



# Windows työasemien tietoturva ja kovennukset 31.10.2025

# Tietoturvasta ei voi puhua liikaa, varsinkaan nyt!

Katso Sami Laihon esitys





# Sisältö

[www.wpninjas.fi](http://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](http://www.wpninjas.fi)



## Kotona

- Yrityksen fyysinen palomuuuri 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](http://www.wpninjas.fi)

## LAPS

Salasana Intune konsolissa



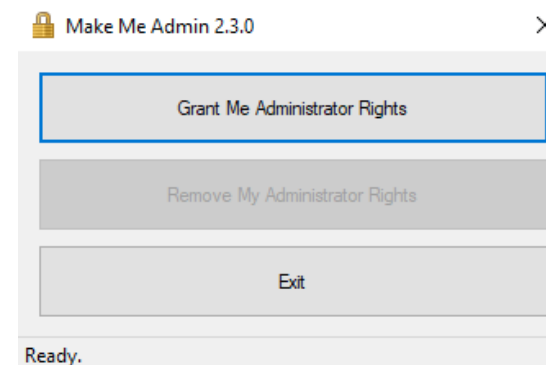
- Netoxin kumppani
- Myöntää 60min admin oikeudet Company Portaalin kautta

## Make Me Admin

Asennetaan työasemalle

Open Source / Github

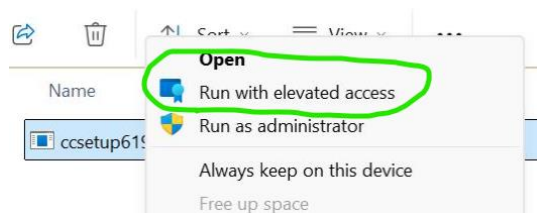
10 minuuttia





# Intune Endpoint Privilege Management

www.wpninjas.fi



Elevation type \*

Validation

Business justification

Child process behavior

User confirmed

User confirmed

Automatic

Deny

Support approved

Elevate as current user



Open this app as administrator?



Enter business justification

0/280

You'll have administrator access to this app.

This information will be sent to your organization's IT admin. [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 lisätyt adminit, mutta vaatii bootin



Add Temp Admin Rights for 5 minutes

LABS

Install ...

Installing this version of Add Temp Admin Rights for 5 minutes will replace other versions of Add Temp Admin Rights for 5

App details

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

Description

Install this app and as soon as Company Portal notifies this has been successfully installed, you have 5 minute of admin time. You can re-run the installation if you need more time and you will have again another 5 minute.

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	
<div>Granted Administrators to AzureAD\MiraMirochnitchenko</div>			
Log Name:	Application	Logged:	14.10.2025 14.34.33
Source:	AddTempAdminRights	Task Category:	(1)
Event ID:	1005	Keywords:	Classic
Level:	Information	Computer:	LBSCD10760YS
User:	N/A		
OpCode:	Info		





# MS Security Baseline vs. CIS

[www.wpninjas.fi](http://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

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

Netox1 - Demo Merge OFF (Pauli) on NTXL0069 - Virtual Machine Connection

File Action Media Clipboard View Help

Console1 - [Console Root\Windows Defender Firewall with Advanced Security on Local Computer\Monitoring\Firewall]

File Action View Favourites Window Help

Console Root

- Windows Defender Firewall with Advanced Security
  - Inbound Rules
  - Outbound Rules
  - Connection Security Rules
  - Monitoring
    - Firewall
  - Connection Security Rules
  - Security Associations

Name	
LABS RDP mstsc	All
LABS RDP Shadow	All
LABS RDP svchost tcp	All
LABS RDP svchost udp	All

Netox2 - Demo Merge ON (Paavo) on NTXL0069 - Virtual Machine Connection

File Action Media Clipboard View Help

Console1 - [Console Root\Windows Defender Firewall with Advanced Security on Local Computer\Monitoring\Firewall]

File Action View Favourites Window Help

Console Root

- Windows Defender Firewall with Advanced Security
  - Inbound Rules
  - Outbound Rules
  - Connection Security Rules
  - Monitoring
    - Firewall
  - Connection Security Rules
  - Security Associations

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](http://www.wpninjas.fi)

## Merge On

- Vähemmän tietoturvaa
- Sovellukset tekee omia sääntöjä asennuksen yhteydessä

## Merge OFF

FW rule kontrolli sinulla  
Tietoturvalisempi



# Vinkki 2

---

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



**Kiitos**

