

5.1.1. Win + GPO troubleshoots

Friday, October 24, 2025

17:02



Ongelmia Windows Serverin GPO-konfiguraatioiden kanssa

Tämä dokumentaatio koskee VM1-virtuaalikonetta, jossa toimii Windows Server ja Active Directory (AD). Palvelimella konfiguroidaan uusia ryhmäkäytäntöjä (GPO), kuten esimerkiksi:

- Käyttäjien pääsyn estäminen **Ohjauspaneeliin**
- Rajoitukset **asetusten muokkaamiseen**
- Käyttäjätointojen rajoittaminen työasemilla

Vaikka nämä asetukset voivat parantaa tietoturvaa ja hallittavuutta, **virheellisesti konfiguroidut GPO:t voivat aiheuttaa ongelmia**, kuten:

- Käyttäjät eivät pääse kirjautumaan työasemiin
- Työasemat eivät näy AD:ssa
- Palvelut eivät käynnisty normaalista
- Järjestelmä voi jopa kaataa (BSOD) tietyissä tilanteissa

Windows serverissä jos on mennyt pitkälle, mutta ensimmäisenä kantsii asettaa koskien snapshot ja jos siitä eteenpäin menee varmasti helpolla esim. GPO konfigurointia ja jne, että asennetun näiden policy asetuksien jälkeen kannattaa ottaa ensimmäisenä back up haltuun esim. Siirtämällä fyysisen työaseman.

Toinen vaihtoehtona powershell - josta voi suorittaa nopeasti backup (varmuuskopiointi)

★ Voiko GPO aiheuttaa bluescreenin?

Mahdollisesti, mutta vain tietyissä tilanteissa:



Riskialttiita GPO-asetuksia:

- Ajureihin tai laitteistoon liittyvät asetukset (esim. pakotettu ajurin asennus tai estäminen)
- Käynnistyskriptit (Startup Scripts), jotka jäävät jumiin tai aiheuttavat virheitä
- Tietoturva-asetukset, jotka estäävät järjestelmän normaalilin toiminnan (esim. oikeuksien poistaminen SYSTEM-tililtä)
- Pakotetut ohjelmat tai ohjelmistopäivitykset, jotka eivät ole yhteensopivia

Jos jokin näistä on konfiguroitu väärin, se voi aiheuttaa BSOD:n (Blue Screen of Death) tai jatkuvia uudelleenkäynnistyskiä.

Sama pätee vmworkstation kannattaa, joka kerta sulkea sen ja sammuttaa ohjelmansa ettei tule bluescroon. Jos jättää keskeneärisen ohjelmansa niin tulee ongelmia mm. bluescreen ja se ajuri suorittakin itsenäisen korjaksen mutta ongelmana pääseekö takaisin windows 10 (windows serverin) ympäristöön - se on suuri kysymys.

Mahdolliset syyt BSOD-virheisiin AD- ja GPO-ympäristössä

- **AD:n epäjohdonmukainen tila:** Jos Domain Controller (DC) sammutetaan ilman asianmukaista replikointia tai synkronointia, ja se käynnistetään myöhemmin, voi syntyä tilanne, jossa AD-tietokanta on vioittunut tai ristiriidassa muiden DC:iden kanssa. Tämä voi johtaa virheeseen kuten *STOP 0xc00002e2*, joka liittyy AD:n käynnistysongelmiin.
- **Palautus tai snapshotin käyttö:** Jos käytetään VM snapshotteja tai palautetaan DC edelliseen tilaan, voi syntyä ristiriitoja AD:n sisäisessä tilassa, mikä voi johtaa BSOD:iin tai muihin virheisiin

#####

Tarkistuslista GPO-muutosten jälkeen

Tämä koskien uusien GPO asetusta esim.

- Uusi pelisääntö
- on olemassa oleva sääntö, johon tehdään muutosta - niin näitä pitää suorittaa mahdolliset toimenpidettä.
- Testaa GPO asetusta esim. VM2 testikoneella ja jos on liittynyt yritysalueverkkon
- Suorita cmd komentoa
 - o Päivitystä (jos ei päivitetä menee normaalisti 90min tai jopa 30min) tämä pakottaa päivityksen samantien
 - \$gpupdate /force
 - o Tarkistus, mitkä käytännöt ovat oikeasti sovellettu
 - \$gpresult /h
 - Tai rsop.msc

- Varmista AD:n ja DNS:n eheys
 - Suorita \$dcdiag \$repladmin /replsummary , \$netdiag.
- SFC ja DISM -skannaukset (Windowsin eheys) - tämä tarkistaa ja korjaat vioittuneet järjestelmätiedostot
 - \$sfc /scannow
- DISM (Deployment Image Servicing and Management) - korjaat windowsin järjestelmäkuvan, jos SFC ei riitä.
 - \$DISM /Online /Cleanup-Image /RestoreHealth

VM1 - Windows serverin (AD) sulkeminen

Ei ole suositeltavaa sammuttaa Windows Server -virtuaalikonetta (varsinkin Domain Controlleria) suoraan "Power Off" -komennolla, etenkään heti GPO-muutosten jälkeen.

Miksi "Power Off" voi olla riskialtista

- AD:n tietokanta (**NTDS.dit**) voi olla kirjoitustilassa, ja suora virran katkaisu voi aiheuttaa vioittumista.
- GPO-muutokset voivat olla vielä soveltumassa tai replikoitumassa muihin DC:iin — keskeytys voi aiheuttaa ristiritoja.
- DNS- ja SYSVOL-jakojen tiedostot voivat jäädä lukituksi tai osittain kirjoitetuiksi.
- Event Viewer -lokit eivät ehdi tallentua kunnolla.
- VMWare Workstationin "Power Off" vastaa fyysisen koneen virtajohdon irrottamista — ei turvallinen tapa sammuttaa palvelin.
- Mahdollisia BSOD- tai käynnistysvirheitä seuraavalla bootilla

Turvallinen tapa sammuttaa Windows Server (AD)

1. Varmista, että GPO-muutokset on sovellettu
 - gpupdate /force
 - rsop.msc tai gpresult /h
2. Tarkista AD:n tila
 - dcdiag
 - repadmin /replsummary
3. Tarkista Event Vieweristä virheet
4. Sammuta palvelin normaalisti
 - Käytä Start > Shut down /s /t 0
 - Kaikki varmistaa kaikki palvelut (kuten Active Directory, DNS, DHCP) sulkeutuvat hallitusti
 - Käynnissä olevat prosessit ja kirjaukset päättyyvät oikein
 - Järjestelmätiedostot ja AD-tietokanta (NTDS.dit) tallentuvat turvallisesti
 - Ei jää lukittuja tiedostoja tai vioittuneita tiloja
5. Odota, että VM sammuu kokonaan ennen virtuaalialustan sulkemista

KOSKIEN "gpupdate /force"

Windowsin ryhmäkäytännön (Group Policy) päivitys

- Windows päivittää ryhmäkäytännöt automaattisesti **90 minuutin välein**, satunnaisella viiveellä **±30 minuuttia**.
- Jos ei jaksa odottaa automaattista päivitystä, voi pakottaa käytäntöjen päivityksen komentoriviltä:
 - **PowerShell / komentokehote:** gpupdate /force
- Tämä toimii sekä **palvelimella** että **työasemalla**, ja pakottaa kaikki käytännöt päivittymään heti.

Lyhyesti sanottuna:

- Uusi ja olemassa olevan policy säännöstää tee testi, suorita päivitystää
- Testaa vm1 (windows server) ja vm2 (käytti win10) kanssa ja jos pelittää
- Tarkista vianmääritykset (SFC ja DISM) järjestelmänkuvat
- Dokumentoi tarvittaessa
- Sulje käyttöliittymän windows ympäristön mukaan se ohjelma, älä sammuta vmworkstation kautta "power off"

#####
#####

Admin oikeus - vaikuttaa itsensä

GPO sääntöjen konfigurointi koskee jopa admin-yläpitäjää itsensä, koska oletuksena konffauksen jälkeen tulee "authenticated users".

- "Authenticated Users" tarkoittaa kaikkia käyttäjiä, jotka voivat kirjautua sisään ja joilla on tunnistetut käyttöoikeudet — ja tämä sisältää myös järjestelmänvalvojat (admin-käyttäjät).

Ryhmä

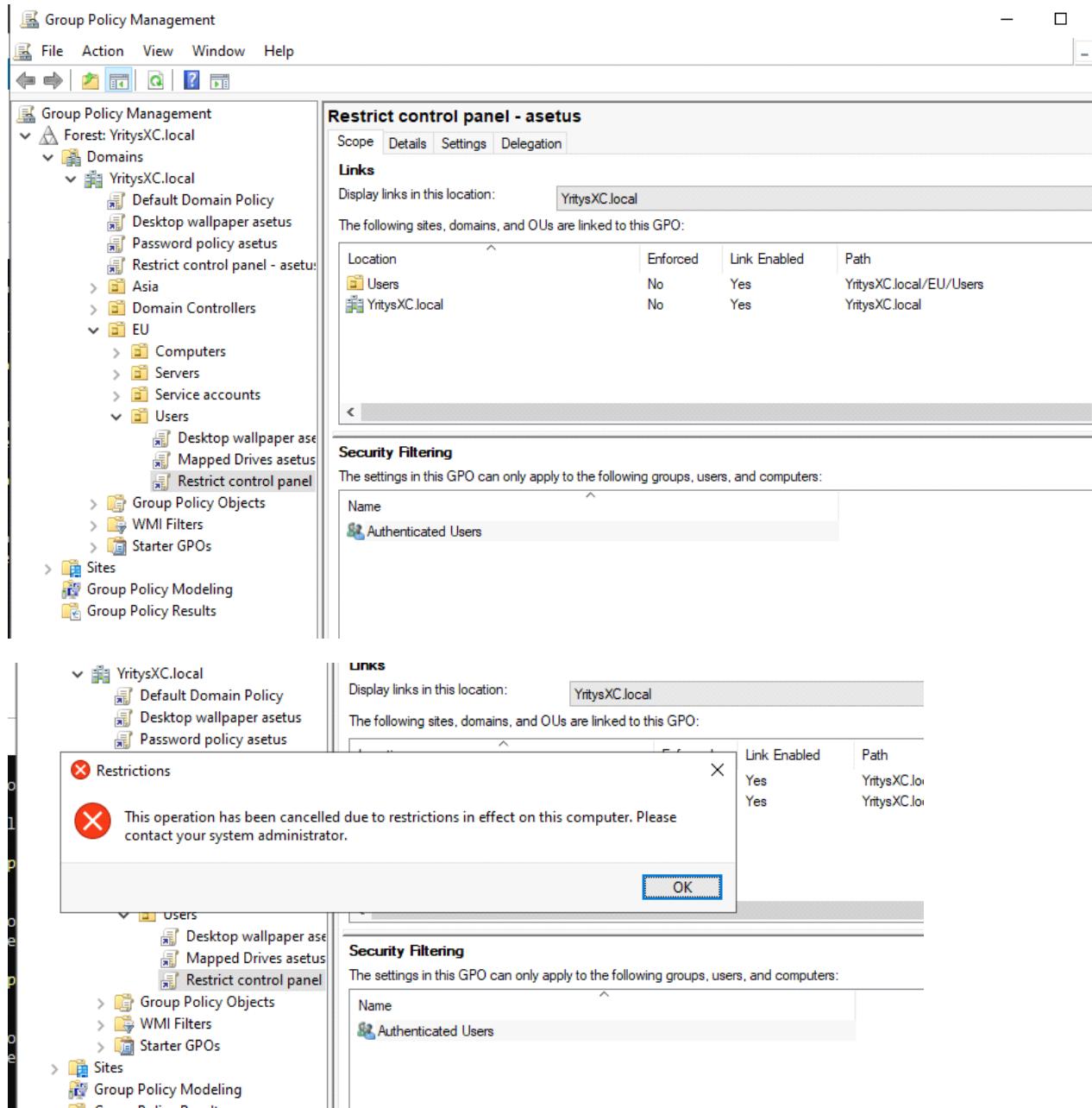
Sisältää

Authenticated Users Kaikki käyttäjät, jotka ovat kirjautuneet sisään — mukaan lukien **adminit, domain users, service accounts**, jne.

Domain Users Vain tavalliset käyttäjät, jotka kuuluvat domainiin

Administrators Vain admin-käyttäjät tai ryhmät, joilla on admin-oikeudet

Esim. Tästä aikaisempi/yksi videoista on konfiguroitu "control panel" estämisen eli ohjauspaneelin. Tässä oletuksena estettää jopa admin itsensä. Tätä on testattu, että tulee se error eli..



Miten tästä korjataan, että vain käyttäjille esim. Yksikköiden tiimi jäsenille, eikä admin käyttäjälle.

Määritettää esim. EU yksikköiden jäsenille, että vain HE eivät saa avata ohjauspaneelia, ja **EU-tiimiin** sisältyy kaikki nämä jäsenen nimet.

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [YritysXC.local]

Name	Type	Description
Alex Applicant	User	
EU-Tiimi	Security Group...	
Jamie Johnson	User	
Jane Simple	User	
John Doe	User	S€rc3ts
Johnny Smith	User	
Mary Major	User	
Pat Person	User	
Team1	Security Group...	
Team2	Security Group...	
User name	User	punajuuriKeitto123

EU-Tiimi Properties

General Members Member Of Managed By

Members:

Name	Active Directory Domain Services Folder
Alex Applicant	YritysXC.local/EU/Users
Jamie Johnson	YritysXC.local/EU/Users
Jane Simple	YritysXC.local/EU/Users
John Doe	YritysXC.local/EU/Users
Johnny Smith	YritysXC.local/EU/Users
Mary Major	YritysXC.local/EU/Users
Pat Person	YritysXC.local/EU/Users
User name	YritysXC.local/EU/Users

Takaisin "restrict control panel- asetus" josta otettaan tämä "security filtering" osuuus:

- Poista "authenticated users" ja korvaa tilalle "EU-tiimi"

BEFORE:

Group Policy Management

Forest: YritysXC.local

Domains

YritysXC.local

- Default Domain Policy
- Desktop wallpaper asetus
- Password policy asetus
- Restrict control panel - asetus
- Asia
- Domain Controllers
- EU

 - Computers
 - Servers
 - Service accounts
 - Users

 - Desktop wallpaper asetus
 - Mapped Drives asetus
 - Restrict control panel

- Group Policy Objects
- WMI Filters
- Starter GPOs

Sites

Group Policy Modeling

Group Policy Results

Restrict control panel - asetus

Scope Details Settings Delegation

Links

Display links in this location: YritysXC.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
Users	No	Yes	YritysXC.local/EU/User
YritysXC.local	No	Yes	YritysXC.local

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

Add... Remove Properties

WMI Filtering

This GPO is linked to the following WMI filter:

After:

- Näin, sekä tuosta kaksoisklikkaus voi tarkistaa ketä EU\users jäseniä niihin kuuluu.

Lisätyn EU-tiimin jälkeen muista päivittää powershell komennolla \$gpupdate /force
 - Tämän jälkeen testaa ja toimiiko, sekä suorita sfc scannow

MINIYHTEENVETO TÄHÄN

Periaatteessa joka kerta kun konfiguroi uuden tai muokkaa olemassa olevan GPO asetuksensa, on hyvä poistaa "authenticated users" - koska tämä koskee Windows server ylläpitäjän itsensäkin ettei vain käyttäjää. Harjoituksen kannalta tämä on hyvä, mutta jos tosi elämässä voi olla erikseen pitää asettaa admin käyttäjä, tai tietty erikseen tiimien esihenkilö oikeus taso, jonka kautta voi hallinnoida oman tiimien oikeuksia ja ei tarvitse joka kerta kysyä adminilta apua.

- "Authenticated Users" ei tarkoita vain tavallisia käyttäjiä — se kattaa **kaikki tunnistetut käyttäjät**, myös adminit

Mitä voit oppia tästä?

- 1. GPO:n kohdistus on yhtä tärkeä kuin sen sisältö**
 - GPO voi tehdä mitä tahansa — mutta **kenelle se kohdistuu**, ratkaisee lopputuloksen
 - **Security Filtering** ja **OU-rakenne** ovat avainasemassa
- 2. Ryhmäperusteinen hallinta on joustava ja skaalautuva**
 - Käytämällä ryhtiä kuten EU-tiimi, voit hallita satoja käyttäjiä yhdellä GPO:lla
 - Voit helposti lisätä tai poistaa käyttäjiä ilman GPO:n muokkaamista
- 3. Admin-käyttäjät tarvitsevat erillistä käsittelyä**
 - Adminit voivat joutua GPO:n vaikutukseen alle, ellei heitä rajata pois
 - Tämä on tärkeää, jotta ylläpito ei esty vahingossa
- 4. GPO-ongelmat voivat näkyä yllättäväissä muodoissa**
 - Esimerkksi: Control Panel ei avaudu, vaikka olet admin
 - Ongelma ei ole tekninen vika, vaan **hallintapolitiikan vaikutus**

#####

Toinen troubleshoots - kysyy joka kerta admin tunnuksen

Tämä on koskien joka kerta VM2 (windows 10/11) työasemalla esim. Avatessa verkkoasetuksensa tai powershell tai muu tietty asetus - niin ponnahtaa harmaa ilmoitus ja kysyy yritysalueverkon ylläpitäjän tunnusta ja salasanaa. Tämä on kuin pienestä asetuksista pitää joka kerta kysyy admin - niin se ärsyttää ja jos käyttäjä kiinnostaa tia haluaa tehdä jotakin tarkistusta se on tosi normaalista.

TTämä voi johtua useista GPO-asetuksista/säännöstä esim. Luoneen yhen tai muutamaista keskeisistä säännöstä. Koska aiheuttamisen, että tavallinen käyttäjä ei voi tehdä tiettyä muutoksia ilman admin-tunnusta.

Mistä nämä rajoitukset voivat tulla GPO:ssa?

◊ 1. UAC (User Account Control) -asetukset

- GPO voi määrittää, että **jopa admin-käyttäjältä vaaditaan vahvistus** ennen kuin järjestelmänvalvojan oikeuksia käytetään.
- Tämä vaikuttaa PowerShellin ja Ohjauspaneelin toimintaan.

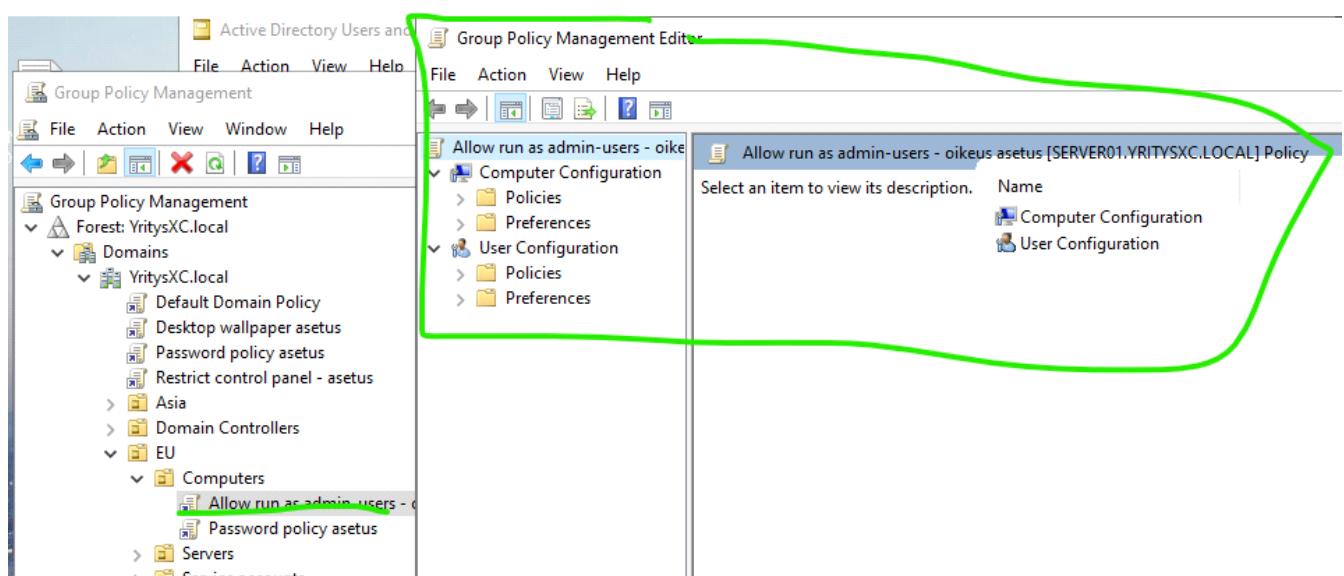
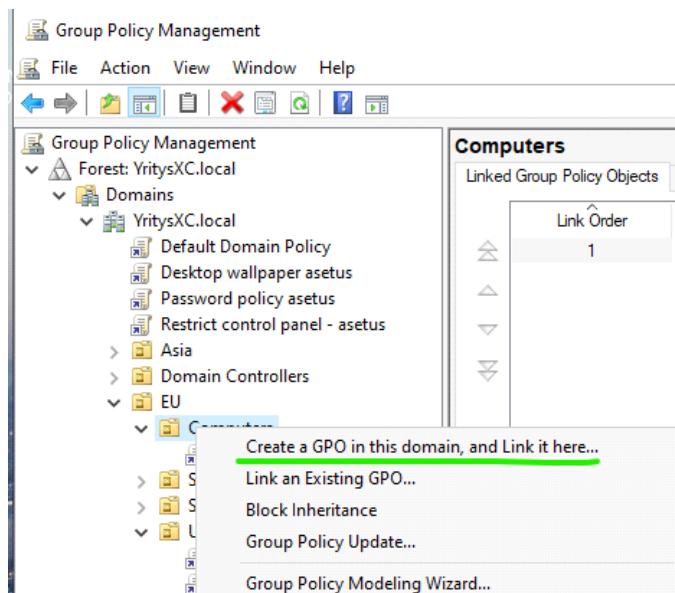
◊ 2. Verkkoasetusten rajoitukset

- GPO voi estää pääsyn verkkoasetuksiin:
 - User Configuration > Administrative Templates > Network > Network Connections
 - Esim. "**Prohibit access to properties of a LAN connection**"
 - "**Prohibit TCP/IP advanced configuration**"

◊ 3. Sovellusten estot (AppLocker / SRP)

- Vaikka et ole itse määrittänyt, domainin Default Domain Policy tai muu GPO voi sisältää:
 - AppLocker-säännön, joka estää powershell.exe
 - Software Restriction Policy, joka rajoittaa sovellusten käyttöä

HUOMOINA Tämä on seurattu ja haettu youtube videon kautta:



Seuraavaan polkuun:

Computer configuration >> policies >> windows settings >> security settings >> local policies >> security options

Allow run as admin-users - oikeus asetus [SERV]		Policy	Policy Setting
Computer Configuration		Network security: Minimum session security for NTLM SSP ...	Not Defined
Policies		Network security: Minimum session security for NTLM SSP ...	Not Defined
Software Settings		Network security: Restrict NTLM: Add remote server exceptio...	Not Defined
Windows Settings		Network security: Restrict NTLM: Add server exceptions in t...	Not Defined
Name Resolution Policy		Network security: Restrict NTLM: Audit Incoming NTLM Traf...	Not Defined
Scripts (Startup/Shutdown)		Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Security Settings		Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Account Policies		Network security: Restrict NTLM: NTLM authentication in thi...	Not Defined
Local Policies		Network security: Restrict NTLM: Outgoing NTLM traffic to ...	Not Defined
Audit Policy		Recovery console: Allow automatic administrative logon	Not Defined
User Rights Assignment		Recovery console: Allow floppy copy and access to all drives...	Not Defined
Security Options		Shutdown: Allow system to be shut down without having to...	Not Defined
Event Log		Shutdown: Clear virtual memory pagefile	Not Defined
Restricted Groups		System cryptography: Force strong key protection for user k...	Not Defined
System Services		System cryptography: Use FIPS compliant algorithms for en...	Not Defined
Registry		System objects: Require case insensitivity for non-Windows ...	Not Defined
File System		System objects: Strengthen default permissions of internal s...	Not Defined
Wired Network (IEEE 802.3) P...		System settings: Optional subsystems	Not Defined
Windows Defender Firewall w...		System settings: Use Certificate Rules on Windows Executab...	Not Defined
Network List Manager Policies		User Account Control: Admin Approval Mode for the Built-...	Not Defined
Wireless Network (IEEE 802.11)		User Account Control: Allow UIAccess applications to prom...	Not Defined
Public Key Policies		User Account Control: Behavior of the elevation prompt for ...	Not Defined
Software Restriction Policies		User Account Control: Behavior of the elevation prompt for ...	Not Defined
Application Control Policies		User Account Control: Detect application installations and p...	Not Defined
IP Security Policies on Active		User Account Control: Only elevate executables that are sig...	Not Defined
Advanced Audit Policy Config...		User Account Control: Only elevate UIAccess applications th...	Not Defined
Policy-based QoS		User Account Control: Run all administrators in Admin Appr...	Not Defined
Administrative Templates: Policy def...		User Account Control: Switch to the secure desktop when pr...	Not Defined
Preferences		User Account Control: Virtualize file and registry write failure...	Not Defined
User Configuration			

Sitten valitse toinen kenttä , aseta define this policy päälle ja "enabled" - APPLY ja OK

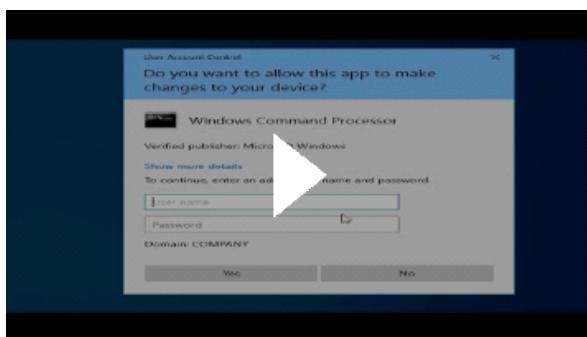
	Policy Setting
User Account Control: Run all administrators in Admin Approval Mode	Not Defined
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Not Defined
User Account Control: Switch to the secure desktop when prompting for elevation	Not Defined
User Account Control: Virtualize file and registry write failures to per-user locations	Not Defined

Samasta windows serveristä päivitä gpupdate /force ja suorita vianmäärityskien skannaukset

Aava VM2 (windows 10/11) jos on käynnissä niin buuttaa työasema varmuuden vuoksi ja testataan

- Avaa normi powershell/cmd toimii
 - o Jos avaa normin powershell/cmd admin kautta niin pitää pyytää admin-tunnuksensa
- Avataan normi verkkoasetukset ja kokeillaan avata esim. Muokkattaisiin IPV4 DNS IP-osoite
 - o Pyytää yhä admin oikeudet

[How To Allow Domain User Run Program AS Administrator Rights Using Group Policy Windows Server 2019](#)



#####

Paljon GPO sääntöjä ja ne pois päältä (Disabled)

GPO säännöstää vaikka pitäisi kaikkia 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 parasta asettaa pois päältä , koska tämän vuoksi voi joutua tarkistaa niitä sääntöjä koskeeko se työasemaa vai käyttäjän konfigurointia että onko policy sääntö vai suositus.
- Säännöstää kannattaa testata yksittelen ja asettaa ne pois päältä, ja pätee määrityn kohdistuuko se YKSIKKÖ-RYHMÄÄN ja tuotantoypäristöön.

GPO säätöjen muokkaus/päivitystä/testausta tai muu teknisen toimesta, josta pitää ehdottomasti dokumentoida ja kertoa käyttäjille. Koska jokaisen pien muutoksen/päivitystä voi vaikuttaa työntekijään ja useimmin se on järjestelmänvalvoja takana kuka suorittaa näitä teknisten toimenpidettä.

- Käyttäjän näkökulmalta voi koskea heitä, koska GPO säännot koskee jokaista konetta tai tilinsä ja käyttäjä voi itse tarkistaa PowerShell komennolla "\$gpresult /R" - Tämä komento näyttää **aktiiviset GPO:t** ja niiden vaikutusalueet (käyttäjä/kone).
 - o On hyvä käytäntö tarjota käyttäjille **ohjeet tai tukikanava**, jos he kohtaavat muutoksen vaikutuksia (esim. estetty ohjauspaneeli, puuttuva verkkolevy, muuttunut salasana-politiikka).

❖ **GPO:n soveltamisjärjestys (tärkeä!)**

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**

▀ **Mitkä GPO:t ovat olennaisia yrityksille?**

Riippumatta koosta, seuraavat GPO:t ovat yleisesti suositeltuja:

🔒 **Tietoturva**

- Salasana-politiikka (pituus, vanheneminen, monimutkaisuus)
- Käyttäjätieni lukituspolitiikka
- USB-laitteiden esto (jos tarpeen)
- Windows Defender / virustorjunta-asetukset

💻 **Käyttöympäristön hallinta**

- Ohjauspaneelin ja asetusten esto tavallisilta käyttäjiltä
- Automaattiset päivitykset ja uudelleenkäynnistykset
- Kirjautumisviestit (esim. tietoturvavaroitus)

📁 **Verkkolevyjen ja resurssien hallinta**

- Mapped drives (käyttäjäkohtaiset tai ryhmäkohtaiset)
- Tulostimien määritys
- Folder redirection (esim. Desktop, Documents)

✳️ **Käyttäjäkokemuksen optimointi**

- Start-menun ja tehtäväpalkin mukautus
- Sovellusten esto (esim. pelit, selaimet)
- Skriptit kirjautumiseen / uloskirjautumiseen

▀ **Kuinka monta GPO:ta yrityksissä yleensä on?**

GPO-määrä ei riipu pelkästään henkilöstön määrästä, vaan myös **IT-infrastruktuurin monimutkaisuudesta, tietoturvavaatimuksista ja hallintamallista**. Tässä kuitenkin suuntaa-antava arvio:

Yrityksen koko **Tyypillinen GPO-määrä** **Huomioita**

Alle 100 hlö	10–30 GPO:ta	Yleensä peruspolitiikat: salasana, levyjako, päivitykset, estoasetukset
Noin 100 hlö	30–60 GPO:ta	Alkaa tulla roolipohjaisia sääntöjä, esim. eri GPO:t asiantuntijoille ja myyynille
Yli 100 hlö	60–200+ GPO:ta	Käytössä usein OU-rakenne, ryhmäkohtaiset GPO:t, WMI-suodattimet, delegointi

⌚ **Tärkeämpää kuin määrä on rakenne ja hallittavuus:** hyvin suunniteltu 40 GPO:ta voi olla tehokkaampi kuin sekava 100 GPO:n kokonaisuus.