



Sami Laiho  
Senior Technical  
Fellow, MVP

# Tietoturva Nyt ja Tulevaisuudessa!

# Sami Laiho

Senior Technical Fellow  
adminize.com

- IT Admin since 1996
- MVP in Windows OS since 2011
- **”100 Most Influencial people in IT in Finland” – TiVi’2019→**
- Specializes in and trains:
  - Troubleshooting
  - Security, Social Engineering, Auditing
- Trophies:
  - **Ignite 2018 – Best Session and #2 (out of 1708) !**
  - Best speaker at Advanced Threat Summit 2020, Poland
  - Best Speaker at NIC, Oslo 2016, 2017, 2019 and 2020
  - Best Session at AppManagEvent 2017, 2018, Utrecht
  - TechEd Europe and North America 2014 - Best session, Best speaker
  - TechEd Australia 2013 - Best session, Best speaker



# Ukrainan tilanne...

← Thread

 Sami Laiho  
@samilaiho

...

Через поточний стан кібербезпеки, та для захисту КОРПОРАТИВНИХ мереж в Україні я вирішив опублікувати прості та безкоштовні інструкції щодо захисту середовищ Windows від зловмисників. Прочитайте весь тред і, якщо вважаєте його корисним, зробіть ретвіт! #StandWithUkraine

[Translate Tweet](#)

2:43 PM · Mar 2, 2022 · TweetDeck

[View Tweet activity](#)

75 Retweets 4 Quote Tweets 167 Likes

blog.win-fu.com | Upda  
Readi

Kunnia Ukrainalle

Muuttuneen kyberturvallisuustilanteen johdosta, maanpuolustushengessä, päätin julkista mahdollisimman yksinkertaiset ohjeet Windows-ympäristön puolustamiseen, ulkoista hyökkääjää vastaan. LUE KOKO KETJU, ja jos koet, että tästä on hyötyä → Retweet!

For all my English followers, normally I would tweet in English but this is a matter of protecting my own country. I'll translate ASAP, until → Google.

Voisin ohjeistaa, että teidän pitää ottaa pois admin-oikat, asentaa AppLocker jne. mutta tosiasi on, että näitä ei tehdä päivässä, eikä kahdessa. Joten seuraavassa nopeat ohjeet, joilla on oikeasti merkitystä ja välitön teho, kyberhyökkäyksiä vastaan.

Tietoturva on lopulta yksinkertaista. Kyse on enemmän oikeista toimintatavoista, konsepteista, kuin kalliista tuotteista. Seuraavassa käyn läpi, mitä tekisiin, jos olisin sotatilanteessa ja suojaus pitäisi saada äkkiä nostettua potensiili kaksi, irroittamatta verkkoa Internetistä.

Ohjeet on tehty estämään kokonaisen ympäristön menetys. Pari sotilasta voidaan tässä menettää, mutta estetään vierasta tahoa valtaamasta koko firmaa. Yritykset eivät joudu uutisiin, koska heidän käyttäjä saa ransomwaren, vaan siksi, että koko yrityksen toiminta voidaan lamauttaa.

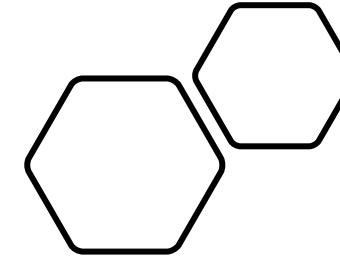
Ohjeet ovat yksinkertaisia, jotka auttavat kaikkia yrityksiä, joilla on hakemistopalvelu(AD/AAD). Näistä saadaan paremmat, jos yhdessä tehdään, juuri teille - Nyt kuitenkin on tarkoitus tehdä ohjeita, jotka sopivat kaikille.

Aina voi parantaa, mutta muistakaan, että tietoturvassa ei saa antaa täydellisen olla hyvän vihollinen. Nyt pitää TEHDÄ näitä asioita, jotta maan yritykset pysyvät turvassa! Ei ole aikaa siihen, että "Tämä ei ole 100% turvallinen" tai "Tämä vuotaan kuitenkin".

Nyt parannetaan olemassa olevaa. Tehdään täydellisempää siten kun perussuojaus on kytketty!

1. Tier0-suojaus. Jokaisen hyökkäyksen graalin malja on Domain Admin -tunnus. Jotta sitä ei voi varastaa, sen käyttö estetään siellä missä sitä ei tarvita. Osoita seuraava policy kaikille koneille, paitsi DC-koneille.

Tietoturva on  
lopulta aika  
yksinkertaista



A close-up photograph of a person's hand holding a small, glowing blue device, likely a smartphone or a key fob. The device is held vertically, with its screen facing towards the viewer. The background is dark and out of focus, creating a dramatic effect with the bright glow of the device.

“You don’t have to make your security perfect, just better than your neighbour’s”

Mikko Hyppönen



# Windows vs Android PC vs Mobile

---



# FluBot

-  **+358 44 272 5795** Sunday >  
Jos h aluat lopettaa viesti en vastaanotta misen, poistu tasta: [www.keepkoop.com...](http://www.keepkoop.com...)
-  **+358 40 505 9843** Saturday >  
Uusi aa niviesti rakkaaltasi [electronicer.tech/elp/?m6nxb-yd2fCW0o...](http://electronicer.tech/elp/?m6nxb-yd2fCW0o...)
-  **+358 40 375 4165** Friday >  
Uusi aa an iviesti: [socialpsyche.com/rlr/?Fj0c494oK3ar-M4tR27w](http://socialpsyche.com/rlr/?Fj0c494oK3ar-M4tR27w)
-  **+358 40 186 6638** Thursday >  
A&D on lahettynt sinu lle vie s t in. Lu e ja va staa: [tradeshow.zone/c-d-u/?A1S...](http://tradeshow.zone/c-d-u/?A1S...)
-  **+358 44 555 9163** Thursday >  
Sinulle on po s tia [naifd.org/nuc/?4gofhhg0q56qj257](http://naifd.org/nuc/?4gofhhg0q56qj257)

# Sisältö

- Älä näytä “osaamattomalta”
- Rajoita kovimpien tunnusten käyttöä radikaalisti
- Estää tunnusten, joilla ympäristöä voi vahingoittaa eniten, käyttö muualta, kuin missä niille on tarve
- Estää hallintaohjelmien yms. ajaminen niiltä koneilta joilta pääsee Facebookiin
- Estää koneita puhumasta järjestelmille, jos ei ole tarvetta
- Estää pelkkien salasanojen käyttö
- Salaa kaikkien koneiden levyt
- Älä anna käyttäjille admin-oikeuksia
- Tärkeimmät tietoturvakontrollit ovat: Ajantasalla olevat rauta- ja softainventaario
- Perusta/ulkoista SoC



# Ulkoinen evaluointi

# Company Branding

Älä näytä amatööriltä



# Global Adminien minimointi

---

3 on monelle liikaa, 1 aina liian  
vähän



# Delegoi

Home > Users > Sami Laiho

## Sami Laiho | Assigned roles

User

Diagnose and solve problems

Manage

- Profile
- Custom security attributes (preview)
- Assigned roles**
- Administrative units

Add assignments Remove assignments Refresh Got feedback?

Administrative roles

Administrative roles can be used to grant access to Azure AD and other Microsoft services. [Learn more](#)

Search by name or description Add filters

Role	Description	Resource Name	Resource Type
<input type="checkbox"/> Billing administrator	Can perform common billing related tasks.	Directory	Organization



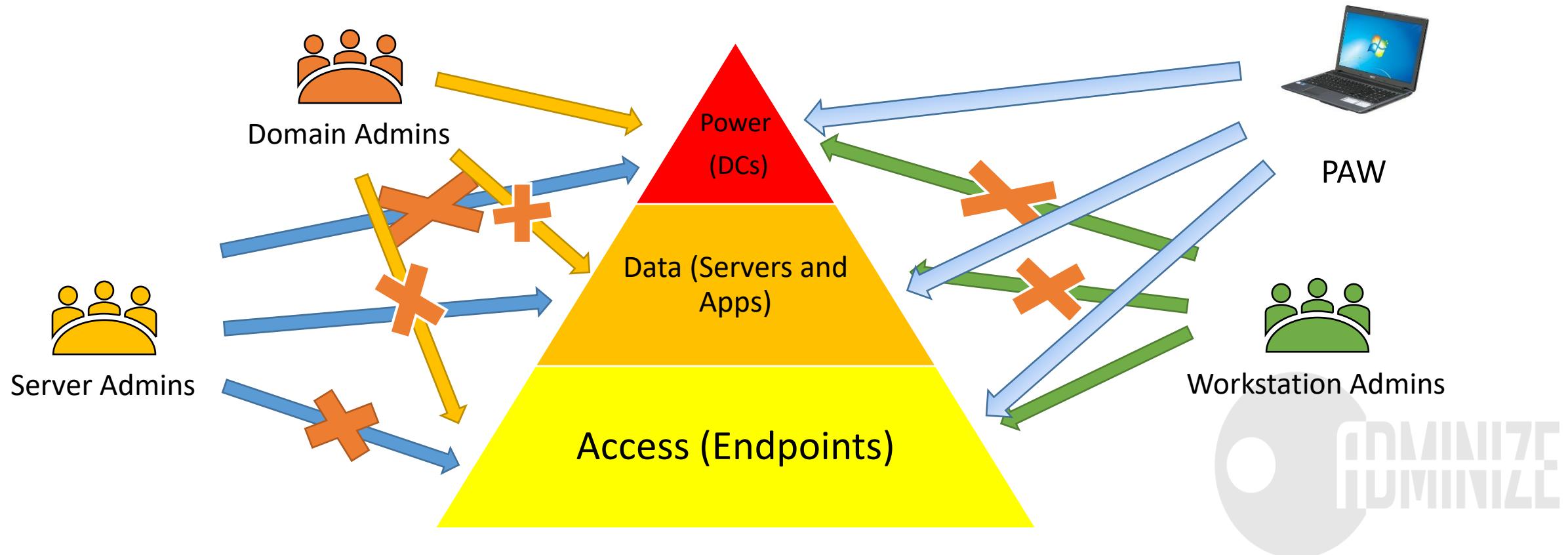
ADMINIZE

# Tier-malli & PAW

Estä vaarallisten käyttäjien käyttö,  
tarpeettomissa paikoissa

# AD:n kerrostaminen (AD Tiering)

- Ympäristö jaetaan osiin, jotta kaikkea ei menetetä, jos tuulettimeen osuu
- Ylemmän tason ylläpitäjät eivät voi kirjautua alempille tasolle



# Jos ei muuta, niin ainakin tämä!

The screenshot illustrates the configuration of a Group Policy Object (GPO) named "Tier0\_Protection" in the "concept.local" domain. The GPO is linked to the "Computers" container under the "Accounts" section of the "concept.local" domain in the Group Policy Management interface. In the Group Policy Management Editor, the "Computer Configuration" section is selected, showing various policy settings. One specific setting, "Deny access to this computer from the network," is highlighted and assigned to the "CONCEPT\Domain Admins" security group. This setting is part of the "Security Settings" section under "Local Policies".

**Group Policy Management**

- Forest: concept.local
- Domains
- concept.local
  - cu\_Custom\_Default\_Domain\_Policy
  - Default Domain Policy
  - Accounts
    - Computers
      - c\_AppLocker\_Hardening
      - Tier0\_Protection
      - PAWs
      - Servers
      - Workstations

**Computers**

Link Order	GPO	Enforced	Link Enabled	GPO Status	W
1	c_AppLocker_Hard...	No	Yes	Enabled	No
2	Tier0_Protection	No	Yes	Enabled	No

**Group Policy Management Editor**

Tier0\_Protection [CONDC1.CONCEPT.LOCAL] Policy

- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment

Policy	Policy Setting
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	CONCEPT\Domain Admins
Deny log on as a batch job	CONCEPT\Domain Admins
Deny log on as a service	CONCEPT\Domain Admins
Deny log on locally	CONCEPT\Domain Admins
Deny log on through Remote Desktop Services	CONCEPT\Domain Admins
Enable computer and user accounts to be trusted for delega...	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined

Group Policy Management Editor

File Action View Help

Tier0\_Protection [CONDC1.CONCEPT.LOCAL]

Computer Configuration

- Policies
  - Software Settings
  - Windows Settings
    - Name Resolution Policy
    - Scripts (Startup/Shutdown)
  - Security Settings
    - Account Policies
    - Local Policies
    - Event Log
    - Restricted Groups**
    - System Services
    - Registry
    - File System
    - Wired Network (IEEE 802.11)
    - Windows Defender Firewall
    - Network List Manager Policies
    - Wireless Network (IEEE 802.11)
    - Public Key Policies
    - Software Restriction Policies

Group Name: CONCEPT\G\_ComputerAdmins

Group Name	Members	Member Of
CONCEPT\G_ComputerAdmins	Administrators	

CONCEPT\G\_ComputerAdmins Properties

Configure Membership for CONCEPT\G\_ComputerAdmins

Members of this group:

<This group should contain no members>

Add... Remove

This group is a member of:

Administrators

Add... Remove

ADMINIZE

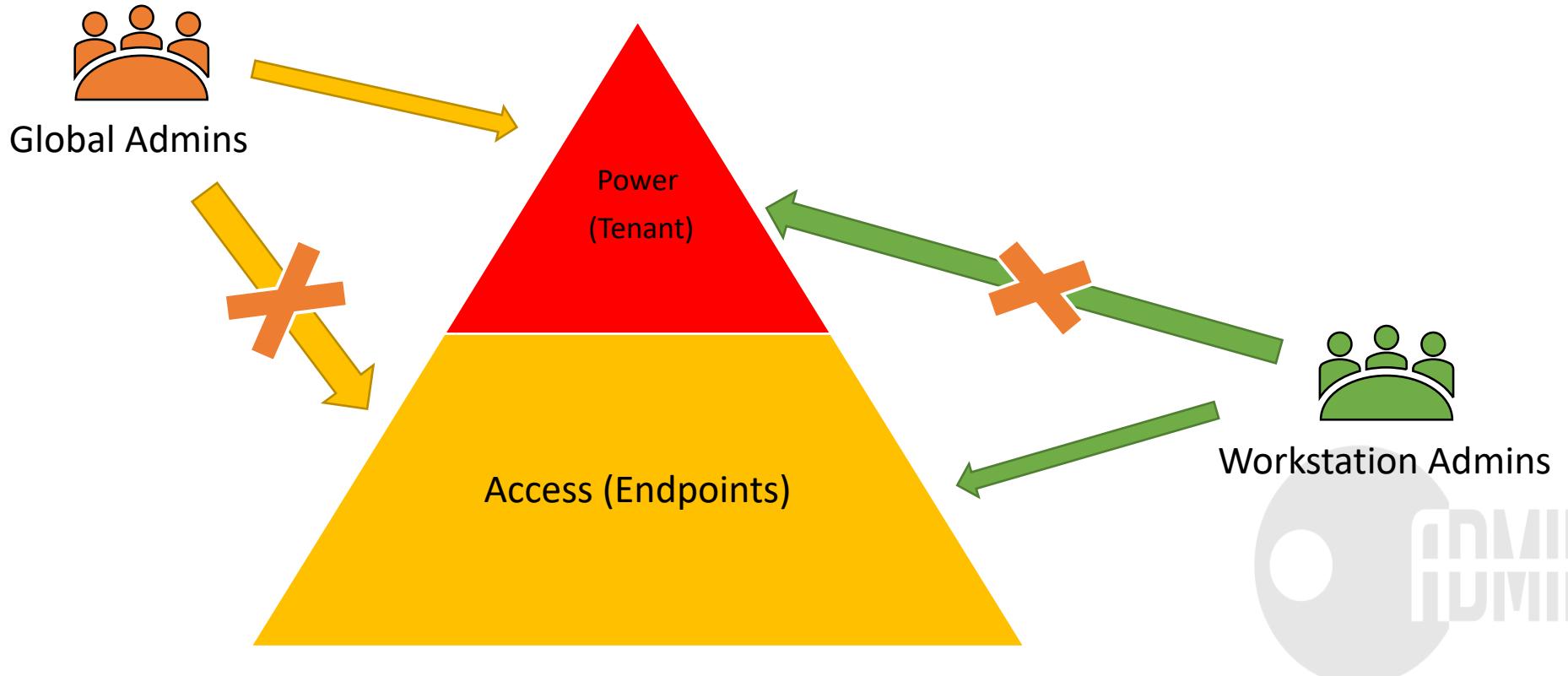


# Pilvessä?

cloud

# ADD Tiering (Native Cloud)

- Ympäristö jaetaan osiin, jotta kaikkea ei menetetä, jos tuulettimeen osuu
- Ylemmän tason ylläpitäjät eivät voi kirjautua alempille tasolle



# Käyttäjien esto pääsemästä AAD-portaaliin

The screenshot shows the 'User settings' page for 'Matti Laiho Oy | User settings' in Azure Active Directory. The left sidebar lists various administrative options: External identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Custom security attributes (Preview), Licenses, and Azure AD Connect. The main content area has three sections: 'Enterprise applications' (Manage how end users launch and view their applications), 'App registrations' (Users can register applications with Yes or No buttons), and 'Administration portal' (Restrict access to Azure AD administration portal with Yes or No buttons). A blue arrow points from the bottom towards the 'Administration portal' section.

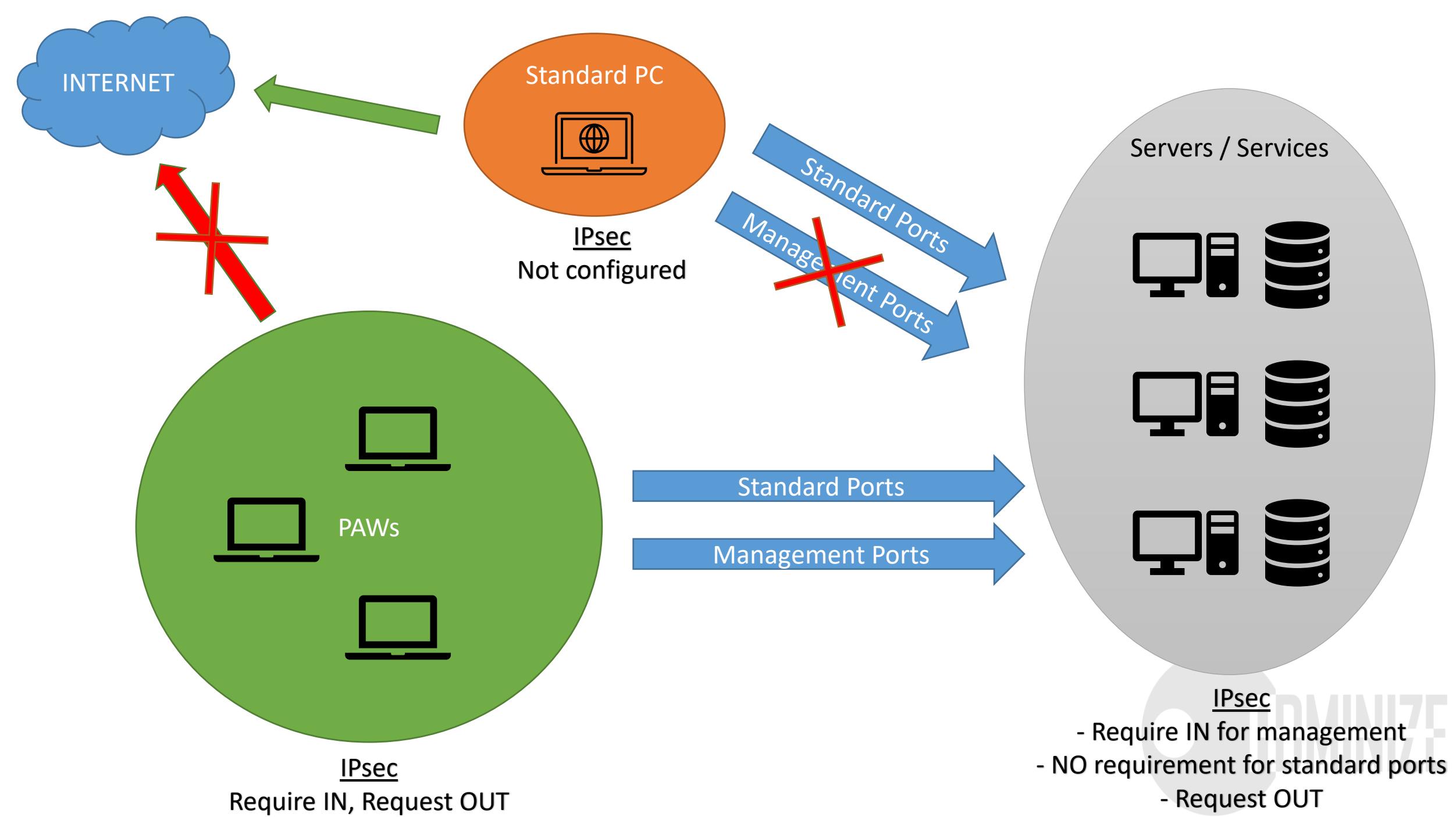


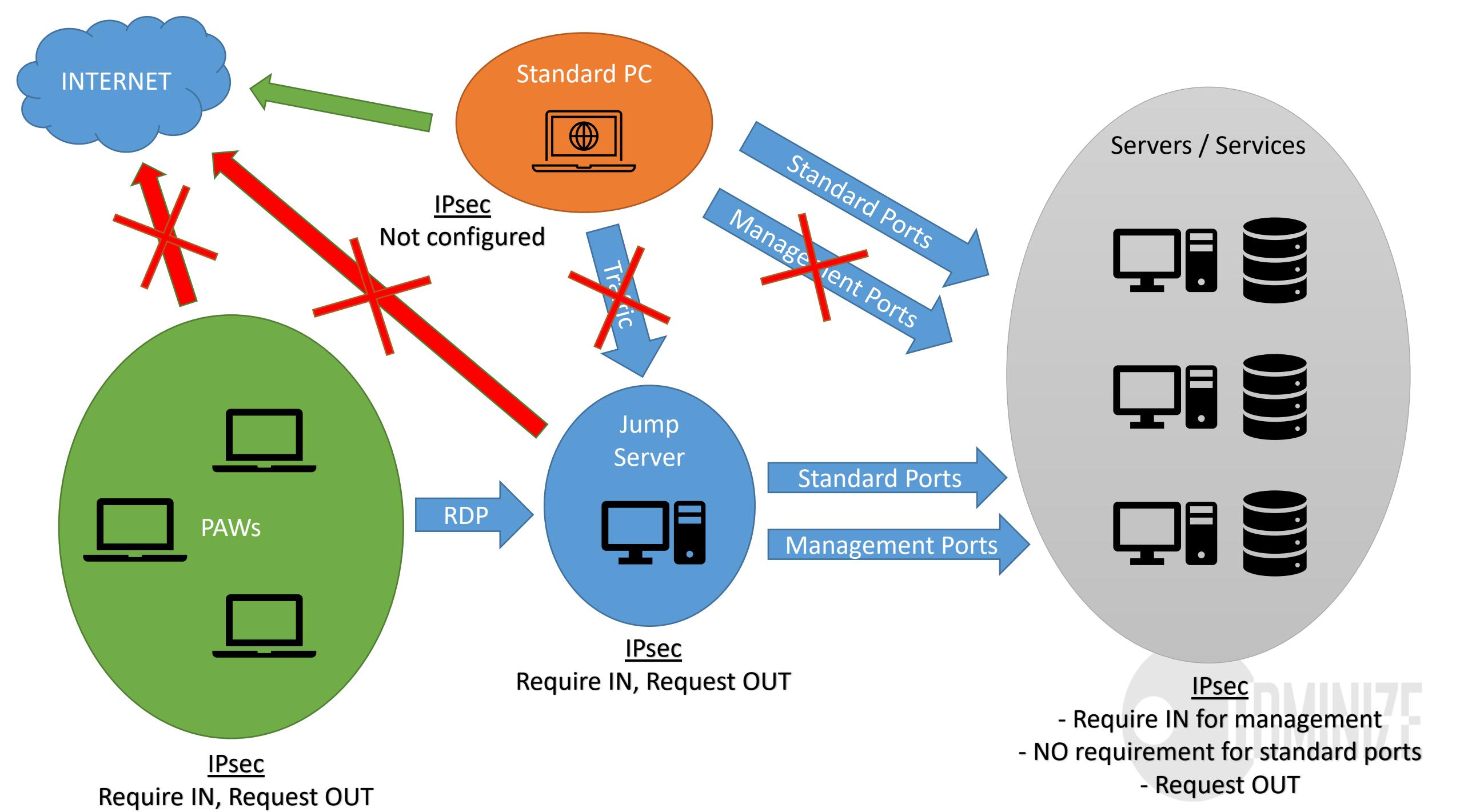
Jos koneelta voi hallita, sieltä  
ei pitäisi voida käyttää  
Facebookia...

Privileged Access Workstation (PAW)

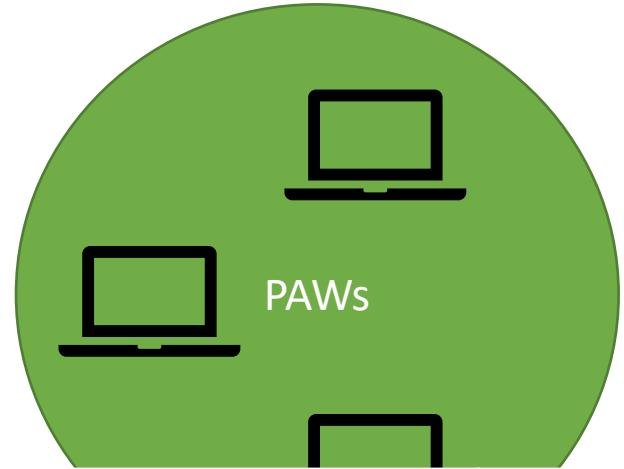
# PAW-työasema

- Vain hallintaan omistettu työasema (virtuaalinen tai fyysinen)
- Hallintatyökalut asennettuna
- Vain IT-osasto pystyy käyttämään
- Kovempi tietoturvataso kuin normaalilla työasemalla
- Ei (vapaata) pääsyä Internetiin
- Ei Office-sovelluksia ym.





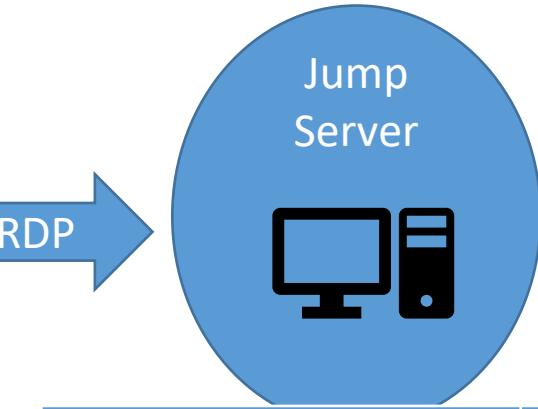
# Administrators- group members



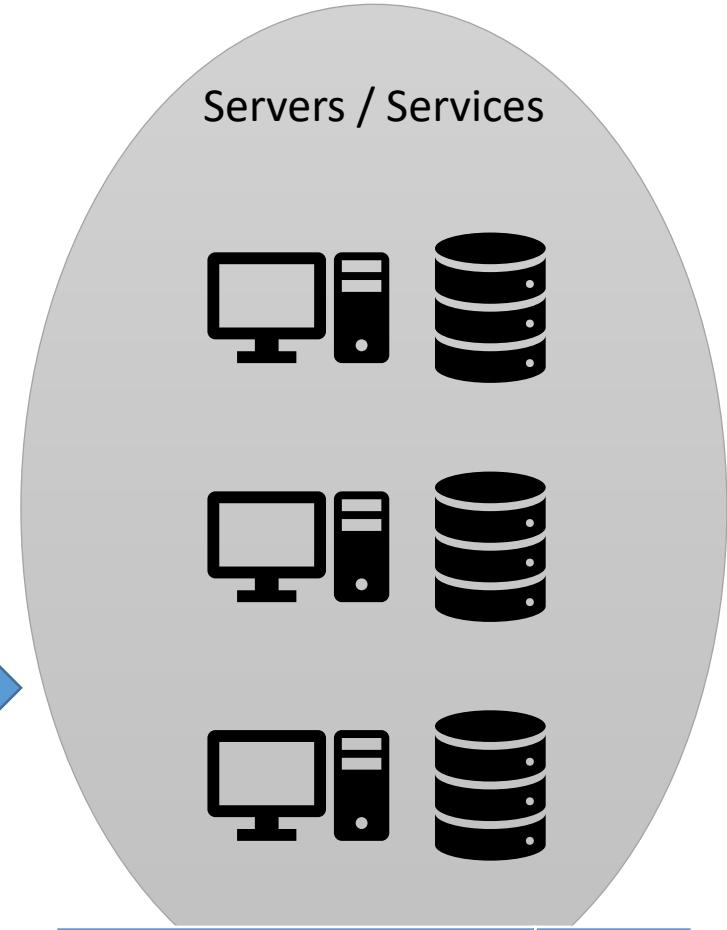
Administrators	
Domain Admins	NO
Workstations Admins	NO
Server Admins	NO
Builtin Administrator (used via LAPS)	YES



Administrators	
Domain Admins	YES
Workstations Admins	YES
Server Admins	NO
Builtin Administrator (used via LAPS)	YES



Administrators	
Domain Admins	NO
Workstations Admins	NO
Server Admins	NO
Builtin Administrator (used via LAPS)	YES

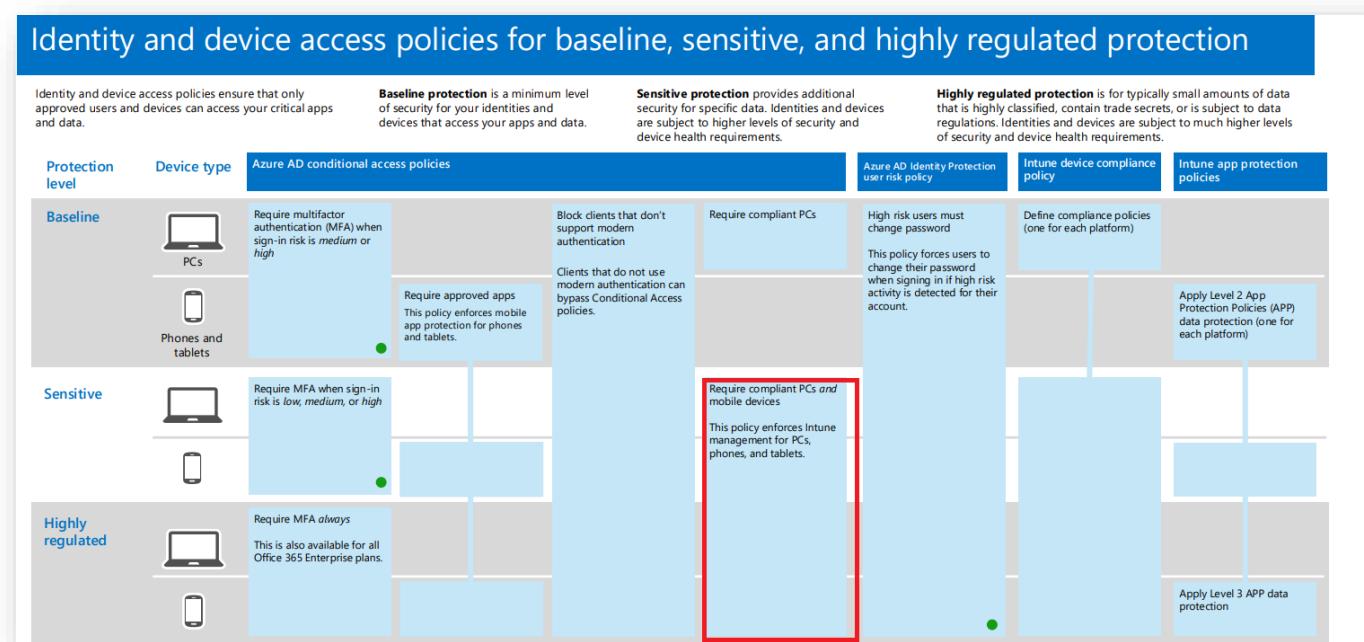


Administrators	
Domain Admins	YES
Workstations Admins	NO
Server Admins	YES
Builtin Administrator (used via LAPS)	YES

RDP

# Native Azure PAW

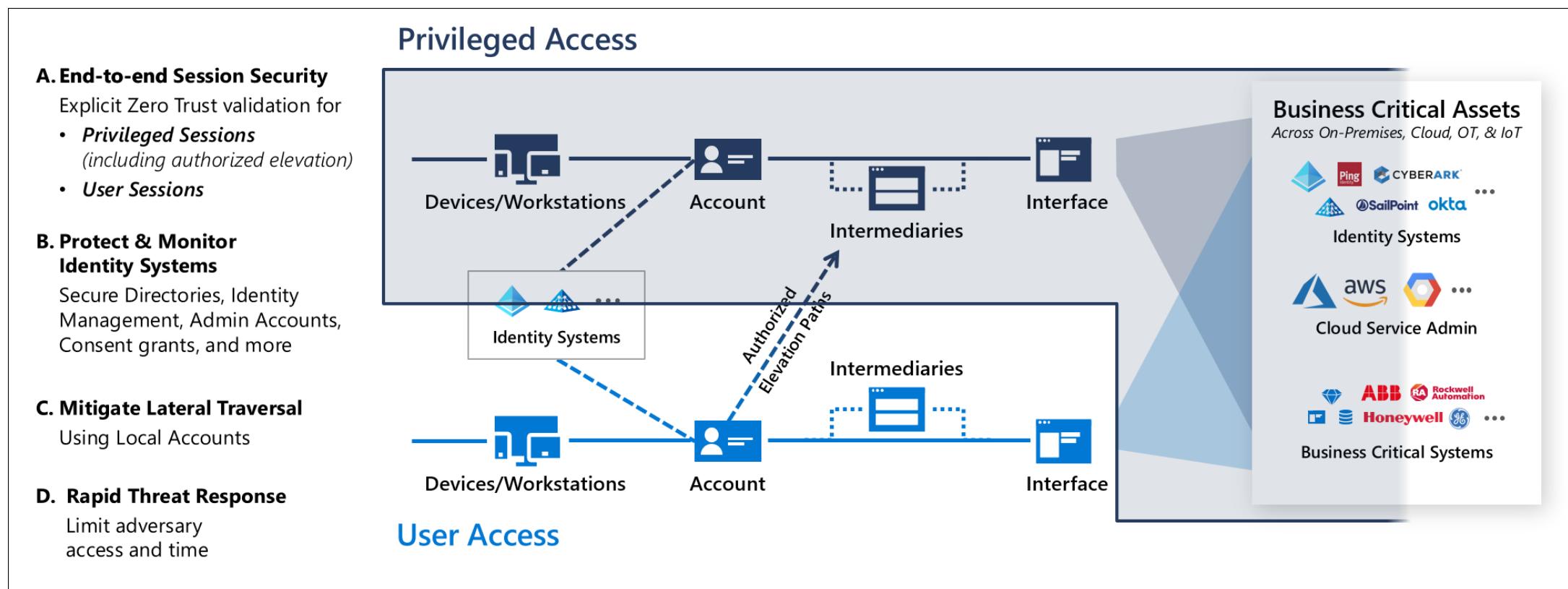
- Loistava ohje, miten tehdään CA:n avulla!
  - <https://call4cloud.nl/2021/11/paw-love-and-thunder/>
- Microsoftin oma: <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-condition-filters-for-devices>



ADMINIZE

# Microsoft RAMP

- <https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan>





Älä käytä pelkkiä  
salasanoja

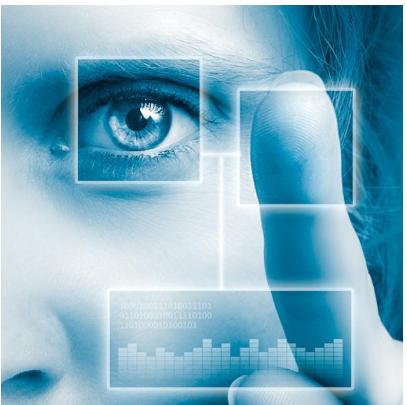


“MFA Everything!”

“If you RDP, you MFA!”

# Biometrics

- Really a game changer
- Great second factor!
  - There are still issues to think about



Smart Cards are difficult, Virtual Smart Cards will be deprecated... So let me introduce the Future of 2FA.....

Name: Token

Token Type: Live, Hedgehog

Token lifetime: 5-8 years

Tamper Protection: Yes





Admin rights

---

Ei admin  
oikkia!

---

Users: “If I don’t have admin rights, I can’t fix my computer”

Reality: “If you don’t have admin rights, you can’t break your computer”



# Estä loppukäyttäjiä vahingoittamasta koneita!

---



Jannik

we had a decrease of 75% of tickets after we implemented no admin rights and acevto.... so price to us is crazy cheap

A screenshot of a social media post. The name 'Jannik' is visible above a blurred black ink smudge. Below the smudge is a text box containing the following message: "we had a decrease of 75% of tickets after we implemented no admin rights and acevto.... so price to us is crazy cheap".

[This Photo by Unknown Author is licensed under CC BY](#)



US Customer: 65% less  
reinstallations



	2020	2019	2018	2017	2016
<b>Number of vulnerabilities</b>	1,268	858	701	685	451
<b>Number of Critical vulnerabilities</b>	196	192	189	235	153
<b>% as Critical</b>	15%	22%	27%	34%	34%
<b>Number of Critical vulnerabilities mitigated</b>	109	147	154	185	142
<b>Number of Critical vulnerabilities mitigated %</b>	56%	77%	81%	79%	93%

# Vaihtoehtoja millä ratkaista

Tarpeen mukaan

- Carillon
  - Hyvä perus Office-käyttäjille

Sääntöpohjainen + On Demand

- PolicyPak
  - Hyvä perus Office-käyttäjille
  - Soveltuu myös sovelluskehittäjille
- BeyondTrust
  - Hyvä perus Office-käyttäjille
  - Soveltuu myös sovelluskehittäjille
  - Paras/kallein



&lt; Home &gt; Endpoint security &gt;

## Create elevation rules policy

Privilege management

✓ Basics 2 Configuration settings

### Elevation rules

Elevation rules provide the ability to complete a managed elevation workflow.

[+ Add](#) [Delete](#)

Name	Action
No rules found.	

## Elevation rule

Elevation rules policy

### Basics

Name \*

Asset Tracking Management System

Description

Application used to track assets

### Elevation behaviors

Rule type \*

Select one

Automatic

Self elevation

Support arbitrated

Applicability \*

File path \* ⓘ

### Import reference file

Upload a file containing desired metadata. You can edit after importing the content.

Upload ⓘ

Select a file

### File properties

# Endpoint security | Privilege management

Search (Ctrl+ /)



Summary

New requests

Elevation history



Last refreshed on 4/5/2022, 8:00:00 AM

## Elevations in last 7 days

Matches rule

0

Not in rule

316

[View report](#)

## Elevation policies

Create policy



Refresh



Export



Search



i

Add filter

Policy ↑

Type ↑

Retail Manager Elevat...

Elevation rules

Contoso Elevation Co...

Client settings

## Privilege management

Do you want to continue as administrator?



Asset Tracking Management System

Verified publisher: Contoso Corporation

### Enter justification

Launching this application to update inventory

### Verify your username and password

Email address



Password

### Contact support



Contoso Corporation

315-555-1212

[support@contoso.com](mailto:support@contoso.com)

[Support website](#)

Yes

No

TECH CONFERENCE



Kaikki koneet salataan!

BitLocker

# Miksi BitLocker tarvitaan kaikilla koneilla?

Se varmistaa laitteen eheyden

Koska yli 800000 laitetta  
varastetaan/katoaa vuosittain  
lentokentillä

Mahdollistaa turvallisen  
kierrätyksen

### Create profile

\* Name  
BitLocker Policy ✓

Description  
Enter a description... ✓

\* platform  
Windows 10 and later

\* Profile type  
Endpoint protection

Settings  
Configure >

**Create**

### Windows encryption

Windows Settings

Require devices to be encrypted (Desktop only) Enable Not configured

Require Storage Card to be encrypted (mobile only) Enable Not configured

BitLocker base settings

Configure encryption methods

Encryption for operating system drives Enable XTS-AES 128-bit

Encryption for fixed data-drives Enable XTS-AES 128-bit

Encryption for removable data-drives Enable AES-CBC 128-bit

BitLocker OS-drive settings

Require additional authentication at startup

Block BitLocker on devices without a compatible TPM chip Enable Not configured

TPM startup Allow TPM

TPM startup PIN Allow startup PINs with TPM

TPM startup key and PIN Allow startup key and PINs with TPM

Minimum PIN length Enable Not configured

Minimum characters Not configured

Enable OS-drive recovery Enable Not configured

Allow certificate-based data-recovery agent Enable Not configured

User creation of recovery password Allow 48-digit recovery password

User creation of recovery key Allow 256-bit recovery key

Hide recovery options in the BitLocker setup wizard Enable Not configured

Save BitLocker recovery information to AD DS Enable Not configured

Configure storage of BitLocker recovery information to AD DS Backup recovery passwords and key packages

Require recovery information to be stored in AD DS before enabling BitLocker Enable Not configured

Enable pre-boot recovery message and URL Enable Not configured

Pre-boot recovery message Use default recovery message and URLs

BitLocker fixed data-drive settings

Deny write access to fixed data-drive not protected by BitLocker Enable Not configured

Enable fixed drive recovery Enable Not configured

Allow data-recovery agent Enable Not configured

User creation of recovery password Allow 48-digit recovery password

User creation of recovery key Allow 256-bit recovery key

Hide recovery options in the BitLocker setup wizard Enable Not configured

Save BitLocker recovery information to AD DS Enable Not configured

Configure storage of BitLocker recovery information to AD DS Backup recovery passwords and key packages

Require recovery information to be stored in AD DS before enabling BitLocker Enable Not configured

BitLocker removable data-drive settings

Deny write access to removable data-drive not protected by BitLocker Enable Not configured

Block write access to devices configured in another organization Enable Not configured

**OK**





Laitteiden hallinta

Local Group Policy Editor

File Action View Help

Device Installation Restrictions

Prevent installation of devices using drivers that match these device setup classes

Setting State

Setting	State
Allow administrators to override Device Installation Restriction policies	Enabled
Apply layered order of evaluation for Allow and Prevent device installation policies across device setup classes	Not configured
Allow installation of devices using drivers that match these device setup classes	Not configured
<b>Prevent installation of devices using drivers that match these device setup classes</b>	<b>Enabled</b>
Display a custom message when installation is prevented by a policy setting	Enabled
Display a custom message title when device installation is prevented by a policy setting	Enabled
Allow installation of devices that match any of these device IDs	Not configured
Prevent installation of devices that match any of these device IDs	Not configured
Allow installation of devices that match any of these device instance IDs	Not configured
Prevent installation of devices that match any of these device instance IDs	Not configured
Time (in seconds) to force reboot when required for policy changes to take effect	Not configured
Prevent installation of removable devices	Not configured
Prevent installation of devices not described by other policy settings	Not configured

Requirements: At least Windows Vista

Description: This policy setting allows you to specify a list of device setup class globally unique identifiers (GUIDs) for driver packages that Windows is prevented from installing. By default, this policy setting takes precedence over any other policy setting that allows Windows to install a device.

NOTE: To enable the "Allow installation of devices that match any of these device IDs" and "Allow installation of devices that match any of these device instance IDs" policy settings, click the "Extended" tab.

Comment:

Supported on: At least Windows Vista

Options:

Prevent installation of devices using drivers for these device setup classes:

Value
{4d36e967-e325-11ce-bfc1-08002be10318}
*

Show...

To create a list of device classes, click Show. In Show Contents dialog box, in the Value column type a GUID that represents a device setup class (for example, {25DBCE51-6C8F-4A72-8A6D-B54C2B4FC835}).

Also apply to matching devices that are already installed.

A collection of various USB drives of different colors and sizes.

A dialog box titled "BLOCKED DEVICE!" with the message "If you need access to USB driver, contact SD!"

2°C Pilvistä 11.55 ENG 8.3.2022 3



# Valvonta

SIEM & SOC

Microsoft Azure

Home > Azure Sentinel

Search resources, services, and docs

admin@contoso.com  
CONTOSO

### Azure Sentinel - Overview

Last week (1/21/2018-1/27/2018)

**GENERAL**

- Overview
- Logs

**THREAT MANAGEMENT**

- Incidents
- Dashboards
- User analytics
- Hunting
- Notebooks

**CONFIGURATION**

- Getting started
- Data collection
- Analytics
- Playbooks
- Community
- Workspace

**Events** 8.2M 978.4K

**ALERTS** 39 6

**INCIDENTS** 18 4

**INCIDENTS BY STATUS**

- NEW (0)
- IN PROGRESS (4)
- CLOSED (RESOLVED) (4)
- CLOSED (DISMISSED) (3)

**Events and alerts over time**

**Recent incidents**

- User logged in to critical assets (9 Alerts)
- Suspicious process execution after co... (9 Alerts)
- Computers with cleaned event logs (8 Alerts)
- Remote procedure call (RPC) attempts (8 Alerts)

**Potential malicious events**

**MALICIOUS IPS EVENTS** 82K

**OUTBOUND** 4K ▲

**INBOUND** 78K ▼

**Most anomalous data sources**

- Azure AD
- Office
- SecurityEvents

**Democratize ML for your SecOps**

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML.

Learn more >

Function1 System Acct

Messages Settings Activity Help Find

Monitoring Console

Settings Run a Search

Save As Close Last 60 minutes

```
o = if (status == "missing", "N/A", sum_kb) | eval avg_tcp_kbps_sparkline = if == "missing", "N/A", avg_tcp_kbps | eval avg_tcp_eps = if (status == "Heavy Forwarder", forwarder_type == "uf", "Universal Forwarder", ed = strftime(last_connected, "%m/%d/%Y %H:%M:%S %z") | search NOT [! hostname] status=missing | replace * WITH "<hostname-IP>" IN hostname
```

Job Smart Mode

arch	avg_tcp_eps	avg_tcp_kbps	avg_tcp_kbps_sparkline	forwarder_type	guid	hostname	last_connected	os	status	sum_kb	version
x86_64	N/A	N/A	N/A	Universal Forwarder	0B985568-4102-4FAF-982B-C6309499D7C6	<hostname-IP>	09/25/2017 16:03:02 -0400	Linux	missing	N/A	6.5.2
x86_64	N/A	N/A	N/A	Universal Forwarder	156AA180-1AF3-4772-BD04-1DD71312C462	<hostname-IP>	09/25/2017 16:00:12 -0400	Linux	missing	N/A	6.5.2
x64	N/A	N/A	N/A	Universal Forwarder	36041654-7EC1-45AA-A5D1-5CEC67339FE0	<hostname-IP>	10/05/2017 05:16:56 -0400	Windows	missing	N/A	6.4.8
x86_64	N/A	N/A	N/A	Universal Forwarder	3E47DAE9-9220-4260-A730-A15C8797668E	<hostname-IP>	09/25/2017 15:59:41 -0400	Linux	missing	N/A	6.5.2
x64	N/A	N/A	N/A	Universal Forwarder	529042BB-1D51-481C-9300-B35C67F55DF8	<hostname-IP>	10/09/2017 05:16:39 -0400	Windows	missing	N/A	6.5.0
x64	N/A	N/A	N/A	Universal Forwarder	58F0F461-0D4D-4BC9-8C8C-47957CE8DED1	<hostname-IP>	09/26/2017 03:07:44 -0400	Windows	missing	N/A	6.5.2
x86_64	N/A	N/A	N/A	Universal Forwarder	69A60123-7714-4BA9-B193-C20598EF8BFD	<hostname-IP>	09/25/2017 16:03:16 -0400	Linux	missing	N/A	6.5.2
x86_64	N/A	N/A	N/A	Universal Forwarder	6CA0E7FE-BE4F-4479-AF48-1ADD1F94F036	<hostname-IP>	09/25/2017 16:00:58 -0400	Linux	missing	N/A	6.5.2



This Photo by Unknown Author is licensed under [CC BY-SA NC](https://creativecommons.org/licenses/by-sa/4.0/)

---

“In Security don’t  
let perfect be the  
enemy of good”

---

# Contact

- [sami@adminize.com](mailto:sami@adminize.com)
- Twitter: @samilaiho
- Blog: <http://blog.win-fu.com/>
- Free newsletter:  
<http://eepurl.com/F-GOj>
- My trainings:
  - <https://win-fu.com/events>
  - <https://win-fu.com/dojo/>
    - **Free for one month!!**
    - **Code:"Trial2018"**
- PluralSight: If you need a code email me!



Järjestelmävalvoja