.10.2025

Tietoturvasta ei voi puhua liikaa,
varsinkaan nyt!
Katso Sami Laihon esitys





Sisältö

www.wpninjas.fi

- **Käyttäjien tekemät virheet**
- **Ylläpidon tekemät virheet**
- **Admin väliaikaisesti - työkalut**
- **Security Baseline & Firewall vinkit**
- **The End**



Käyttäjien virheet (Zero Trust)

www.wpninjas.fi



Kotona

- Yrityksen fyysinen palomuuri ei ole käytössä
- Työt tehdään ilman VPN yhteyttä
- Kuitu liittymän kaapeli suoraan koneeseen
- Lapset konffaa reitittimen pelejä varten (siltaa)

Operaattori

- 4G/5G yhteys puhelimesta ilman NAT
- Reitittimet vanhenee nopeasti

Julkisissa paikoissa

- WIFI ilman salasanaa
- Julkinen WIFI jaetulla salasanalla myös riski

Ylläpidon virheet

- Tietoturvapäivityksiä viivästytetään liikaa
- Käyttäjät ajaa koneitaan admin oikeuksilla





Ratkaisuja väliaikaiseen adminiin

www.wpninjas.fi

LAPS

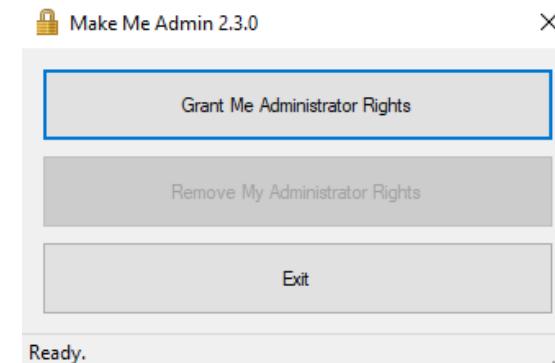
Salasana Intune konsolissa

- Netoxin kumppani
- Myöntää 60min admin oikeudet Company Portaalilin kautta



Make Me Admin

Asennetaan työasemalle
Open Source / Github
10 minuuttia





Intune Endpoint Privilege Management

www.wpninjas.fi

The screenshot shows the Microsoft Intune Endpoint Privilege Management interface. On the left, there's a list of apps with a context menu open for one named 'ccsetup619'. The 'Run with elevated access' option is highlighted with a green oval. Below this, there are sections for 'Elevation type *', 'Validation', and 'Child process behavior', each with dropdown menus or input fields. On the right, a separate window titled 'Endpoint Privilege Management' displays a confirmation dialog: 'Open this app as administrator?'. It shows the app icon for 'ccsetup619.exe', the publisher information ('Verified publisher: PIRIFORM SOFTWARE LIMITED'), and a field labeled 'Enter business justification' with a character count of '0/280'. A note at the bottom states, 'You'll have administrator access to this app.' and includes a link to 'Privacy info'.

- Vain sovellus asennuksiin
- Raportit ja audit

Uutta – käyttäjäprofiilissä evaluointi virtuaalisen sijaan.



Add Temp Admin Rights

www.wpninjas.fi

(Chat GTP + Pavel + Github Copilot)

- Powershell pohjainen
- Käyttää Detection Methodia päälle ja pois
- Lokitus Event Vieweriin
- Piilotettu, ei pääse helposti väliin
- Ei erillistä pop-up promptia, vain CP
- Poistaa myös muulla tavalla lisättyt adminit, mutta vaatii bootin

App details

Version 1.2
Date Published 14/10/2025
Management Service Intune

Application Number of events: 1 456		
Level	Date and Time	Source
Information	13.10.2025 12.02.02	AddTempAdminRights
Information	13.10.2025 11.57.03	VSS
Information	13.10.2025 11.57.00	AddTempAdminRights

Event 1005, AddTempAdminRights	
General	Details
Granted Administrators to AzureAD\{Miramirochnichenko}	
Log Name:	Application
Source:	AddTempAdminRights
Event ID:	1005
Level:	Information
User:	N/A
OpCode:	Info
Logged:	14.10.2025 14.34.33
Task Category:	(1)
Keywords:	Classic
Computer:	LBSCD10760YS



MS Security Baseline vs. CIS

www.wpninjas.fi

Microsoft

- Helppo ottaa käyttöön
- Microsoftin ylläpitämä, seuraa Windows 11 build julkaisuja

Voivat toimia myös yhdessä



CIS

- Tiukempi
- Eri tasoja (TIER)
- Yksityiskohtaisempi, tarkempi
- Takana on yhteisö (Center of Internet Security)
- Päivitykset ja oma versiointi (ei ilmesty yhteen Windows 11 building kanssa)
- Muitakin tuotteita, (Apple, AWS)



Vinkki 1

www.wpninjas.fi

- Windows Firewall Local Policy Merge Off/Disabled = Paikalliset säännöt eivät ole enää voimassa

The screenshot displays a Windows Firewall configuration interface with several windows open:

- Netox1 - Demo Merge OFF (Pauli) on NTXLT0069 - Virtual Machine Connection**: Shows the main navigation menu.
- Console1 - [Console Root\Windows Defender Firewall with Advanced Security on Local Computer\Monitoring\Firewall]**: Shows a tree view of firewall rules under Monitoring > Firewall.
- Console2 - Demo Merge ON (Paavo) on NTXLT0069 - Virtual Machine Connection**: Shows a detailed table of Inbound Firewall Rules.

The detailed table from Console2 is as follows:

Name	Profile	Action	Override	Direction	Program	Local Ad
Core Networking - Destination Unreachable (ICMPv6-In)	All	Allow	No	Inbound	System	Any
Core Networking - Destination Unreachable Fragmentation Nee...	All	Allow	No	Inbound	System	Any
Core Networking - Dynamic Host Configuration Protocol (DHC...	All	Allow	No	Inbound	C:\WINDOWS\system32\svchost.exe	Any
Core Networking - Dynamic Host Configuration Protocol for IPv...	All	Allow	No	Inbound	C:\WINDOWS\system32\svchost.exe	Any
Core Networking - Internet Group Management Protocol (IGMP...	All	Allow	No	Inbound	System	Any
Core Networking - IPv6 (IPv6-In)	All	Allow	No	Inbound	System	Any
Core Networking - Multicast Listener Done (ICMPv6-In)	All	Allow	No	Inbound	System	Any
Core Networking - Multicast Listener Query (ICMPv6-In)	All	Allow	No	Inbound	System	Any
Core Networking - Multicast Listener Report (ICMPv6-In)	All	Allow	No	Inbound	System	Any
Core Networking - Multicast Listener Report v2 (ICMPv6-In)	All	Allow	No	Inbound	System	Any
Core Networking - Neighbour Discovery Advertisement (ICMPv...	All	Allow	No	Inbound	System	Any
Core Networking - Neighbour Discovery Solicitation (ICMPv6-In)	All	Allow	No	Inbound	System	Any
Core Networking - Packet Too Big (ICMPv6-In)	All	Allow	No	Inbound	System	Any
Core Networking - Parameter Problem (ICMPv6-In)	All	Allow	No	Inbound	System	Any
Core Networking - Router Advertisement (ICMPv6-In)	All	Allow	No	Inbound	System	Any
Core Networking - Router Solicitation (ICMPv6-In)	All	Allow	No	Inbound	System	Any
Core Networking - Time Exceeded (ICMPv6-In)	All	Allow	No	Inbound	System	Any
Delivery Optimization (TCP-In)	All	Allow	No	Inbound	C:\WINDOWS\system32\svchost.exe	Any
Delivery Optimization (UDP-In)	All	Allow	No	Inbound	C:\WINDOWS\system32\svchost.exe	Any
Desktop App Web Viewer	All	Allow	No	Inbound	Any	Any
mDNS (UDP-In)	Public	Allow	No	Inbound	C:\WINDOWS\system32\svchost.exe	Any
Microsoft Edge (mDNS-In)	All	Allow	No	Inbound	C:\Program Files (x86)\Microsoft\EdgeWebView...	Any
Microsoft Edge (mDNS-In)	All	Allow	No	Inbound	C:\Program Files (x86)\Microsoft\Edge\Applicati...	Any
Microsoft Media Foundation Network Source IN [TCP 554]	All	Allow	No	Inbound	C:\WINDOWS\system32\svchost.exe	Any
Microsoft Media Foundation Network Source IN [UDP 5004-5009]	All	Allow	No	Inbound	C:\WINDOWS\system32\svchost.exe	Any
Microsoft Office Outlook	Public	Allow	No	Inbound	C:\Program Files\Microsoft\Office\root\Office16...	Any
Microsoft Store	All	Allow	No	Inbound	Any	Any
Microsoft Teams	All	Allow	No	Inbound	C:\Program Files\WindowsApps\MSTeams_2524...	Any
Microsoft Teams	All	Allow	No	Inbound	C:\Program Files\WindowsApps\MSTeams_2524...	Any
Microsoft Teams	All	Allow	No	Inbound	Any	Any
WFD ASP Coordination Protocol (UDP-In)	All	Allow	No	Inbound	C:\WINDOWS\system32\svchost.exe	Any
Wireless Display Infrastructure Back Channel (TCP-In)	All	Allow	No	Inbound	C:\WINDOWS\system32\CastSrv.exe	Any



Merge or not Merge

www.wpninjas.fi

Merge On

- Vähemmän tietoturvaa
- Sovellukset tekee omia sääntöjä asennuksen yhteydessä

Merge OFF

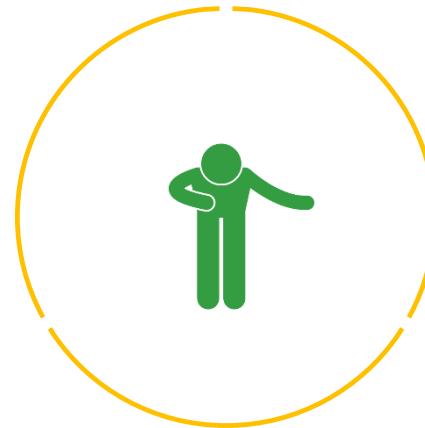
- FW rule kontrolli sinulla
- Tietoturvallisempi



Vinkki 2

www.wpninjas.fi

- Firewall sääntöihin Protokolla on määriteltävä!
- (help-teksti virheellinen)



Kiitos

