

6.1. service account and sysinternals

Sunday, November 2, 2025 13:22

Tämä on harjutus demo , koskien mitä videossa menekään ja harjoitus jatkuu - **Windows Server Homelab: Implementing Service Accounts| Single Purpose Computers (Ep 6)**

"Implementing service account" tarkoittaa palvelutilin käyttöönottoa, ja "Sysinternals" viittaa Microsoftin työkalupakettiin Windows-järjestelmien hallintaan.

⌚ Implementing Service Account (Palvelutilin käyttöönotto)

Palvelutili on erityinen käyttäjätili, jota käytetään ohjelmien, palveluiden tai automaattisten prosessien suorittamiseen – ei ihmisten kirjautumiseen.

Tarkoitus ja käyttö:

- Palvelutili tarjoaa *turvallisen käyttöympäristön* palveluille ja sovelluksille.
- Se voi olla *paikallinen* tai *verkkotunnukseen liitetty* (domain account).
- Käytetään esimerkiksi SQL Serverin, IIS:n tai varmuuskopiointiohjelmistojen taustapalveluihin.

Tyypit Windowsissa:

- *Standalone Managed Service Account (sMSA)* – yksittäiselle palvelimelle.
- *Group Managed Service Account (gMSA)* – useille palvelimille ja automaattinen salasanan hallinta.
- *Virtual Account* – automaattisesti luotu, ei vaadi salasanaa.

Hyviä käytäntöjä:

- Käytä *vähimmän oikeuden periaatetta* (least privilege).
- Dokumentoi, missä palvelutiliä käytetään.
- Vaihda salasanat säännöllisesti tai käytä automaattista hallintaa.

📋 Sysinternals

Sysinternals on Microsoftin tarjoama kokoelma edistyneitä työkaluja Windowsin hallintaan ja vianmääritykseen.

Tunnetuimpia työkaluja:

- **Process Explorer** – tarkempi versio Tehtävienhallinnasta.
- **Autoruns** – näyttää kaikki automaattisesti käynnistetyt ohjelmat.
- **PsExec** – mahdollistaa komentojen suorittamisen etäkoneella.
- **ProcMon (Process Monitor)** – seuraa tiedosto-, rekisteri- ja prosessitoimintoja reaalialajassa.

Käyttötarkoitus:

- Diagnosoi suorituskykyongelmia.
- Selvitä haittaohjelmien toimintaa.
- Hallitse järjestelmän prosesseja ja palveluita.

Yhdessä palvelutilien kanssa: Sysinternals-työkaluja voidaan käyttää palvelutilien konfigurointiin, valvontaan ja vianmääritykseen – esimerkiksi tarkistamaan, mitä resurssia palvelutili käyttää tai miten se toimii tietystä ympäristössä.

Objektives:

- Gain practical experiences with AD service accounts
- Practice setting up and managing a single-purpose computer with service account and special configuration
- Use sysinternals tools to set up and manage computers

Group Managed Service Account (GMSA)

Group Managed Service Account (gMSA) liittyy vahvasti *implementing service account* -konseptiin, ja se voi olla olennainen osa palvelutilien käyttöönottoa erityisesti Windows-ympäristössä.

🔐 Mikä on Group Managed Service Account (gMSA)?

gMSA on Microsoftin Active Directory -ominaisuus, joka tarjoaa **automaattisesti hallittavan palvelutilin** useille palvelimille tai palveluille. Se on suunniteltu korvaamaan manuaalisesti hallittavat tilit, kuten tavalliset domain-tilit, joita käytetään palveluiden ajamiseen.

☑ gMSAn edut

- **Automaattinen salasanan hallinta:** AD vaihtaa salasanan automaattisesti, eikä sinun tarvitse huolehtia siitä.
- **Usean palvelimen tuki:** Voidaan käyttää useilla palvelimilla, toisin kuin tavallinen Managed Service Account (MSA).
- **Parempi tietoturva:** Ei tarvitse tallentaa salasanoja konfiguraatioihin tai skripteihin.
- **Yhteensopiva monien palveluiden kanssa:** Esimerkiksi IIS, SQL Server, Task Scheduler, jne.

📋 Miten gMSA liittyy Sysinternalsiin?

Vaikka Sysinternals ei suoraan hallinnoi gMSA-tilejä, sen työkaluilla voi:

- Tarkastella, mitä tilejä palvelut käyttävät (esim. *Process Explorer*).
- Seurata gMSA-tilin käyttöä ja oikeuksia (*ProcMon*).
- Varmistaa, että palvelu toimii oikein gMSA-tilillä.

Windows - Kiosk software



Windows Serverin ja Active Directoryn (AD) avulla voi käyttää kiosk-tilaa esimerkiksi mainoksiin, palautteeseen ja ruokatilausnäyttöihin. Se ei ole kovin vaikeaa, ja siitä on monia hyötyjä. Kuitenkin sähköä ja vaattii se ohjelma pelittää esim. 24/7 tai ajastettuna 7-20 arkipäivinä ja viikonloppuna se on suljettu.

- Kiosk-tila tarkoittaa, että tietokone tai näyttö toimii *vain yhdellä tai tietyillä sovelluksilla*. Käyttäjä ei pääse muualle koneessa – ei työpöydälle, ei asetuksiin, ei nettiin (ellei niin haluta). Se on kuin lukittu käyttötila.
- Microsoft on rajannut tietyt hallinta- ja yritysminaisuudet vain Pro-, Enterprise- ja Education-versioihin. Home on tarkoitettu kotikäyttöön. Joten kiosk on saatavilla pro-, enterprise- ja education versioon.
- Kiosk - ohjelma on saatavilla Microsoft Store apps - mutta vian rajoitettu osa.

Miten se liittyy Windows Serveriin ja AD:hen?

- **Windows Server + Active Directory (AD)**: AD hallinnoi käyttäjiä ja laitteita keskitetysti. Voit määrittää, että tietyt koneet toimivat kiosk-tilassa.
- **Käyttöönotto**: Voit tehdä asetukset esimerkiksi PowerShellillä, Intune-hallintatyökalulla tai paikallisesti koneen asetuksista.

Mihin kiosk-tilaa voi käyttää?

- **Mainosnäytöt**: pyörittää jatkuvaa videota tai kuvaesitystä.
- **Palautejärjestelmät**: asiakas voi painaa nappia tai täyttää lomakkeen.
- **Ruokatilausnäytöt**: ravintolassa asiakas voi tilata ruovan itse.
- **Infopisteet**: esim. kartta tai aikataulut julkisissa tiloissa.
- **Sisäänkirjautuminen**: hotellit, tapahtumat, vastaanotot.
- **Tulostus- ja lipunmyntiautomaatit**: lentokentät, asemat.

Mitä hyötyä siitä on?

- **Turvallisuus**: käyttäjä ei pääse vahingossa tai tahallaan muualle koneessa.
- **Helpaus**: laite tekee vain yhtä asiaa – ei tarvitse kouluttaa käyttäjiä.
- **Hallittavuus**: AD:n kautta voit hallita useita laitteita kerralla.
- **Kustannustehokkuus**: ei tarvita henkilökuntaa jokaiseen pisteeseen.
- **Luottavuus**: vähemmän virheitä ja vähemmän huoltoa.

Onko se vaikeaa?

- **Ei kovin vaikeaa**, jos osaat vähän Windowsin hallintaa.
- Tarvitset:
 - Windows 10/11 tai Windows Server 2016/2019/2022
 - Sovelluksen tai verkkosivun, jota haluat näyttää
 - Mahdollisesti AD tai Intune, jos haluat hallita useita laitteita

Vaikuttaako se muuhun?

- **Kyllä**, kone lukittuu kiosk-tilaan, eli se ei toimi normaalina tietokoneena.
- Jos haluat käyttää konetta muuhun, kiosk-tila pitää poistaa.
- Kannattaa käyttää erillisiä laitteita kiosk-käyttöön.

#####
#####

HARJOITUS DEMON VIDEOON MUKAAN - START HERE:

Display a specific web page

- Use a service account as login account
- The account should auto login when computer was rebooted
- Web browser should startup automatically once logged in and in full screen
- Set the computer to always be ON
- Restrict logon for service account

Tässä harjoituksessa käytetään VM1 (windows server) ja toisena VM2 (Windows 10/11)

Periaatteessa harjoituksen ideana on kuin avatessa nettisivun menee vaikapa oletuksena "iltalehti.fi" tai muu nettisivustoona vaikapa html koodattu webbisivustoon tai example.com oletuksena.

Avaa ensimmäisenä windows serveri ja luo uusi tunnus (normi user tunnus) - ja kirjoitettu ylös talteen (joku helppo tunnistettava). Koska tämä pätee jos on satoja tai tuhansia tunnuksia, että tunnisteltavissa. Valitse tai luo esim. OU josta itse tietää ja jää muistiin mikä tämä.

Tuohon tuli dollarin merki, josta työelämässä saatetaan käyttää jos on paljon laitetta ja tunnisteltavina, ja sama pätee AD haku kun etsitään superhakua löytyy x nimellä.

The screenshot shows the Windows Server Active Directory Users and Computers console. On the left, the navigation pane lists domains: Asia, Builtin, Computers, Domain Controllers, and EU. Under EU, there are sub-folders: Computers, Service accounts, Servers, and Users. The 'Service accounts' folder is selected. In the center, a 'New Object - User' dialog box is open. It displays the 'Create in:' path as YritysXC.local/EU/Service accounts. The 'First name:' field contains 'Website', 'Last name:' contains 'Login', and 'Full name:' is 'Website Login'. The 'User logon name:' field is set to '\$website-login' with the domain '@YritysXC.local' selected. Below it, the 'User logon name (pre-Windows 2000):' fields show 'YRITYSXC\' and '\$website-login'. At the bottom of the dialog are buttons for '< Back', 'Next >', and 'Cancel'.

The second part of the screenshot shows the continuation of the 'New Object - User' dialog. It asks for a password, which is entered as 'P@sswOrd'. The 'Confirm password:' field also contains 'P@sswOrd'. Below the password fields are several checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (checked), 'Password never expires' (checked), and 'Account is disabled' (unchecked). The bottom of the dialog includes '< Back', 'Next >', and 'Cancel' buttons.

Salasana: P@sswOrd

Tätä ei tulla muuttaa ikinä ja huomoina tämä onkin harjoitus, mutta tosi elämässä tästä jouduttaisiin dokumentoida ja käyttää vain pitkää salasanaa.

Avaa toinen vm2 (windows 10) ja mene nettiin, sekä lataa "sysinternals suite".

- Lataa tuo paketti ja ignore oikea ala kulman mukaan tai nettiyhteys ei pelitä (aikaisempien säätöjä)

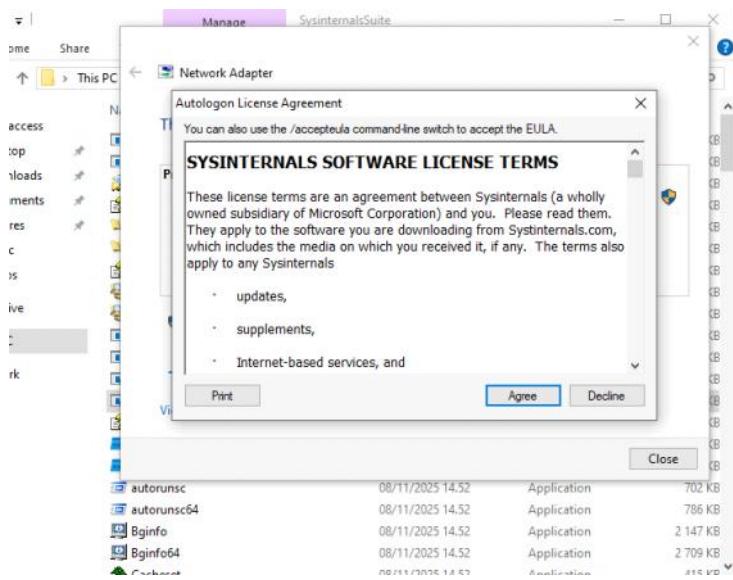
The screenshot shows a Microsoft Edge browser window with the URL <https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>. The page content includes a sidebar with links like Home, Downloads, and Sysinternals Suite. The main content area has a TOC, author information, and several download links. A red box highlights the first download link: "Download Sysinternals Suite" (166.1 MB). Below it are links for "Download Sysinternals Suite for Nano Server" (9.5 MB), "Download Sysinternals Suite for ARM64" (15 MB), and "Install Sysinternals Suite from the Microsoft Store". At the bottom of the page, there's an "Introduction" section and a note about the suite containing individual troubleshooting tools.

This screenshot is identical to the one above, showing the Sysinternals Suite download page in Microsoft Edge. The "Download Sysinternals Suite" link is again highlighted with a red box.

Latauksen jälkeen purkkaa zip tiedosto ja avaa se, sekä otetaan sellainen ohjelma käyttöön kuin "autologon"

The screenshot shows a Windows File Explorer window with the path "This PC > Downloads > SysinternalsSuite". The folder contains several files, including "accesschk", "AccessEnum", "AdExplorer", "ADExplorer64", "ADInsight", "ADInsight64", "adrestore", "adrestore64", "Autologon", and "Autologon64". The file "Autologon64" is highlighted with a green box.

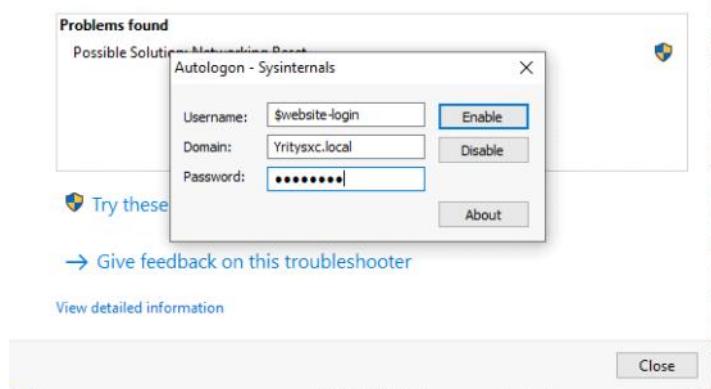
Ponnahti et syötä yritysalueverkkon admin-tunnus - tämä koska johtuen GPO-asetuksista, että vaikuttaa tähän mitä ohjelmia VM2 tavallinen käyttäjä käyttääkään



Tähän kenttään tule "website-login" tunnuksensa, ja alkuun luki "minä".

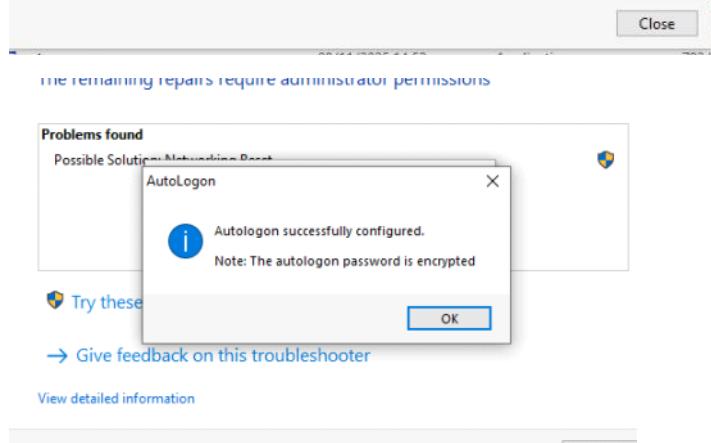
- Varmistahan on kirjoitettu oikein ettei välilyöntiä tai yms
- "enable"

THE REMAINING REPAIRS REQUIRE ADMINISTRATOR PERMISSIONS



→ Give feedback on this troubleshooter

[View detailed information](#)



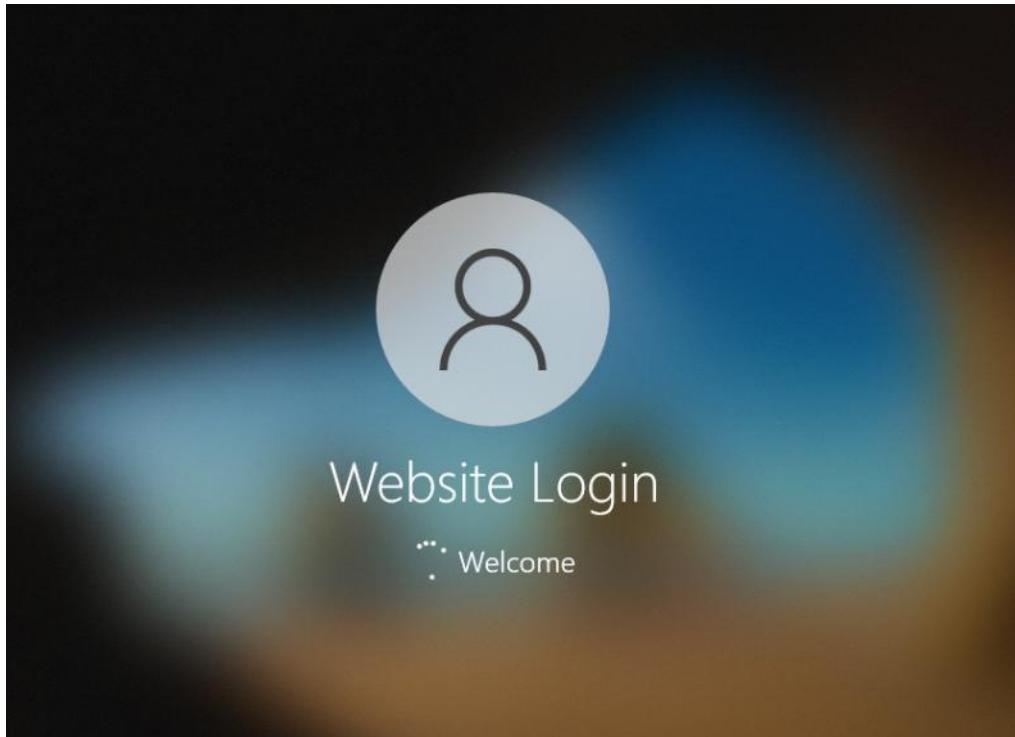
→ Give feedback on this troubleshooter

[View detailed information](#)

Seuraavaksi buuttaa kone (restart) - To be continue...

- En syöttänyt mitään tunnusta et normi buuttaus ja sitten tuli näkyviin tällainen näkymänsä

HUOMIO!!! Muistutuksena User1 tunnuksella kirjaudutti sisään siellä on se ladattu ohjelma "sysinternals" - tätä ei löydy "\$website login" tunnuksella ja jos tarkistaa "File explorer / Download" kansiosta.



AutoLogon ja käyttäjätunnukset – käytännön muistio

- AutoLogon määrittää **yhden käyttäjätunnusken**, jolla Windows kirjautuu automaattisesti sisään.
- Kun kone on käynnistynyt, voit **manuaalisesti vaihtaa käyttäjää** (esim. kirjautua ulos ja sisään "user1":llä).
- AutoLogon ei vahda tunnusta automaattisesti — se käyttää aina sitä, joka on sille asetettu.

📁 Käyttäjäkohtaiset lataukset

- Jos "user1" on ladannut ohjelman (esim. Sysinternals), se löytyy vain **user1:n latauskansiosta** (C:\Users\user1\Downloads).
- Jos kirjaudut sisään toisella tunnuksella (esim. "\$website login"), et näe user1:n latauksia — jokaisella käyttäjällä on **oma erillinen profiili ja kansiorakenne**.
- Tämä on tärkeää, jos haluat käyttää ladattua ohjelmaa tai tiedostoa — sinun täytyy olla **oikea käyttäjä**, jolla se on ladattu tai siirtää tiedosto yhteiseen sijaintiin.

💻 Yhden tunnuksen käyttö esityksissä tai asiakasnäytöissä

- Jos rakentaa **mainoksen**, **ohjelman** tai **kyselyn**, jonka haluat näyttää asiakkaille tai ohikulkijoille:
 - Käytä **yhtä käyttäjätunnusta**, johon kaikki tarvittavat ohjelmat ja asetukset on valmiiksi määritetty.
 - Voi käyttää **AutoLogonia** varmistamaan, että kone kirjautuu aina sisään oikealla tunnuksella.
 - Voi määrittää, että **Chrome tai video-ohjelma käynnistyy automaattisesti koko näytön tilassa**.

❖ VM1 hallitsemassa VM2:ta

- VM1 (Windows Server) voi hallita VM2:ta, jos se toimii **Hyper-V-isäntänä**.
- VM1 voi:
 - Käynnistää VM2:n automaattisesti.
 - Buutata tai sammuttaa VM2:n etänä.
 - Asettaa VM2:lle **automaattikäynnistyksen** ja määrittää, että esim. Chrome avautuu heti.
 - Lisäksi VM2 avatessa siinä on se kiinteä tunnus ja kirjautuessa ei kysy salasana esim. Uudelleen käynnistäessä
- Tämä mahdollistaa sen, että VM2 toimii **itsenäisenä esityskoneena**, mutta VM1 hallinnoi taustalla.

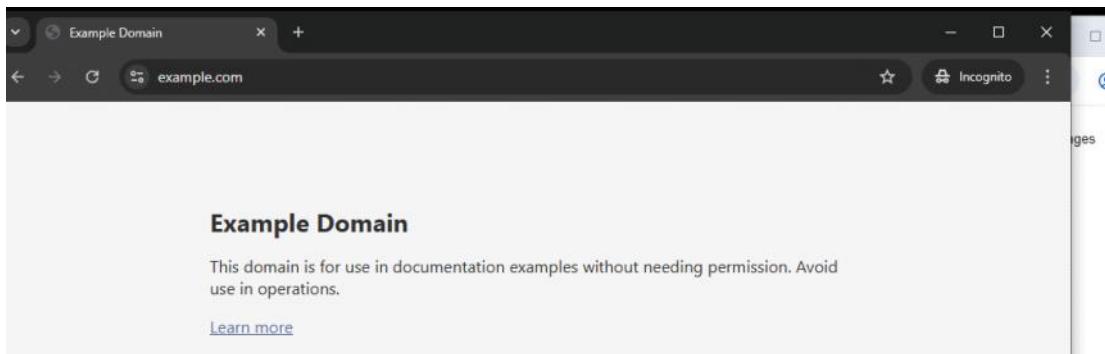
#####

Seuraavaksi ja jatkuu:

Seuraavaksi asetetaan joku nettisivusto, josta esim. Haluttaan toimia kuin aktiivisena käytöön - tästä voi esim. Asettaa ja luoda html koodina (examle.com) vaikappa (löytyy toinen video ohje)

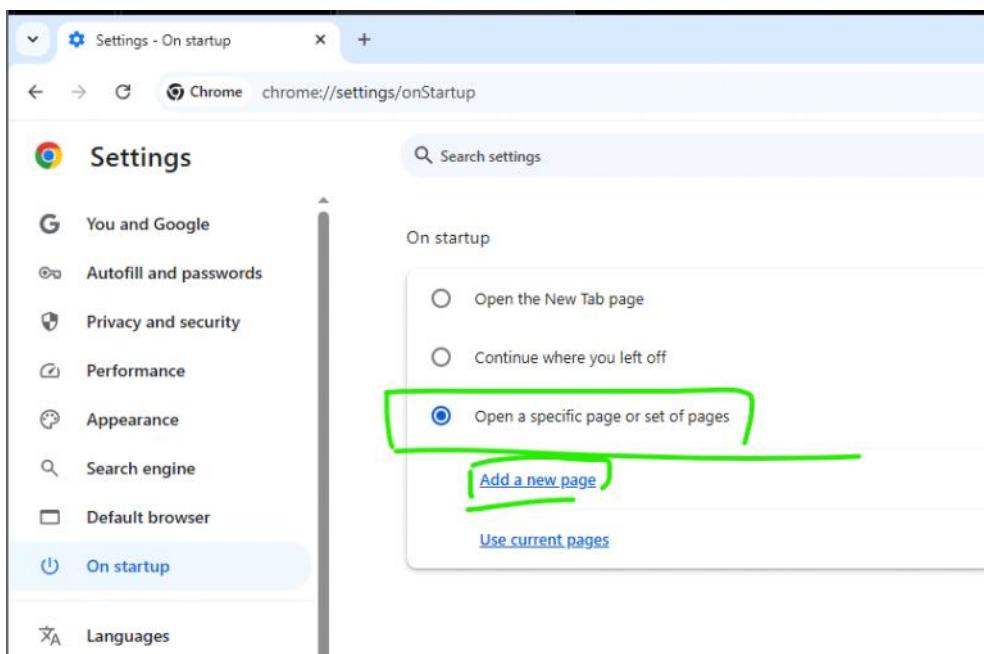
Video ohjeessa menee chromen kautta ja varmistettaan win10 on lisätty chrome tai jouduttaan lataa normaalista uusiksi

Asettaan tällainen sivusto esim. (mutta tämä tulee avattu siviston mukaan sitten ponnahtaa kuin ensimmäisenä sivustona) - vähä kuin koulussa ensimmäisen avattu siviston koulun nettisivu.

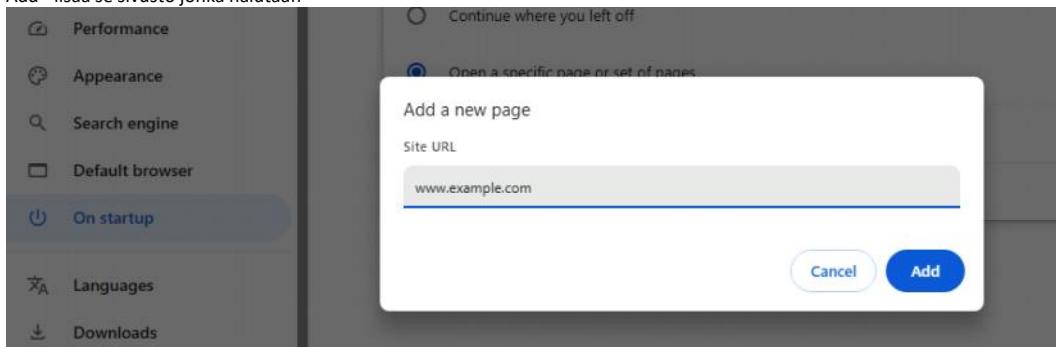


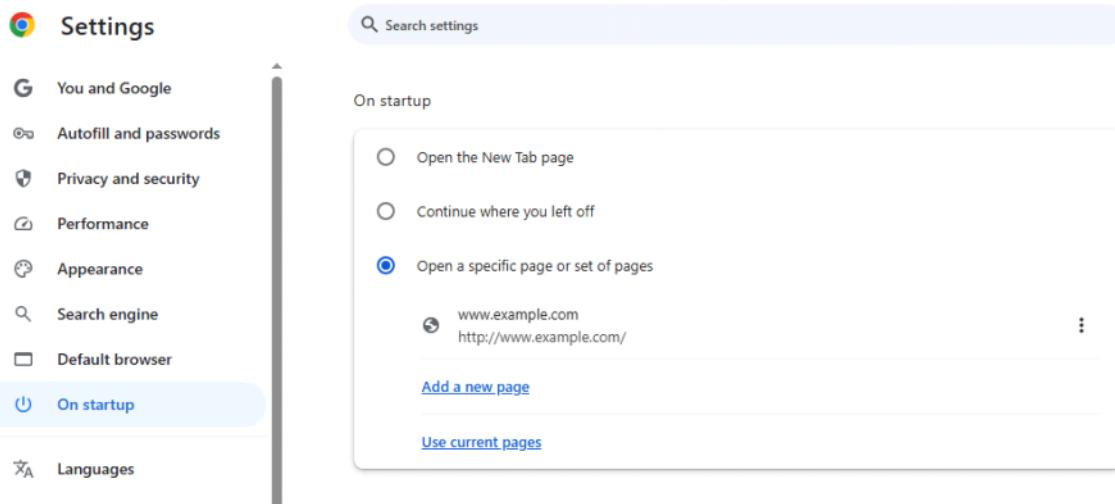
Avaa siis ihan chrome sivusto, jossa on kirjautumisen menetelmä ja Ei incognito tyyppiä

Valitse asetukset (settings) ja "on startup"



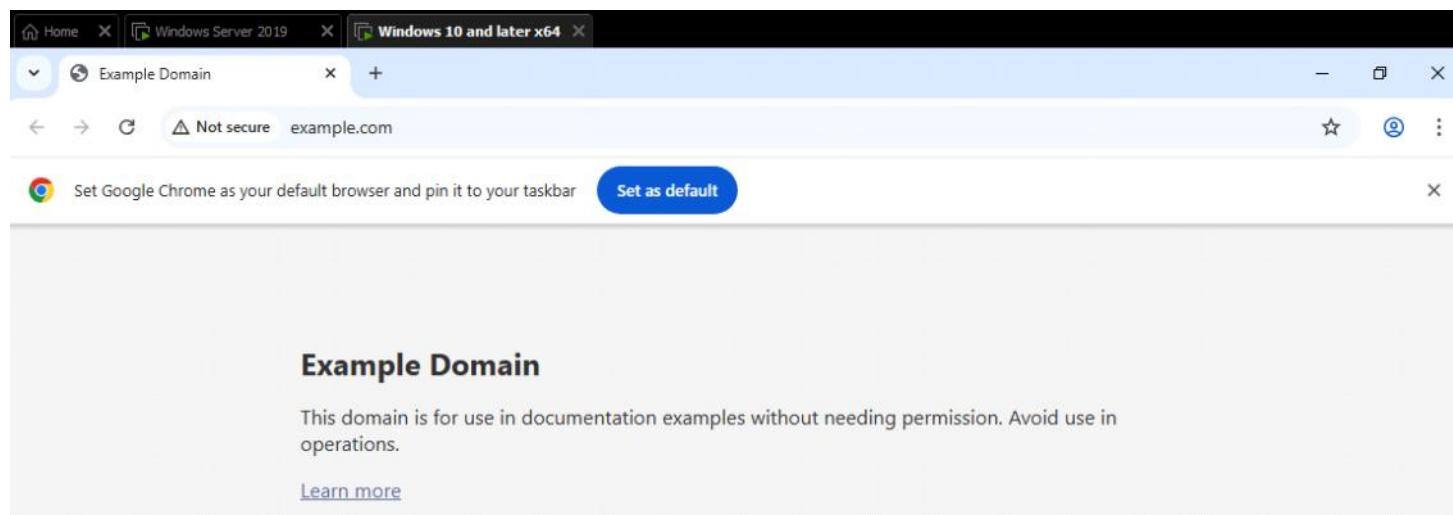
Add - lisää se sivusto jonka halutaan



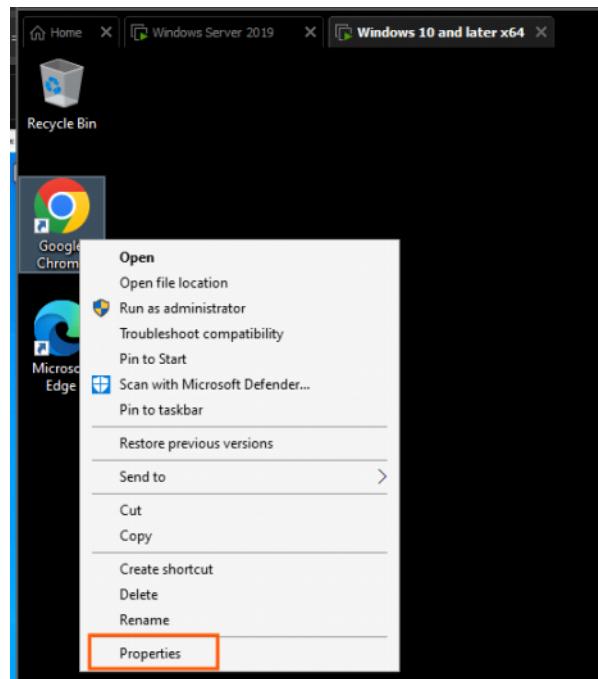


Sulje koko selain ja avaa normaalista chrome uusiksi

- Saattaa avautua toinen välilehti, mutta tältä pitääsi tulla näkyviinsä ja pieni viive DNS ongelmansa

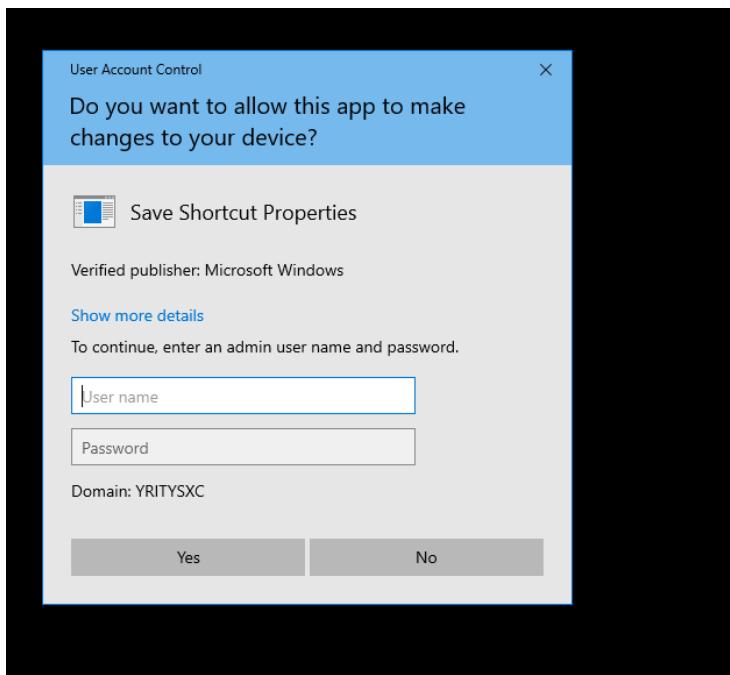
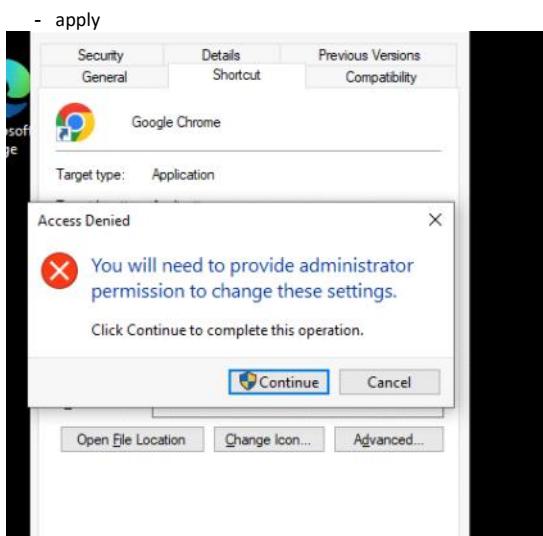
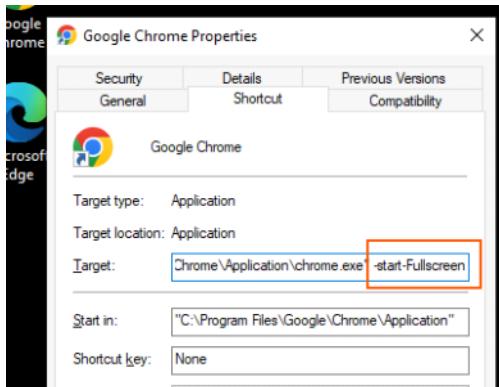


Seuraavaksi pientä säättöä ja säädellään sitä kauniimmaksi



Lisää perään tollainen :: -start-Fullscreen

- Varmista ettei molemmissa ole välilyöntiä, että on viiva ja huom yhteen



Ja viimeisenä OK

Pari buuttausta ja troubleshoots - ei aina toimi yhdellä lävitse sekä suoritettu gpupdate /force
- Jossain määrin saattoi tulla netti ongelmia

Nyt alkoi pelittää, mutta näin että menee täys kokonaiseen ruudun näkyviin.

- Periaatteessa jos ei asettaisi " --start-fullscreen" niin kaksois klikkausella voi periaatteessa tai jollakin näppäimistön kautta asettaa kokonäyttöksi se selain ja tästä riippuu mitä mainosta/ohjelmaa/kyselyä laitetaan näkyviin
- Muutin exaple.com --> iltalehteen (vähä jotakin kivempaa)

Lauantai 8.11.2025 Aatos

TV-OHJELMAT ETUA KATTOKORKO NÄKÖISLEHTI

ILTALEHTI

To exit full screen, press and hold Esc

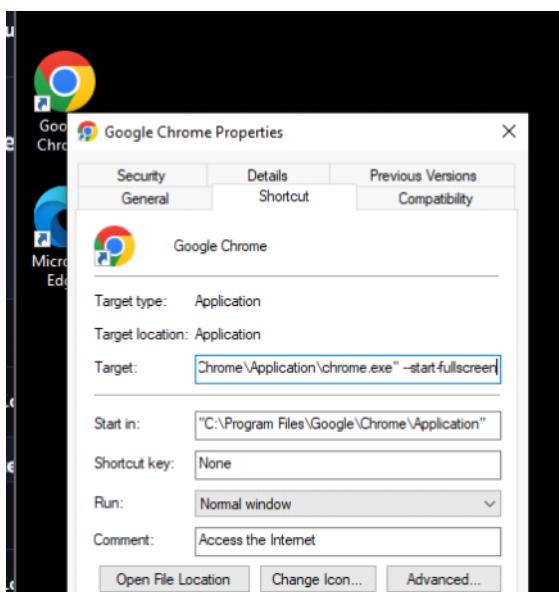
KIRJAUDU

Etusivu Uutiset Urheilu Viihde Plus Sää Videot Autot Terveys Hyväolo Tyylili.com Asuminen Perhe Pippuri.fi Matkailu Bitti Podcast

JUURI NYT Sanna Marinilta suora vastaus vaalielehdokkuudesta – Suora lähetys käynnissä

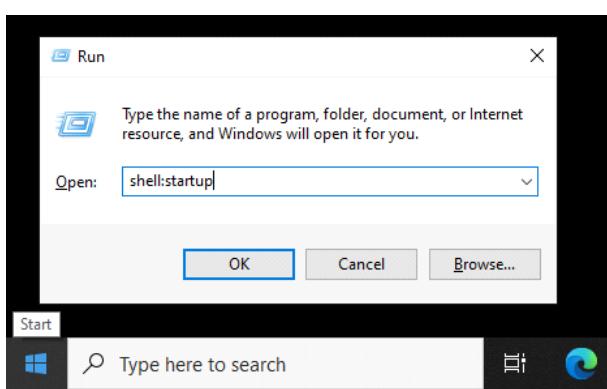
JUURI NYT Tamperelaisjohtaja toivoi kaupunkiin "vähemmän Popedaa" – Costello Hautamäki tulistui

PLUS Harva ymmärtää, että tämä outo tunne jaloissa onkin hälytysmerkki – Varaa aika lääkärille



Seuraavaksi

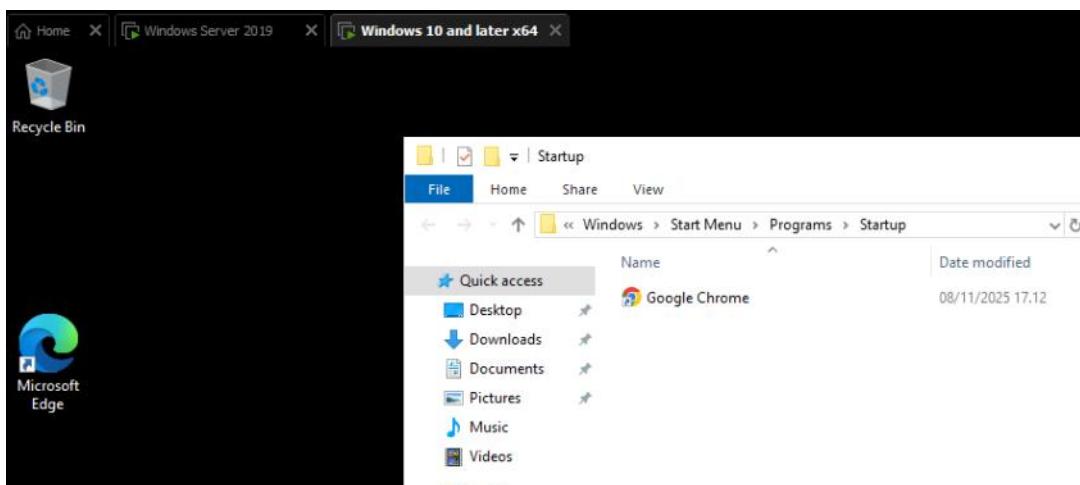
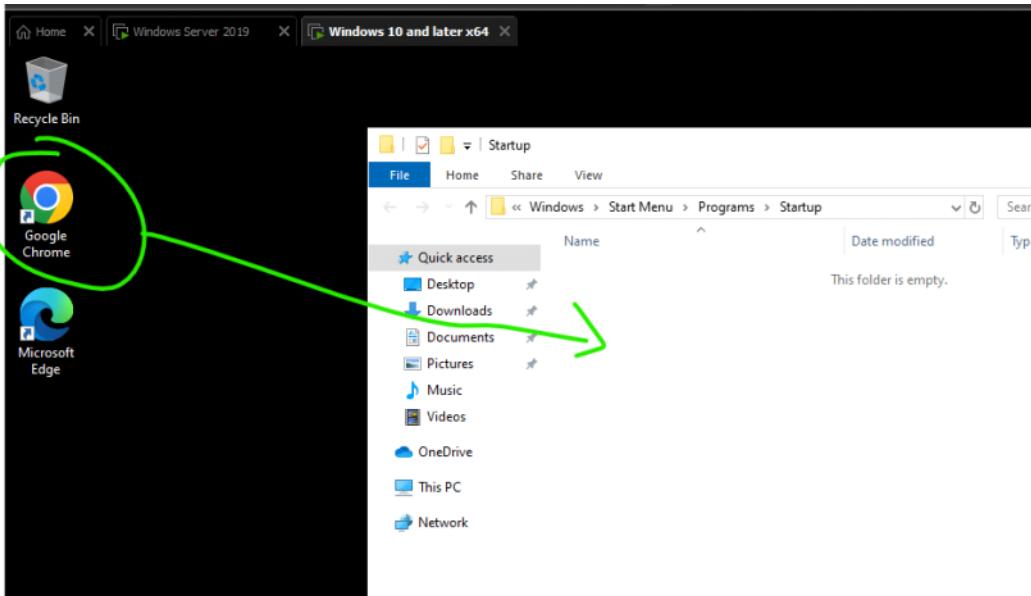
- Avaa näppäimistöstä (win logo + R) ja syötä tällainen teema:



Tähän kansioon voidaan asettaa kaikkia ohjelmia ja just käyttäen esim. Niitä "startup" näkyvimiä ja voidaan avata automaattisesti.

Siirrä koko chrome siis tämä desktop kuvake kansion alle.

- Taas kysellyä yritysverkkoalueen admin-tunnusta ja sallitetaan se



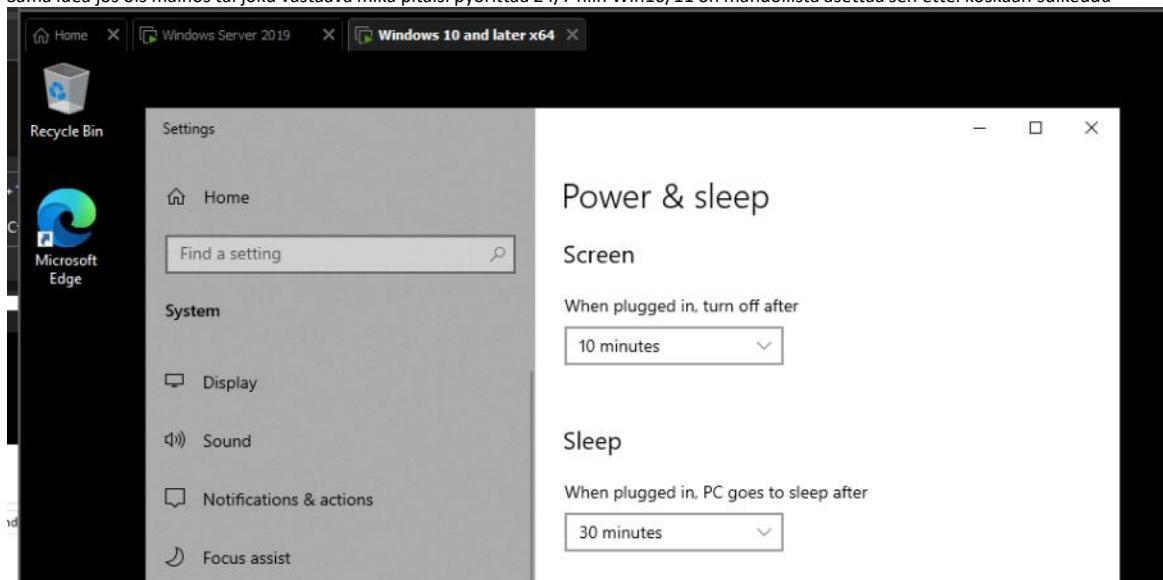
Tämän jälkeen sen pitäisi avautua automaattisesti (jos buuttaa koneen) eli kirjauttuessa tähän työaseman (winsite login)

- Tässä väliin buutataan konetta ja check check
- Alhaalla (tiedosto) on se kuvakaappaus video, josta siinä on jokin viive et se avaa automaattisesti sen chrome sivustonsa mutta niin saattaisiin käyntiinsä (esim. Mainos)
- Kuitenkin kiosk-moodi pitää olla



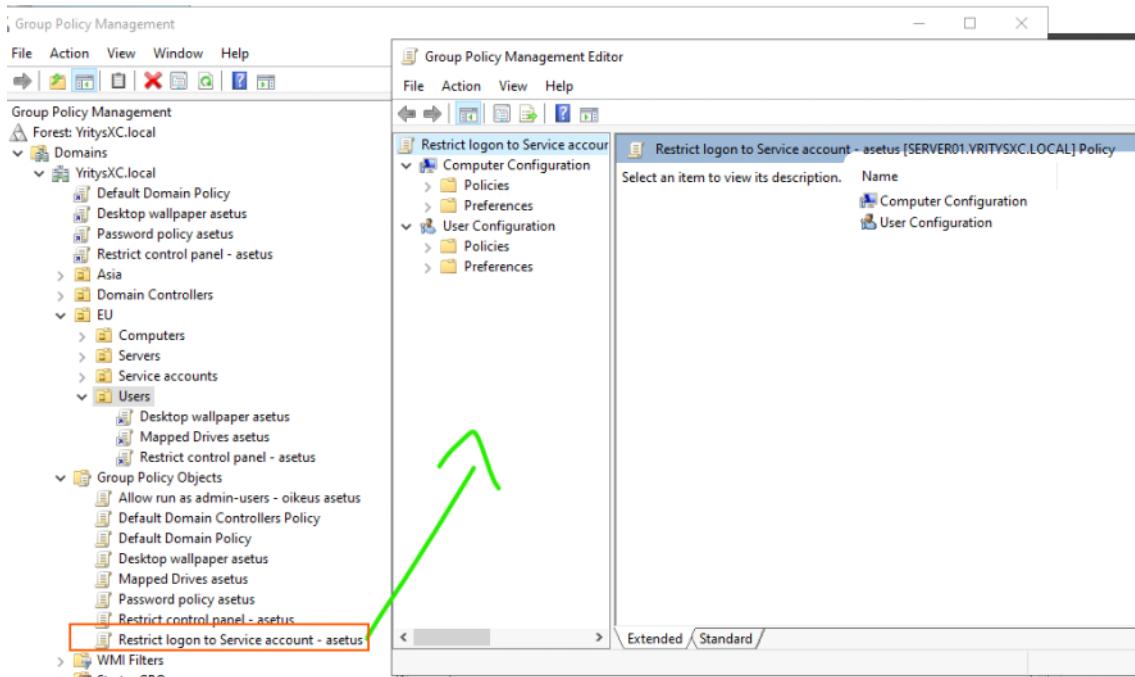
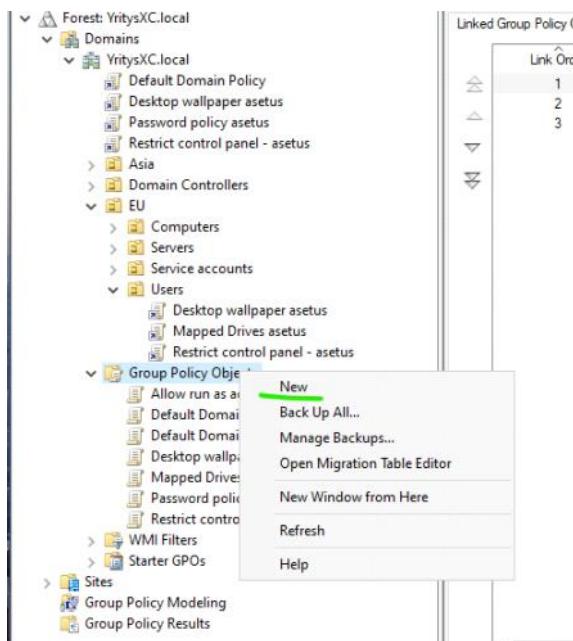
Näyttötalle
nnus 202...

Sama idea jos ois mainos tai joku vastava mikä pitäisi pyörittää 24/7 niin Win10/11 on mahdollista asettaa sen ettei koskaan sulkeudu



Seuraavaksi / aiheen viimeinen juttu

Luodaan uusi GPO, jonka ideana on kuin tähän kiosk (website login) tunnuksensa ei päästetä muita käyttäjiä ja vain tähän esim. Mainos joka pyörii 24/7 niin vain tälle tunnukselle. Jos yritysalueenverkkoon kirjautuu toinen käyttäjä niin sillä tulee jatkuvasti esto paitsi admin itsnesä varmaan. Testataan ja varmisitthaan, voi olla tästä GPO policy:ä poistettaan testauksen jälkeen



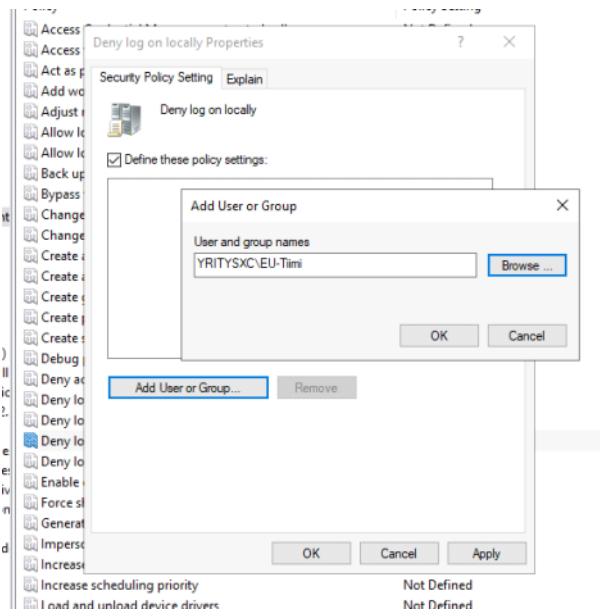
Nyt ideana käytettääksi "website login", ettei sallita muita active directory käyttäjiä työaseman kirjautumiseen eli vaihtaa tunnuksen prosessia. GPO asetuksesta mennään "computer configuration" ja se on "policies" koska ei haluta muutosta.

Tän alla on paljon access policyä, että koskien käyttäjätunnusken sääntöä ja nyt tämän demon osalta otetaan tämä "deny log on locally". Kielettää standardiset/tavalliset käyttäjät, ettei ne pääse tähän vm2 työaseman.

- Ennen kuin aktivoidaan tämä policy yksi osa sääntöä ja varmista on gruppi ryhmä olemassa.

Browse... - tuosta vaa ikkunansa, että mitä käyttäjää/ryhmiä haettaan ja ketä nimettiä - näitä käyttäjiä estettääni toisiaan.

- Apply ja OK

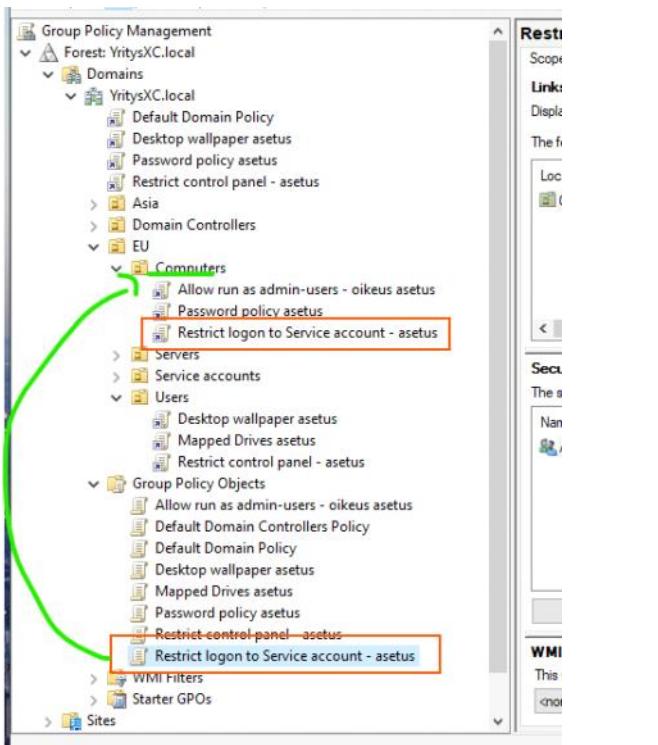


Group Policy Management Editor

File Action View Help

Policy	Policy Setting
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Not Defined
Act as part of the operating system	Not Defined
Add workstations to domain	Not Defined
Adjust memory quotas for a process	Not Defined
Allow log on locally	Not Defined
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Not Defined
Bypass traverse checking	Not Defined
Change the system time	Not Defined
Change the time zone	Not Defined
Create a pagefile	Not Defined
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	YRITYSXC\EU-Tiimi
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delegation	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined

GPO objekti kansiosta "drag-drop" toi sääntö tonne computers kansion alle



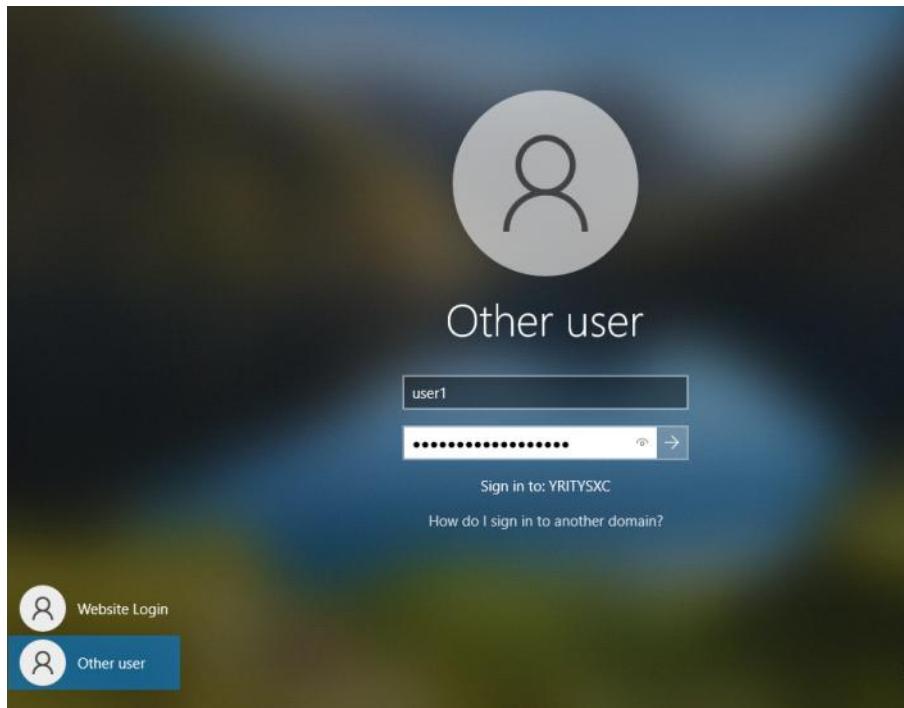
Seuraavaksi suoritetaan päivitystä samantien VM2:ssa eli gpupdate /force
Päivityksen jälkeen testataan toisella tunnuksella esim. EU/yritys yksi tunnuksista.. - tarkista jos ei musita niiden passua

Kokeillaan näitä

- \$website-login ; P@ssw0rd

User1 ; punajuuriKeitto123 | Pääsi sisään ja welcome??

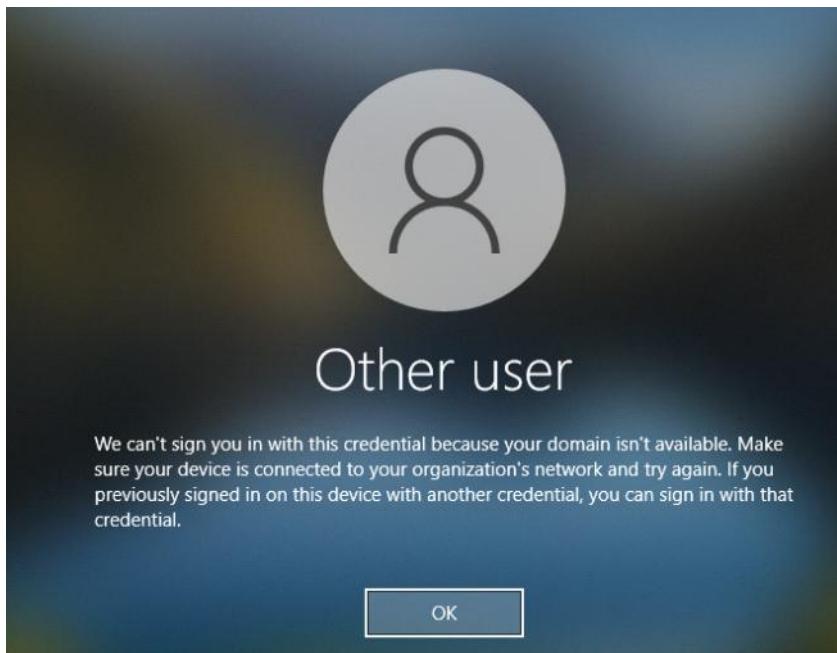
Team1 - alex applicant, jane simple, johndoe1, user1 (user name)
Tässä tuli ongelmia gpo asetuksien kanssa että osat pitää asettaa pois päältä ettei ota niitä käyttöön..



AD >> EU/Team Leader / JohnDoe2 (#Team-leader1)

Johndo2 ; P@ssw0rd

Salasana >> S4laS\$na



Taas säätöjä ja toistui paljon \$gpupdate /force kanssa

```
PS C:\Users\$website-login> gpupdate /force
Updating policy...

Computer policy could not be updated successfully. The following errors were encountered:

The processing of Group Policy failed. Windows could not resolve the computer name. This could be caused by one of more of the following:
a) Name Resolution failure on the current domain controller.
b) Active Directory Replication Latency (an account created on another domain controller has not replicated to the current domain controller).

User Policy could not be updated successfully. The following errors were encountered:

The processing of Group Policy failed. Windows could not resolve the user name. This could be caused by one of more of the following:
a) Name Resolution failure on the current domain controller.
b) Active Directory Replication Latency (an account created on another domain controller has not replicated to the current domain controller).

To diagnose the failure, review the event log or run GPRESULT /H GReport.html from the command line to access information about Group Policy results.

PS C:\Users\$website-login> ping 192.168.100.10

Pinging 192.168.100.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.100.13: Destination host unreachable.

Ping statistics for 192.168.100.10:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
PS C:\Users\$website-login> ping 192.168.100.10
```

Nyt testastiin tämä käyttis (user1 ; punajuuriKeitto123)

- Eli toimi ja kyllä!!
- Tästä pitää varmistaa se ryhmä ketä siellä alla on listattuna. (johndoe1 ; S€cr3ts - Team1)



Tämä on vain esim. Estettään näitä tiimejä/käyttäjiä kirjautumatta tonne "Website-login" työasemaan.

The screenshot shows the Group Policy Management console. A GPO named 'Restrict logon to Service account - asetus' is selected under 'Computer Configuration / Policies / Windows Settings / Name Resolution Policy'. The 'WMI Filtering' button is visible at the bottom. The 'Deny log on locally Properties' dialog is open, showing the 'Security Policy Setting' tab with a user 'user1' selected.

Tämä on yksi Team1 jäsenistä, mutta ei turha testattu muita ainakin "johndoe1" ei pääsyt sisään

The screenshot shows the Active Directory Users and Computers console. A security group named 'Team1' is selected. The 'Members' tab is open, showing the following members:

Name	Active Directory Domain Services Folder
Alex Applicant	YritysXC.local/EU/Users
Jane Simple	YritysXC.local/EU/Users
John Doe	YritysXC.local/EU/Users
User name	YritysXC.local/EU/Users

Ratkaisu osuu ja miten saatiin tämä toimimaan??

VM2:ssa pitää varmistaa että se "website-login" on liittänyt DNS yrityalueelle, ja jos ei varmista se - admin-tunnuksilla - ja useita toistoja voi tulla

Takaisin VM1 windows serveriin

- Tästä jouduttiin asettaa muutama GPO asetukset/pelisääntöä pois päältä - koska tämä päätee aikaisempia harjoituksia ja osat ei ole poistettu.
- Ei turhaa poistetta luoneita GPO sääntöjä, mutta voidaan asettaa niitä pois päältä (Disabled) - ja säilytetään ne olemassa olevaksi listaksi. Minkä GPO säännöt laitettiin pois?

Allow run as admin-users - oikeus asetus	GPO STATUS: ALL SETTINGS DISABLED
Password policy - asetus	GPO STATUS: ALL SETTINGS DISABLED
Restrict logon to Service account - asetus	GPO STATUS: ENABLED
Desktop wallpaper asetus	GPO STATUS: ENABLED
Mapped Drives asetus	GPO STATUS: ENABLED
Restrict control panel - asetus	GPO STATUS: ALL SETTINGS DISABLED

- Kun on asettanut pois päältä niin muista päivittää powershell kautta VM1 ja VM2:ssa.

The screenshot shows the Group Policy Management console. The 'Restrict logon to Service account - asetus' GPO is selected. The 'Scope' tab is active, showing the following details:

- Domain: YritysXC.local
- Owner: Domain Admins (YRITYSXC\Domain Admins)
- Created: 8.11.2025 8.45.38
- Modified: 9.11.2025 5.16.01
- User version: 0 (AD), 0 (SYSVOL)
- Computer version: 7 (AD), 7 (SYSVOL)
- Unique ID: {25A8AEA0-8343-4349-A628-FD22873F82CE}
- GPO Status: Enabled
- Comment:

#####

MINIYHTEENVETO JA POHDINTA - START HERE;

- GPO säännöstää vaikka pidetään kaikki päällä - josta voi kuitenkin aiheuttaa jotakin ristiriittoja/esteitä ja sama pätee viivettäkin.
- Ristiriidan syntymisestä voi koskea mm. kohdistuvat samaan kohteeseen (sama käyttäjä tai kone) ja linkitysjärjestys ja prioriteetti vaikuttavat siihen, mikä asetus voittaa.
 - Kuitenkin osasta GPO säännöstää on asetettu pois päältä, tämän vuoksi joudut tarkistaa niitähän sääntöjä koskeeko se työasema vai käyttäjän konfigurointia etää onko policy vai suositus.

❖ GPO:n soveltamisjärjestys (tärkeää!)

1. Local Group Policy
2. Site
3. Domain
4. Organizational Unit (OU) – lähimmästä OU:sta tulee korkein prioriteetti
5. Jos useita GPO:ita samassa OU:ssa → **järjestys GPMC:ssä ratkaisee**

Pohdinta: Kiosk-ohjelman ja Sysinternals-konfiguraation hyödyntäminen mainoslaitteessa

Tämä koskee VM2-laitteessa toimivaa "kiosk"-ohjelmaa ja siihen liittyvää Sysinternals-konfiguraatiota. Kyseessä on hyödyllinen ratkaisu nyky- ja tulevaisuuden teknologioihin, erityisesti silloin kun halutaan näyttää mainoksia, esityksiä tai muuta sisältöä automaattisesti – joko 24/7 tai ajastetusti.

1. Laite käynnistyvää automaattisesti.
2. Automaattinen kirjautuminen ilman salasanaa voidaan toteuttaa Sysinternalsin **AutoLogon**-työkalulla. Samalla voidaan estää muiden käyttäjien pääsy, jos käytössä on sisäinen tiimi ja määritetty DNS/IP-osoite.
3. Chrome voidaan käynnistää viiveellä ja ohjata suoraan halutulle sivustolle. Tämä mahdollistaa esimerkiksi MP4-videoainosten toiston koko näytön tilassa.
 - a. Ratkaisu voidaan toteuttaa työasemalla, kuten Intel NUC:lla, jossa on Windows 10/11.
 - b. Lyhyesti: voidaan rakentaa automaattisesti käynnistyvä, ajastettu ja vuorokauden ympäri pyörivä mainosvideon toisto Windows Server - ympäristössä (esim. VM1), hyödyntäen Chromea kiosk-tilassa tai muita kevyempää ratkaisuja.
 - c. VM1 voi hallita ja buuttaa toisen laitteen etänä, jos etähallinta on käytössä ja laite on verkossa.
 - d. d. Suurin haaste on, että VM1 ei voi käynnistää VM2:ta, jos VM2 on fyysisesti eri sijainnissa ja virta on poikki – esimerkiksi jos laite sijaitsee kaukana eikä siinä ole etähallittavaa virranhallintaa.
4. Kokonaisuus riippuu yrityksen toiminnasta ja palvelumallista: kannattaako rakentaa useita laitteita eri sijainteihin? Vianmääritysessä on huomioitava, että paikan päälle meneminen voi olla välttämätöntä.
 - Paikan päällä tarvitaan oikeat välineet ja kärsivällisyys, jotta laite saadaan toimimaan pitkäjänteiseksi. Tämä riippuu myös siitä, onko järjestelmä rakennettu esimerkiksi Ubuntu Linuxin tai muun alustan päälle – ja miten se on toteutettu.
- I. **Linux-pohjainen järjestelmä ja verkkojohdeiden muodostaminen**
 - I. Jos käytössä on Linux-pohjainen järjestelmä (esim. Ubuntu, Debian, Fedora) ja laitteena vaikkapa Intel NUC tai muu litteä tietokone, nettiyhteyden voi muodostaa monella eri tavalla – aivan kuten Windowsissa, ja usein jopa joustavammin.
 - II.
 - I. **Langallinen tai langaton yhteys** voidaan toteuttaa esimerkiksi Wi-Fi:n kautta, jolloin käytössä voi olla 5G SIM-kortti ja konfiguroitu reititin.
 - II. **Yhteyden muodostaminen voi vaatia komentoivin käyttöä**, kuten: \$nmcli device wifi connect "VerkonNimi" password "Salasana"
 - I. tai vaihtoehtoisesi graafisen käyttöliittymän kautta ilman komentoja.
 - III. **VPN- tai SSH-tunnelointi** mahdollistaa suojuvan yhteyden muodostamisen tai yhdistämisen sisäverkkoon, mikä voi olla tarpeen etähallinnassa tai tietoturvan varmistamisessa.

Harjoituksien kannalta tätä "kiosk-ohjelma" voi poistaa ja muuttaa sen automaattisen kirjautumisen takaisin Windows asetuksensa, että syötä virallinen AD käyttäjätunnus. Tästä on lisätty oma pieni sivu projekti ja erillinen oma **sivu 6.1.1. mini kiosk ohjelma**- pieni oma sivu kiinnostus ja tästä voi esim. Joskus myöhemmin testata rakentaa yhdellä tunnuksella.

Entä pilvipalvelu?

Jos rakentaisi kiosk-laitteita, jotka toimivat eri paikoissa ja haluat hallita niitä keskitetyisti, **Microsoft Entra ID + Intune** on erittäin tehokas yhdistelmä. Se mahdollistaa **automaattisen kirjautumisen, etäkonfiguroinnin, kiosk-tilan hallinnan ja tietoturvan**, ilman että käyttäjää/asentajaa tarvitsee käydä fyysisesti paikan päällä.

Microsoft Entra ID (entinen Azure AD) toimii erinomaisesti kiosk-laitteiden ja etähallinnan kanssa, kun halutaan keskitettyä identiteetti- ja laitehallintaa pilven kautta. Se mahdollistaa automaattisen kirjautumisen, laitekäytännöt, etäkonfiguroinnin ja jopa kiosk-tilan hallinnan Intunen tai muiden MDM-ratkaisujen kautta.

🔒 Mitä Microsoft Entra ID tekee kiosk-laitteiden kanssa?

1. Laiteidentiteetin hallinta

- Laitteet voidaan rekisteröidä Entra ID:hen (Azure AD Join tai Entra Join).
- Mahdollistaa käytännönhallinnan, pääsynhallinnan ja etävalvonnan.

2. Automaattinen kirjautuminen

- Voit määrittää automaattisen kirjautumisen kiosk-laitteelle ilman salasanaa.
- Tämä vaatii usein rekisteröintiä tai Intune-profiiliin, koska Entra ID ei oletuksena tue automaattista kirjautumista ilman käyttäjän vuorovaikutusta.

3. Kiosk-tila ja konfiguraatioprofilil

- Intune tai muu MDM voi määrittää laitteen kiosk-tilaan, jossa vain yksi sovellus (esim. Chrome) on käytettävissä.
- Voit käyttää konfiguraatioprofiileja määrittämään, mitä sovelluksia ja asetuksia laitteessa on.

4. Etähallinta ja valvonta

- Entra ID yhdistetynä Intuneen mahdollistaa:
 - Sovellusten etäasennuksen
 - Laitekäytännöt (esim. verkkojohdeet, VPN, Wi-Fi)
 - Etäbuutin tai uudelleenkäynnistys (jos laitteessa on tuki)
 - Tietoturvakäytännöt ja compliance-tarkastukset

Microsoft Entra ID + Intune toimii kuin pilvipohjainen versio fyysisestä **Windows Server -ympäristöstä**, mutta **hajautetusti ja skaalautuvasti**. Se tarjoaa

keskitetyn hallinnan, automaattisen konfiguroinnin ja etävalvonnan. Mutta kuten kysyt, **poikkeustilanteet kuten katkokset** tuovat omat haasteensa.

⚠️ Mitä tapahtuu katoksen tai häiriön aikana?

◊ 1. Laitteen verkkojohde katkeaa (esim. 5G-reitin pois päältä)

- Intune ei voi ottaa yhteyttä laitteeseen.
- Etähallinta ei toimi ennen kuin yhteys palautuu.
- Laite toimii **viimeksi ladattujen asetusten mukaan** – esim. kiosk-tila jatkuu normaalista.

◊ 2. Sähkökatko tai laitteen sammuminen

- Laite ei ole käynnissä → ei yhteyttä pilveen.
- Intune ei voi tehdä mitään ennen kuin laite käynnistyy uudelleen.
- Jos BIOS-asetus on "Power On After Power Loss", laite voi käynnistyä automaattisesti, ja yhteys pilveen palautuu.

◊ 3. Azure-palvelun häiriö

- Harvinaista, mutta mahdollista.
- Intune ja Entra ID voivat olla tilapäisesti poissa käytöstä.
- Laitteet toimivat edelleen paikallisesti, mutta uusia asetuksia ei voi puskea.

Pilvipohjainen hallinta (Entra ID + Intune) toimii kuin moderni, globaali versio Windows Serveristä – mutta se **riippuu verkkojohdeesta ja laitteen virrasta**. Katkokset eivät yleensä riko laitetta, mutta **estävä etähallinnan hetkellisesti**. Siksi on tärkeää suunnitella laitteet niin, että ne **toimivat itsenäisesti** myös offline-tilassa.

🌐 Miten varautua poikkeustilanteisiin?

Toimenpide	Hyöty
Offline-käytännöt	Laitteet toimivat ilman pilviyhteyttä, jos asetukset on ladattu etukäteen
BIOS-asetus: Power On After Power Loss	Automaattinen käynnistys sähkökatkon jälkeen
UPS-varavirtalähde	Pitää laitteja ja reittimien käynnissä lyhyissä katkokissa
Reitin, joka käynnistyy automaattisesti	Nettiyhde palautuu ilman manuaalista toimenpidettä
Intune-konfiguraatio: pitkä refresh cycle	Varmistaa, että laite ei menetä asetuksia lyhyen yhteyskatkon aikana

🔒 Pilvhallinnan etu vs. haaste

Pilvhallinta (Entra + Intune)	Fyysisen hallinta (Windows Server)
Skaalautuu helposti	Rajoittuu paikalliseen verkkoon
Etähallinta mistä tahansa	Vaatii VPN tai suoran yhteyden
Automaattiset käytännöt	Manuaalinen konfigurointi
Riippuvainen nettiyhdeestä	Toimii LAN:ssa ilman nettiä
Katkokset vaikuttavat etähallintaan	Katkokset vaikuttavat koko verkkoon

❖ Yhteenveto: Fyysisen vs. pilvipohjainen hallinta

Toisin sanoen molemmissa ratkaisuissa – fyysisessä Windows Server -ympäristössä ja pilvipohjaisessa Entra ID + Intune -mallissa – on omat hyvät ja huonot puolensa sekä poikkeustilanteensa. Valinta riippuu yrityksen palvelumallista ja siitä, miten laitteita aiotaan käyttää, hallita ja sijoittaa. Älä unohta tästä vaadittaan jopa lisensi kustannus hintaa riippuu onko kuukausittain vai vuosi lisensi.

Ratkaisuun vaikuttavat muun muassa:

- **Säilytsratkaisut ja fyysisen tila**
- **Ajankäyttö ja resurssit hallintaan**
- **Tarpeen laajuus ja laitteiden määrä**
- **Kokonaiskustannukset (laitteet, yhteydet, hallinta)**
- **Lisenssikustannukset**, jotka voivat olla kuukausi- tai vuosipohjaisia – tämä on tärkeä huomio erityisesti pilvipohjaisessa mallissa

Esimerkiksi yksi mainoslaiteratkaisu voi sisältää:

- 5G SIM-kortilla varustettu reitin
- Intel NUC tai muu pienikokoinen tietokone (Windows 10/11 tai Linux)
- Näyttö, mahdollinen koteloointi ja muut elektroniset johdot

Poikkeustilanteissa, kuten sähkö- tai verkkokatkoksissa, on tärkeää, että:

- **Laitteista kerätään lokitietoa**, jotta järjestelmänvalvoja tai IT-tuki voi seurata tapahtumia.
- **Automaattiset hälytykset** voidaan määrittää, esim. sähköpostiviesti: "Laitte XXXXX-12345 (Kaupunki) on offline."
- Sama pätee **varalaite** ja on valmiina hyllyllä esim. Laitte XXXXXX-12345 on viallinen, että toimistolta löytyy sille varalaite.

Tällainen valvonta ja reagointi mahdollistaa nopeamman vianmäärityksen ja paremman palvelun laadun – erityisesti, jos laitteita on hajautettu useisiin sijainteihin.

Tämä on malli ja jonkin ohje rakentamaan kuinka se toimisi jos rakentaa kiosk + Intune kanssa.

<https://www.joeyverlinden.com/entra-id-joined-kiosk-or-autologon-device-on-a-budget/>