Windows videot: <https://www.youtube.com/playlist?list=PLZw_fXxI6L51dB6hD03-MAX8cBc7FqR6l>

Contents

[Mitä ryhmäkäytännöt ovat? 2](#_Toc184028397)

[Ryhmäkäytäntöjä 2](#_Toc184028398)

[Organisaatioyksiköt ja ryhmäkäytännöt 2](#_Toc184028399)

[Mistä ja miten ryhmäkäytäntöjä tehdään? 3](#_Toc184028400)

[Miten löydän halutun ryhmäkäytännön? 4](#_Toc184028401)

[Hyvät käytänteet ryhmäkäytännöistä 5](#_Toc184028402)

[Computer vs User configuration 6](#_Toc184028403)

[Kotisivut: 6](#_Toc184028404)

[Etätyöpöytäyhteydet: 6](#_Toc184028405)

[Etätyöpöytäyhteyden salliminen palomuurin läpi: 6](#_Toc184028406)

[Remote PowerShell 7](#_Toc184028407)

[Remote Powershell IP rajoittaminen 10](#_Toc184028408)

[Päivitysten automaattinen asennus: 11](#_Toc184028409)

[Kirjautumisyritysten valvonta: 12](#_Toc184028410)

[Ohjauspaneeli pois käytöstä: 12](#_Toc184028411)

[CMD/Powershell pois käytöstä: 13](#_Toc184028412)

[Estä edellisen käyttäjän näkyminen kirjautumisikkunassa: 13](#_Toc184028413)

[Kansioiden uudelleenohjaukset: 13](#_Toc184028414)

[Tervetuloa teksti ennen kirjautumista 14](#_Toc184028415)

[Ohjelman asennus ryhmäkäytäntöjen kautta 14](#_Toc184028416)

[Published asennus 15](#_Toc184028417)

[Assigned asennus 16](#_Toc184028418)

[Vianselvitys 17](#_Toc184028419)

[Liikkuva profiili ja kotihakemistojen oikeudet 19](#_Toc184028420)

[Verkkojaon teko 21](#_Toc184028421)

[Security Filtering 22](#_Toc184028422)

[Esimerkki Security Filtering käytöstä 24](#_Toc184028423)

[Varmuuskopionti 26](#_Toc184028424)

[Central Store 27](#_Toc184028425)

# Mitä ryhmäkäytännöt ovat?

**Ryhmäkäytännöillä saadaan tehtyä haluttuja asetuksia monille käyttäjille/tietokoneille keskitetysti**. Jos haluat esimerkiksi vaihtaa 200 tietokoneen taustakuvaksi kissakuvan, saat hoidettua sen ryhmäkäytännöillä eikä sinun tarvitse mennä jokaiselle koneelle erikseen sitä vaihtamaan. Ryhmäkäytäntöjä on tuhansittain joten niiden avulla pystyt tekemään lähes mitä tahansa asetuksia.

# Ryhmäkäytäntöjä

Ryhmäkäytännöt voi pakottaa päivittymään komennolla:

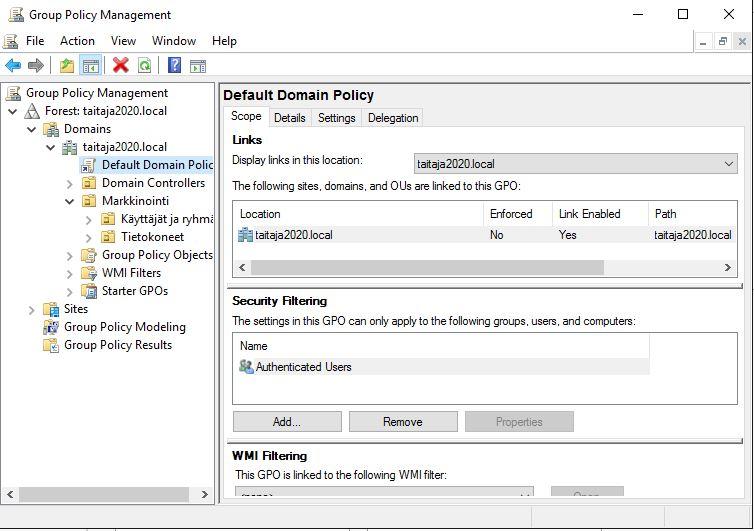
**gpupdate /force**

Suorita kyseinen komento työasemalla ja palvelimella.

Tähän on kerätty lista yleisimmistä ryhmäkäytännöistä ja miten ryhmäkäytäntöjä tehdään.

Ryhmäkäytäntöjä tehdään toimialuepalvelimen Group Policy Management ohjelmalla. Se näyttää seuraavalta. Ensimmäinen tärkeä asia on tämä: **Älä tee Default Domain Policyyn muita muutoksia, kuin salasanoihin liittyviä asetuksia.**

Jos muokkaat Default Domain Policya ja teet sinne huonoja asetuksia, voit mahdollisesti lukita itsesi ulos toimialuepalvelimesta ja tämä on äärimmäisen huono asia.

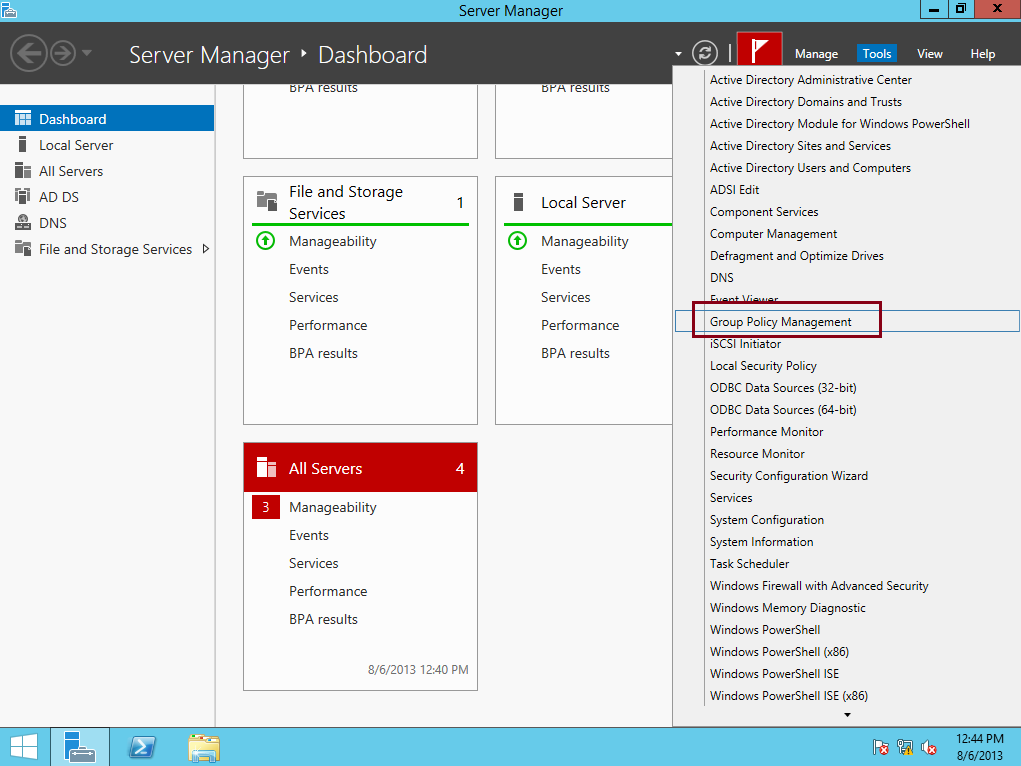


# Organisaatioyksiköt ja ryhmäkäytännöt

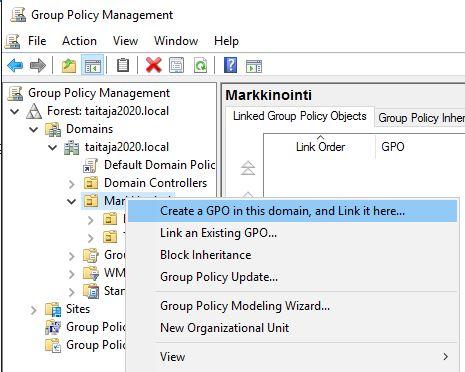
Ryhmäkäytäntöjä varten toimialueessa on eri organisaatioyksiköitä. Käytäntöjä tehdään niille. Tämän takia hyvä organisaatiorakenne on tärkeä! Ryhmäkäytäntö koskee vain niitä käyttäjiä/tietokoneita, jotka ovat kyseisen organisaatioyksikön alla.

# Mistä ja miten ryhmäkäytäntöjä tehdään?

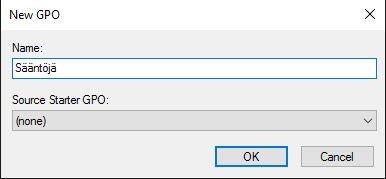
Avaa Server Manager -> Group Policy Management



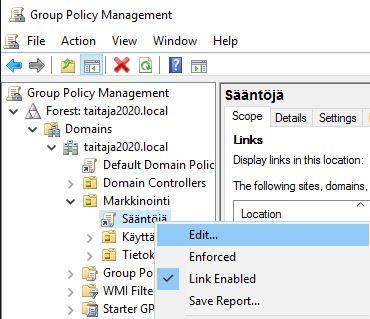
Group Policy Management alla voit luoda uuden ryhmäkäytäntöobjektin (GPO) suoraan jonkin organisaatioyksikön alle. Joissain tapauksissa muokataan suoraan Default Domain Policya.



Anna uudelle ryhmäkäytäntö objektille jokin nimi. Käytä nimeä, joka kuvaa sääntöä hyvin. Esimerkiksi: Block Control Panel tai Add printer.



Itse ryhmäkäytäntöjä pääsee tekemään valitsemalla Edit…



Edit… kautta aukeaa samanlainen ryhmäkäytäntöeditori, jota olet käyttänyt yksittäistä konetta hallitessasi aikaisemmin opinnoissa.

Erilaisia ryhmäkäytäntöjä käsitellään seuraavilla sivuilla.

Jokaiselle ryhmäkäytännölle on hyvä tehdä oma objektinsa (eli New GPO), näin ne pysyvät helposti järjestyksessä.

# Miten löydän halutun ryhmäkäytännön?

Valitettavasti GPO ei ole hakutoimintoa. Paras keino löytää ryhmäkäytäntö on hyödyntää hakupalveluita tai tekoälyä. Esimerkksi hakusanoilla: ”GPO how to block command prompt”

Löytyy hyvin vastauksia siihen, mistä polusta kyseinen ryhmäkäytäntö löytyisi. Tähän löytyi esimerkiksi tällainen vastaus ja polku:

A screenshot of a computer

Description automatically generated

## Hyvät käytänteet ryhmäkäytännöistä

Hyvä käytänne on, että jokaiselle säännölle tehdään oma ryhmäkäytäntöobjekti (GPO), jotta niiden hallinta on helpompaa ja selkeämpää. Esimerkiksi tässä on oma sääntö seuraaville:

* Disable Sign-in Animation, jolla otetaan pois käytöstä ensimmäisen kirjautumisen Hi animaatio
* Livinroom Printer, jolla lisätään käyttäjille tulostin
* Remote Desktop, jolla mahdollistetaan etätyöpöytäyhteys
* Remote Powershell, jolla mahdollistetaan etä Powershell yhteys

A screenshot of a computer

Description automatically generated

Lisäksi ryhmäkäytännöille voidaan lisätä kommentit, joissa kerrotaan mikä ryhmäkäytännön tarkoitus on eli miksi se on tehty.

A screenshot of a computer

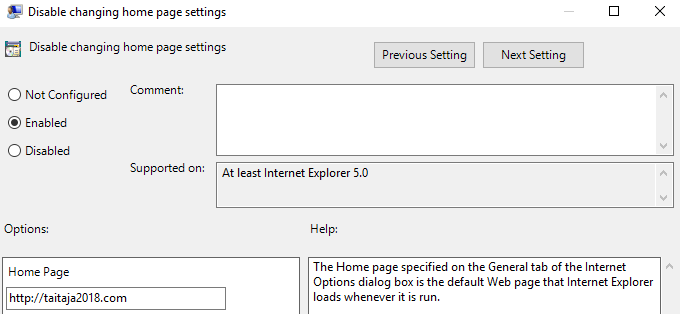
Description automatically generated

## Computer vs User configuration

**On olemassa kahdenlaisia ryhmäkäytäntöjä. Computer Configuration alla olevat ryhmäkäytännöt vaikuttavat vain TIETOKONEISIIN, jotka ovat kyseisen organisaation alla. User Configuration alla olevat ryhmäkäytännöt vaikuttavat vain KÄYTTÄJIIN, jotka ovat kyseisen organisaation alla.**

## Kotisivut:

User Configuration -> Policies -> Administrative Templates -> Windows Components -> Internet Explorer -> Disable changing home page settings.

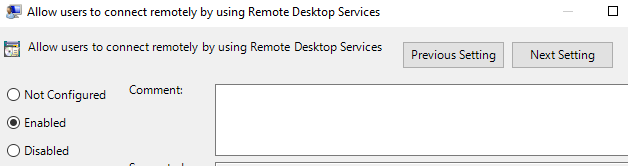


Huom. Tämä muuttaa vain IE selaimen kotisivua. Jos haluat muuttaa Firefox/Chrome kotisivua joudut latailemaan lisäohjelmia tai lisäosia. Firefox ohjeita: <https://support.mozilla.org/en-US/kb/customizing-firefox-using-group-policy>

## Etätyöpöytäyhteydet:

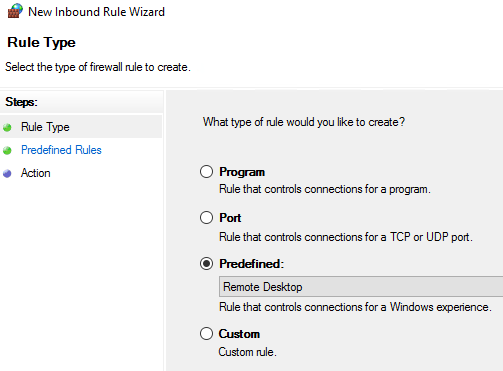
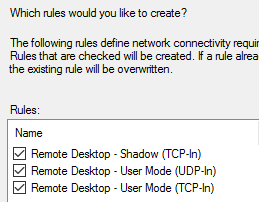
Tämä vaatii kahden eri säännön tekemistä. Etätyöpöytäyhteyden käyttöönotto:

Computer Configuration – Administrative Templates – Windows Components – Remote Desktop Services – Remote Desktop Session Host – Connections - Allow users to connect remotely using Remote Desktop Services



### Etätyöpöytäyhteyden salliminen palomuurin läpi:

Computer configuration -> Windows settings -> Security Settings -> Windows Firewall -> Windows Firewall -> Inbound rules. Tee uusi sääntö, valitse Predefined ja Remote Desktop. Seuraavassa ikkunassa valitse kaikki kolme vaihtoehtoa.

Jos haluat sallia Remote Desktop yhteyden esimerkiksi vain yhdestä IP-osoitteesta. Sinun tulee asettaa se näihin kolmeen palomuuri sääntöön niiden Scope asetuksesta. [Tästä esimerkkiin joka tehtiin Remote Powershelliin.](#_heading=h.30j0zll)

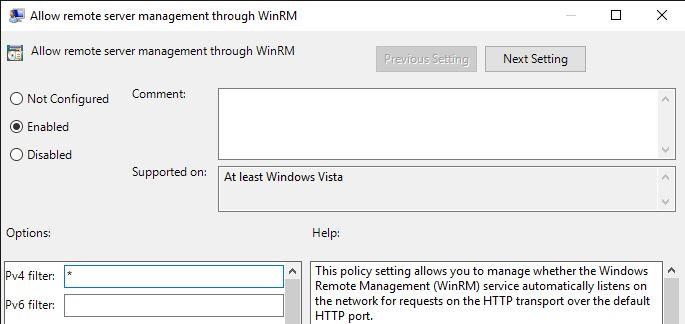
## Remote PowerShell

**Tehnyt: Aleksi Sievälä**

Remote PowerShell ominaisuudella voidaan ottaa etänä powershell yhteys tietokoneisiin, joita sääntö koskee. Tämän toimimaan saanti vaatii useiden eri ryhmäkäytäntöjen asettamisen.

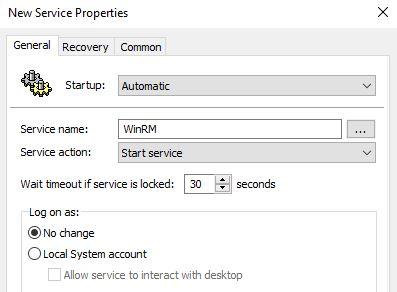
**Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service > Allow remote server management through WinRM.**

Tähti \* merkillä voidaan määrittää että etäyhteys voidaan ottaa mistä tahansa osoitteesta.

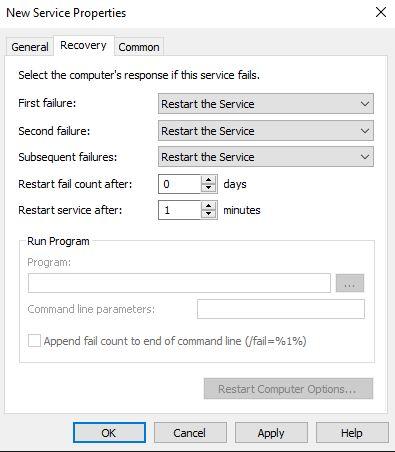
****

Seuraavassa säännössä asetetaan WinRM palvelu käynnistymään automaattisesti tietokoneen käynnistyksen yhteydessä.

**Computer Configuration > Policies > Preferences > Control Panel Settings** **> Klikkaa hiiren oikealla > New > Service > Käytä kuvan mukaisia asetuksia.**

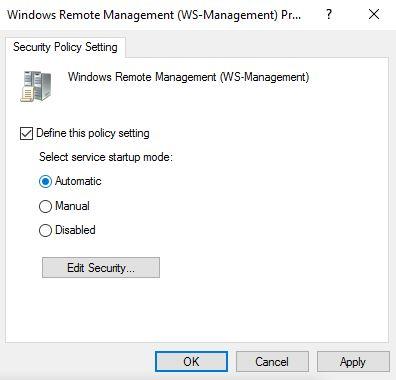
****

Recovery välilehdellä käytä seuraavia asetuksia.

****

Asetetaan WinRM käynnistymään automaattisesti.

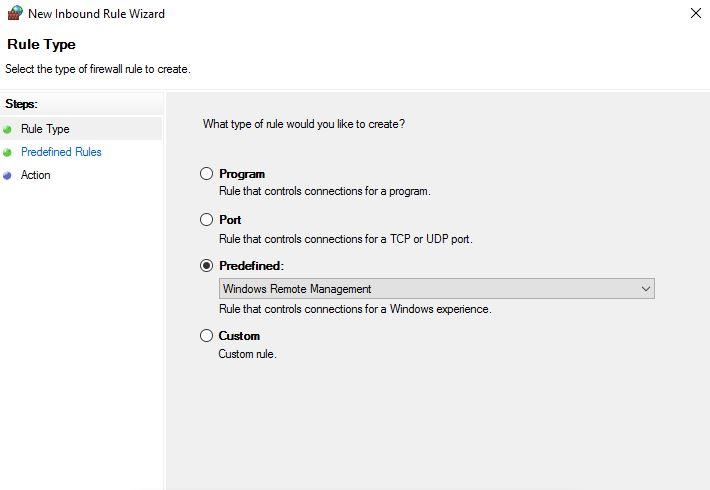
**Computer Configuration > Windows Settings > Security Settings > System Services > Windows Remote Management (WS-Management) > Define this policy setting > Automatic**



Joudutaan myös sallimaan WinRM etäyhetys palomuurista.

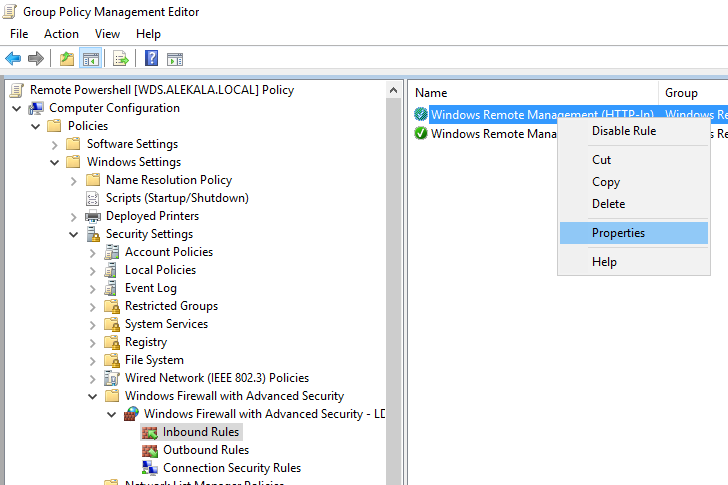
**Computer Configuration > Policies > Security Settings > Windows Firewall with Advanced Security > Inbound Rules > New Rule… > Predefined: Windows Remote Management.**

Salli tämä yhteys.



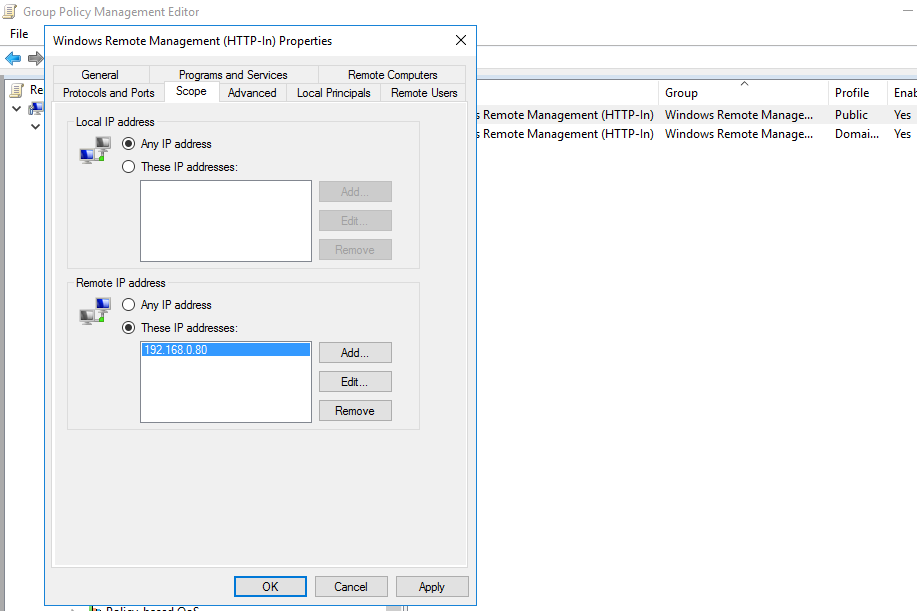
Tämän jälkeen Remote Powershell yhteys voidaan ottaa määritettyihin työasemiin. Yhteyden voi kuitenkin ottaa mikä tahansa palvelin, joten rajoitetaan yhteys vain yhteen palvelimeen juuri asettamastamme palomuurisäännöstä:

**Tee tämä seuraava prosessi kumpaankin alla olevaan kahteen sääntöön!**



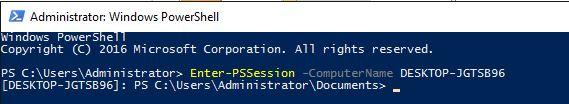
### Remote Powershell IP rajoittaminen

Tässä alla olevassa esimerkissä Remote Powershell yhteys on mahdollistaa otaa vain osoitteesta 192.168.0.80.

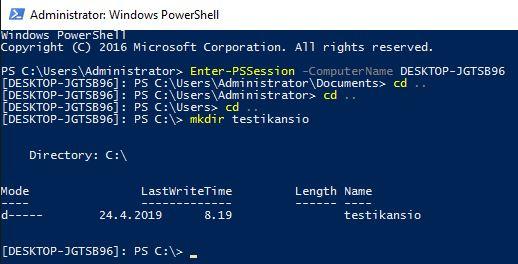


Näillä neljällä ryhmäkäytännöllä saadaan Remote Powershell toimimaan työasemissa, joita käytännöt koskevat. Ennen testausta käynnistä työasema uudestaan.

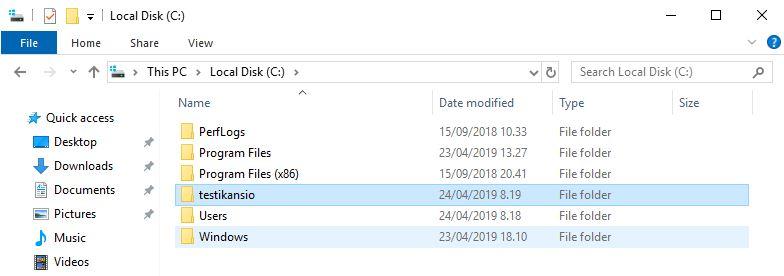
Remote PowerShell yhteys muodostetaan seuraavasti. Tässä tapauksessa työaseman nimi on DESKTOP-JGTSB96.



Testinä tehdään työaseman C:\ juureen kansio nimeltään testikansio.



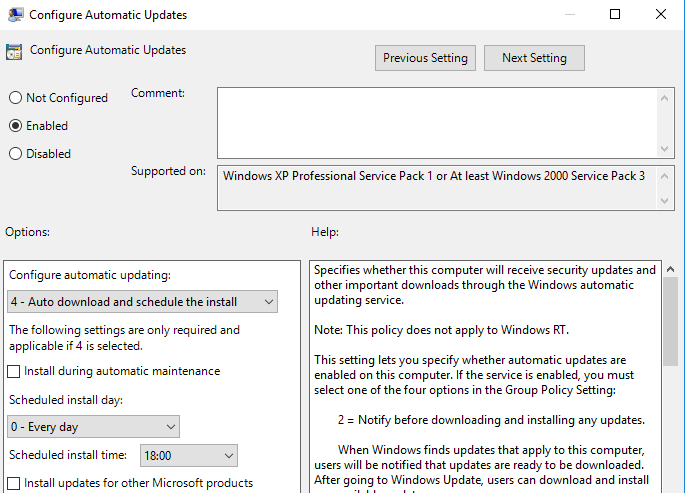
Kirjautumalla työasemalle voidaan vielä tarkistaa että kansio tuli luotua.



## Päivitysten automaattinen asennus:

Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Update > Configure Automatic Updates

Valitse sitten tarkempi asetus (2-5) ja mihin kellonaikaan ja mina päivinä haluat että päivitykset asennetaan ja tarkistetaan.

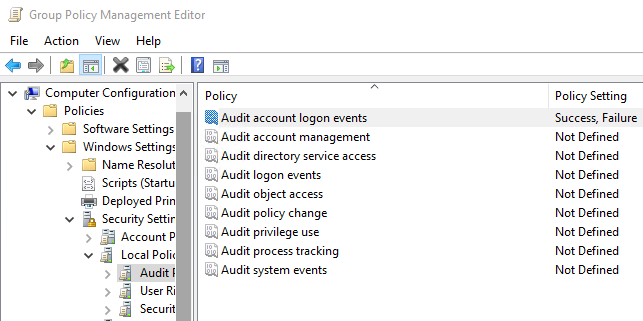


## Kirjautumisyritysten valvonta:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit account logon events.

Varmuuden vuoksi voi laittaa päälle myös säännön Audit logon events, joka löytyy samasta polusta.

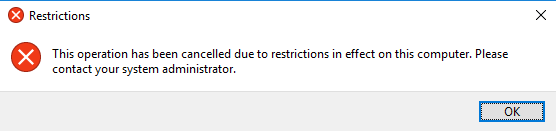
Laita päälle molemmat Success ja Failure



## Ohjauspaneeli pois käytöstä:

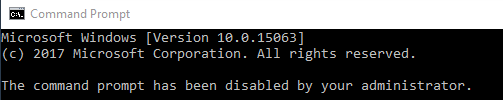
User Configuration -> Administrative Templates -> Control Panel -> Prohibit access to Control Panel and PC settings. Aseta Enabled.

Kohteessa se näyttää tältä:

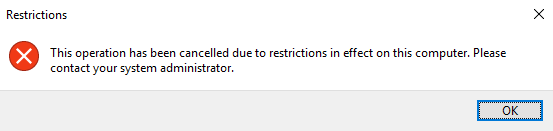


## CMD/Powershell pois käytöstä:

User Configuration -> Administrative Templates -> System -> Prevent access to the command prompt.



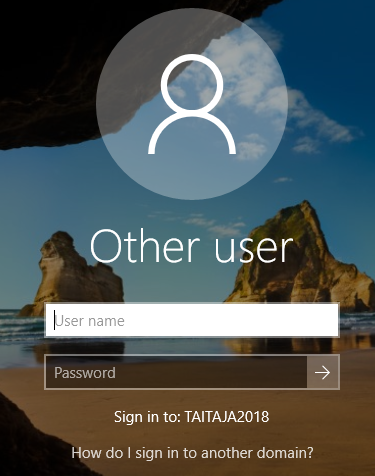
User Configuration > Administrative Templates > System > Don’t run specified Windows applications. Lisää powershell.exe.



## Estä edellisen käyttäjän näkyminen kirjautumisikkunassa:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name. Aseta enabled.

Tämä on ns. Classic login. Kirjautumisikkunasta tulee kuvan näköinen, eli siitä ei näe edellistä kirjautujaa.



## Kansioiden uudelleenohjaukset:

Kansioita voi uudelleenohjata seuraavasta paikasta:

User Configuration/Policies/Windows Settings/Folder Redirection/

Valitse mitä kansiota haluat uudelleenohjata. Voit esim. Määrittää että Pictures kansio uudelleenohjataan käyttäjän kotikansioon.

## Tervetuloa teksti ennen kirjautumista

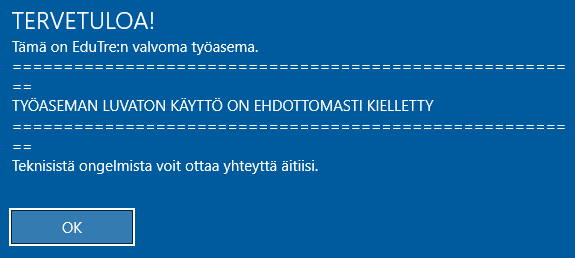
Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies

Interactive logon: Message text for users attempting to log on

Interactive logon: Message title for users attempting to log on

Molemmat Text ja Title tulee olla käytössä ja niissä tekstiä.

Se voisi näyttää esim. tältä:

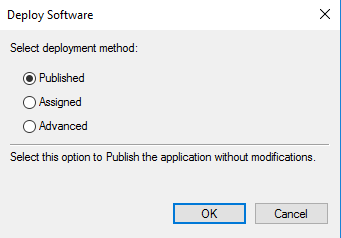


## Ohjelman asennus ryhmäkäytäntöjen kautta

Aluksi varmista, että asennuspaketit ovat .msi muodossa ja ne ovat palvelimella jaossa niin, että työasemat ja niiden käyttäjät pääsevät niihin käsiksi. Eli oikeudet ovat kunnossa jne. Jaot voisivat olla esim. Polussa \\wsrv1\GPOjako . Tässä polussa voisi sitten olla asennuspaketti Firefoxille ja 7zipille.

Sovellusten asentamiseen GPO kautta on muutama eri vaihtoehto. Kaikki vaihtoehdot ovat käytettävissä jos GPO on tehty User Configuration asetuksille. Computer Configuration käytössä on vain Assigned ja Advanced.

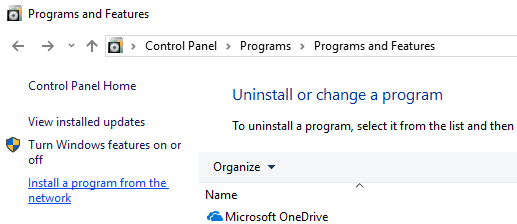
### Published asennus

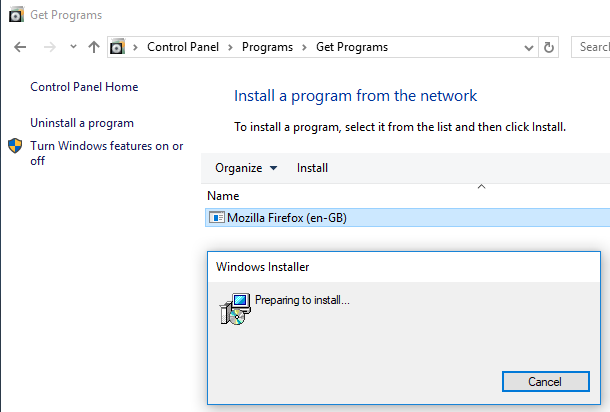


Jos teet säännön User Configurationiin voit käyttää Published vaihtoehtoa. Tämän avulla käyttäjä työasemalla voi itse asentaa ohjelmiston kun hän niin haluaa.

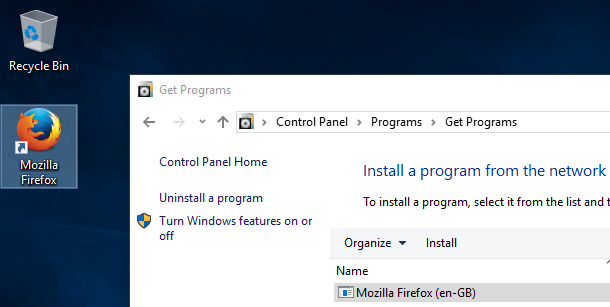
Tälläinen näkymä työaseman Programs and Features:

Install a program from the network kautta voit asentaa Firefoxin.



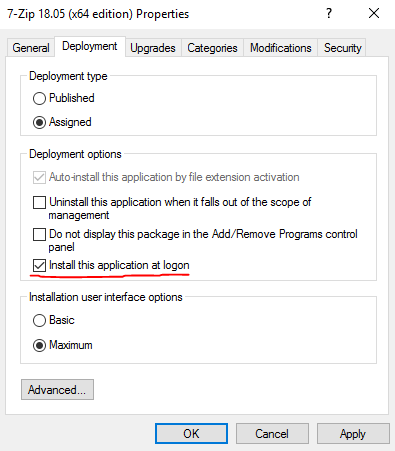


Firefox asennettu verkon yli.

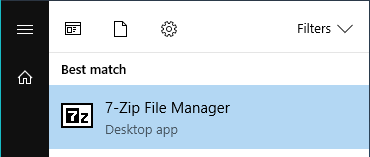


### Assigned asennus

Jos teet asennuksen Assigned tyypillä tulee sovellus asennettua automaattisesti seuraavan kerran, kun käyttäjä kirjautuu työasemalle. **Käytä User Configuration alla olevia ryhmäkäytäntöjä.**



7zip on asennettu, kun käyttäjä kirjautui tietokoneelle. Kirjautumiskerta luultavasti kesti pidemmän aikaa koska sen aikana sovellus asennettiin. Jos asennettava ohjelma olisi hyvin suuri, menisi vielä enemmän aikaa.



HUOM. Ota huomioon teetkö Software installation GPOn Computer vai User configurationille. Computer säännöt tulevat vain kyseisessä organisaatiossa oleville tietokoneille. User säännöt tulevat vain kyseisessä organisaatiossa oleville käyttäjille. Esim. Jos teet GPOn Computer sääntöihin, mutta kyseinen tietokone ei ole kyseisessä organisaatioyksikössä, ei tapahtuisi mitään.

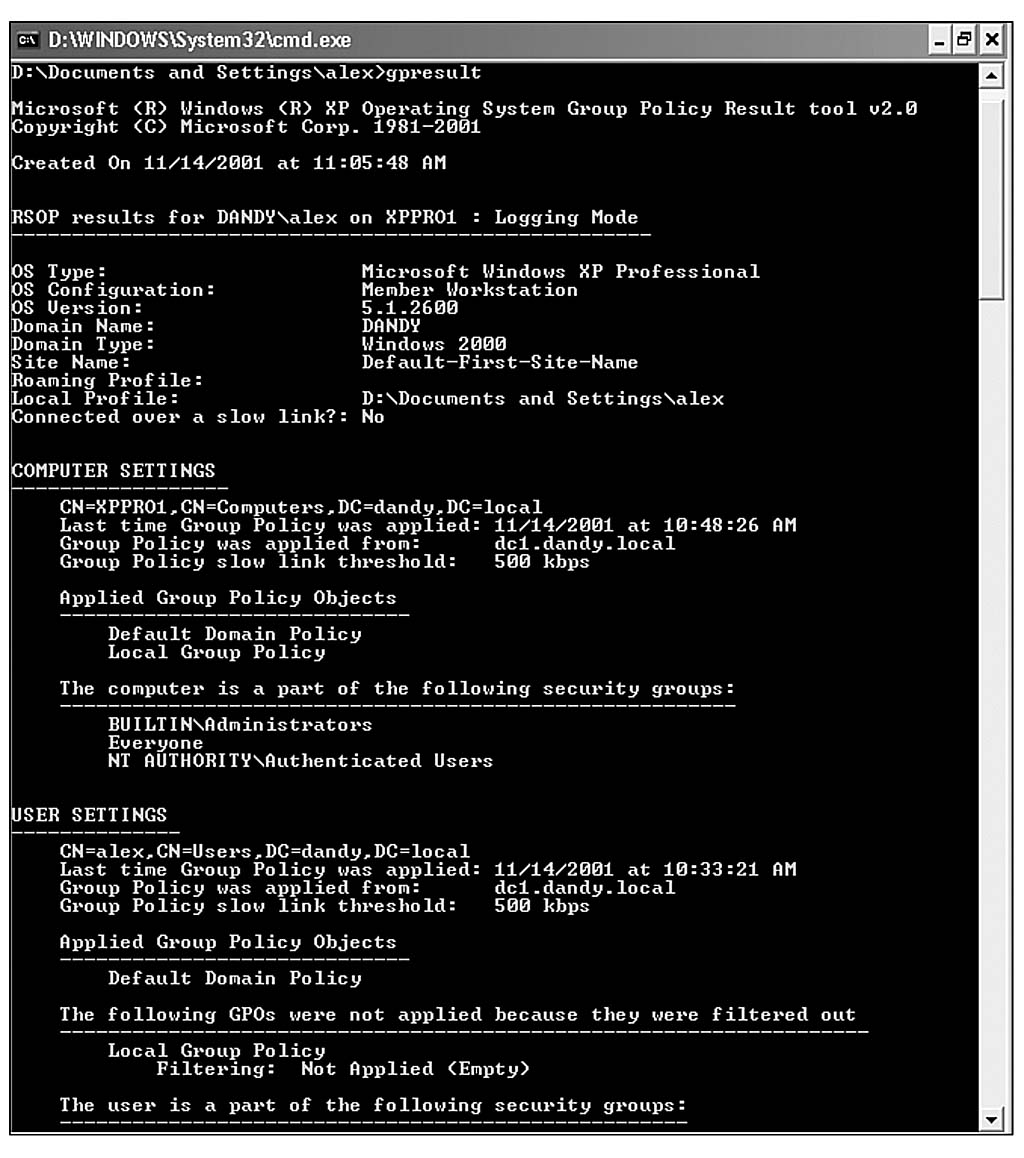
# Vianselvitys

Jos tuntuu siltä että ryhmäkäytäntö ei toimi käy läpi huolella palvelimelta Group Policyt, että olet tehnyt ne oikein ja ne kohdistuvat oikeisiin käyttäjiin ja ryhmiin. Varmista Active Directory Users and Computers puolelta tämä myös. Eli ovatko objektit siellä missä niiden pitää olla.

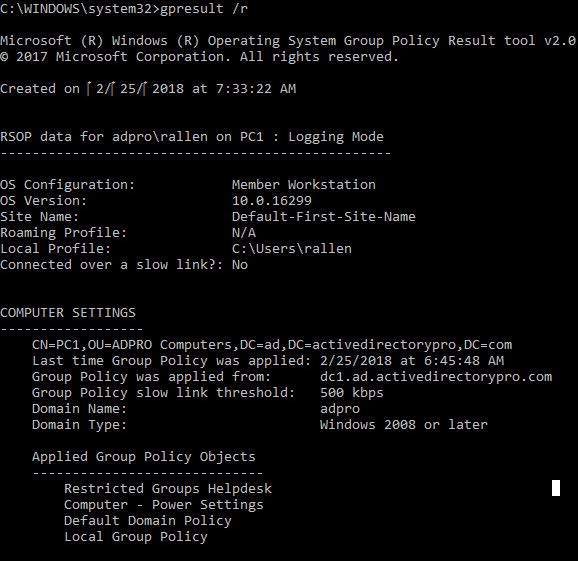
Lisäksi työasemalta voi suorittaa komennon gpresult, jolla saa tiedot ryhmäkäytännöistä, jotka vaikuttavat siihen. Kirjaudu työasemalle käyttäjällä ja suorita komento **gpresult /r**, ja katso mitkä ryhmäkäytännöt vaikuttavat KÄYTTÄJÄÄN. TIETOKONEESEEN vaikuttavat ryhmäkäytännöt saat selville, kun avaat komentorivin Admin oikeuksilla ja suoritat komennon **gpresult /r /scope COMPUTER**.

Kiinnitä huomiota kohtaan **”Applied Group Policy Objects”**

Käyttäjän oikeuksilla:



Admin oikeuksilla:



Lisätietoja tästä muun muassa täältä: <https://activedirectorypro.com/gpresult-tool/>

# Liikkuva profiili ja kotihakemistojen oikeudet

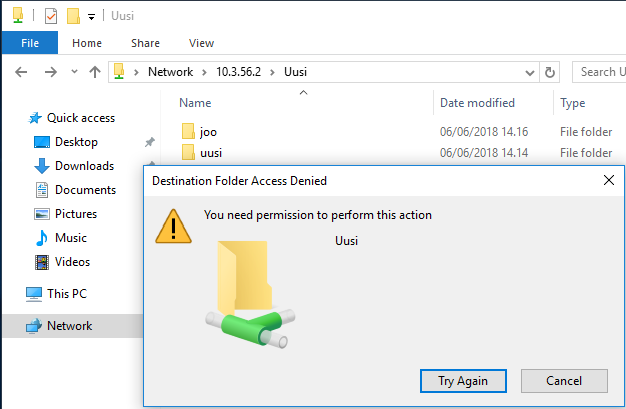
Kun teet jakoja toimialueelle tulee kiinnittää erityistä huomioita jakokansioiden oikeuksiin. Jos niitä ei tee kunnolla on mahdollista että käyttäjä pääse käsiksi toisen käyttäjän kotikansioon ja tekee siellä muutoksia.

Seuraavista linkistä löytyy erinomaiset ohjeet miten tämä suoritetaan:

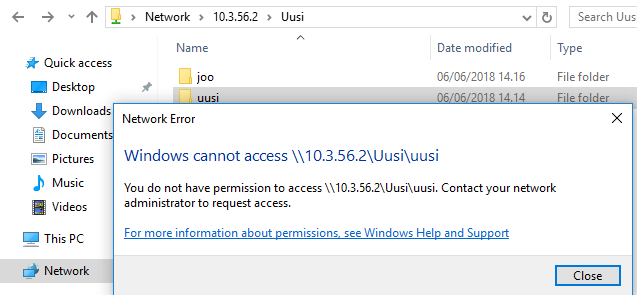
<https://www.faqforge.com/windows-server-2012-r2/set-correct-permissions-home-folder-active-directory-domain-services-windows-server-2012-r2/>

Varalinkki: <https://web.archive.org/web/20180606125415/https://www.faqforge.com/windows-server-2012-r2/set-correct-permissions-home-folder-active-directory-domain-services-windows-server-2012-r2/>

Kun oikeudet ovat kunnossa tulisi käydä näin jos käyttäjä yrittää luoda kansioita ylempänä olevaan kansioon.

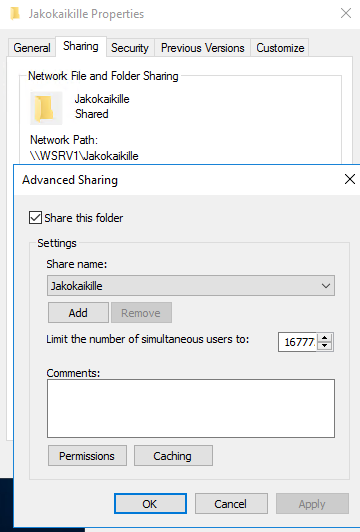


Jos käyttäjä yrittää päästä käsiksi toisen käyttäjän kansioon käy näin.

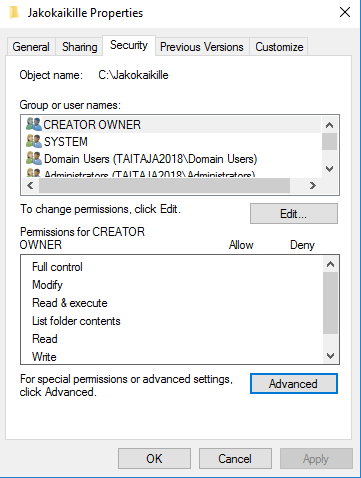


Yllä olevassa kuvassa ollaan kirjautuneena **joo** nimisellä käyttäjällä ja hän yrittää ottaa yhteyden **uusi** nimisen käyttäjän kansioon. Kansioden oikeudet ovat siis kohdillaan.

# Verkkojaon teko

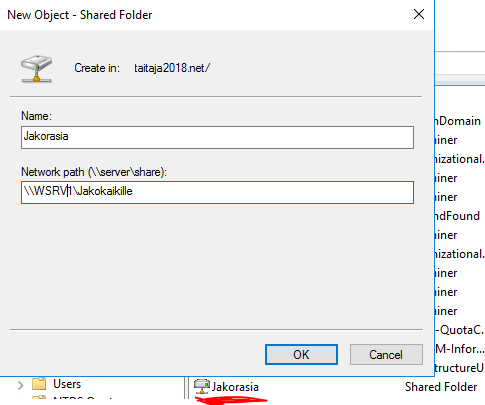
Luo esim. C:\ aseman juureen Jakokaikille niminen kansio ja laita se jakoon. 

Jos haluat tehdä käyttöoikeuksiin enemmän muutoksia pääset niihin Security välilehdeltä kohdasta Advanced. Sitä kautta voit asettaa esim. Kansiolle luku- ja kirjoitusoikeudet.

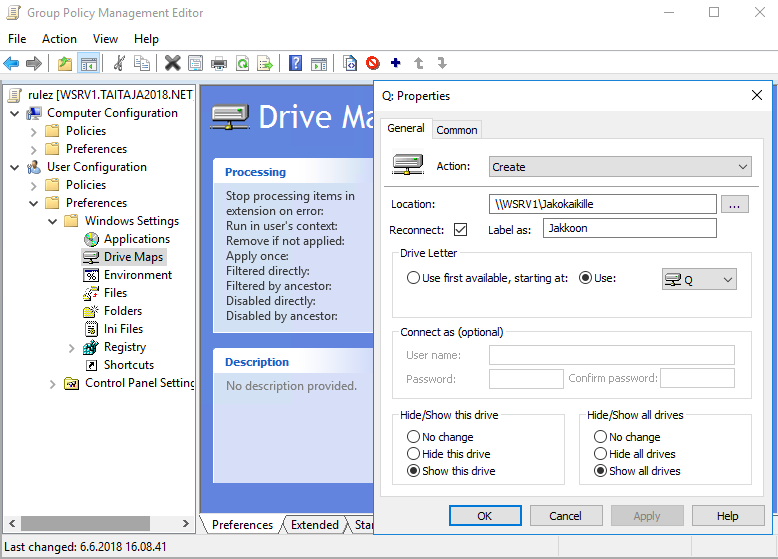


Kopio jaetun kansion polku leikepöydälle tai pidä se mielessä.

Mene AD Users and Computers ja luo uusi Shared Folder objekti.



Seuraavaksi tämä jaettu kansio tulee jakaa ryhmäkäytäntöjen kautta. Se löytyy kuvan mukaisesti polusta GPO editorissa. Muista valita oikea asemankirjain ja käytä samoja asetuksia kuin alla olevassa kuvassa (polkusi on tietenkin eri)!



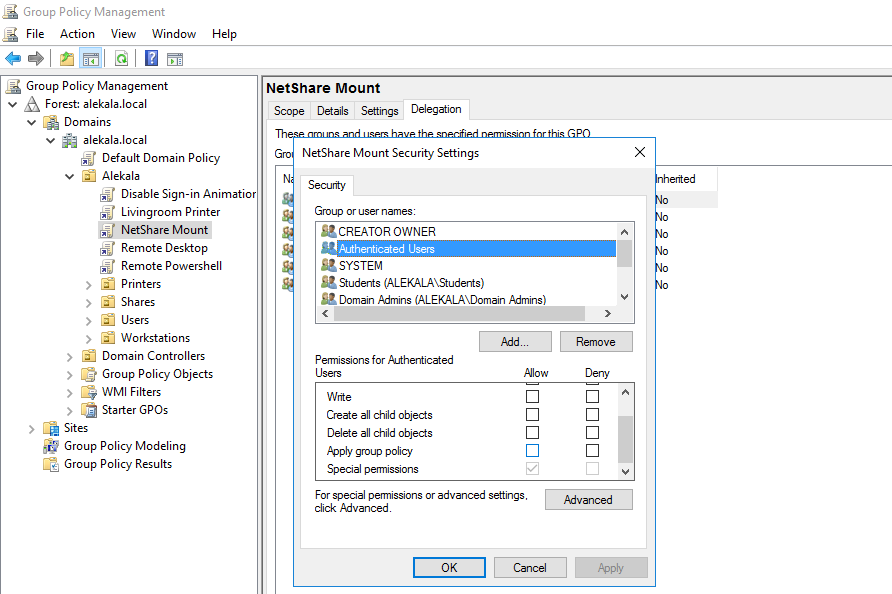
# Security Filtering

Tehnyt: Aleksi Sievälä

Jos Group Policy Objectin luo Organizational Unitin alle, vakiona se vaikuttaa kaikkiin työasemiin/käyttäjiin. Security Filteringillä voidaan vaikuttaa keneen GPO vaikuttaa OU:in alla.

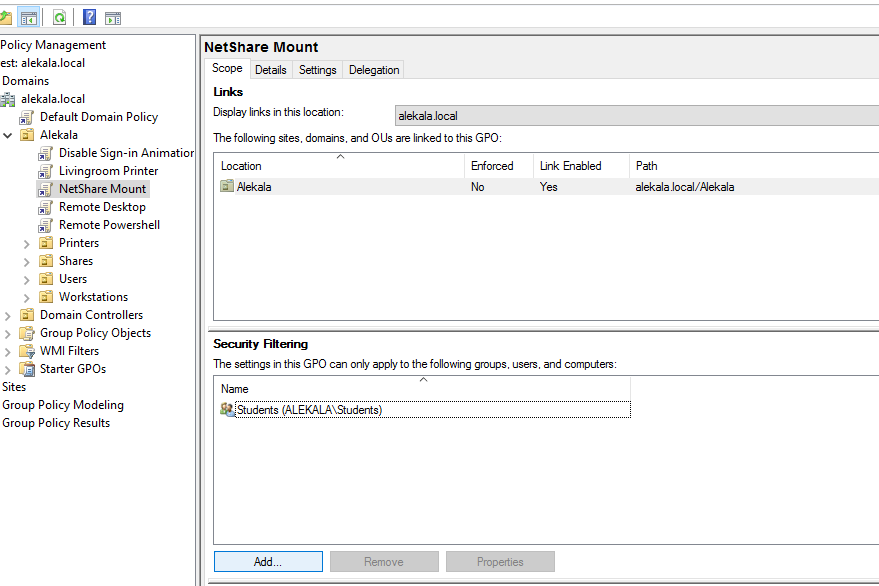
Otetaan vakio oikeus pois, eli poistetaan Authenticated Usersilta Apply group policy oikeus pois, jätä kuitenkin Read oikeus Authenticated Usersille:

Server Manager > Tools > Group Policy Management > Haluamasi GPO > Delegation > Advanced



Seuraavaksi mene haluamasi GPOn välilehdelle Scope, kuten alla olevassa kuvassa on. Poistaa Security Filtering kohdasta oletusryhmä, eli Authenticated Users.

Sitten lisätään haluttu ryhmä:



Tässä esimerkissä sääntö koskisi vain Students nimistä ryhmää, mutta ryhmäkäytäntö on edelleen organisaatioyksikölle.

Kun Security Filteringiin lisätään ryhmä tai käyttäjä, tulee sille automaattisesti tarvittavat oikeudet, eli Read ja Apply group policy.

Oikeudet voidaan myös määrittää vastoinpäin, eli estää osilta objekteilta GPO:in vaikutus. Esim. Jos OU:in alla on 10 käyttäjää ja halutaan kahdeksalle käyttäjälle verkkojako, voidaan lisätä GPO OU:in alle ja estää sen vaikutus kahdelta käyttäjältä joille verkkojakoa ei haluta.

**Tärkeä huomio!** **Security filtering tapauksissa GPO itse pitää tehdä sellaisen OU:hun, jonka sisällä halutut käyttäjät/tietokoneet ovat.** Esimerkiksi alla olevassa kuvassa GPO:ta ei voisi tehdä Groups alle, sillä sen alla ei ole lainkaan käyttäjiä tai tietokoneita. Tässä tapauksessa hyvä sijainti GPO:lle on Skills Co niminen OU.

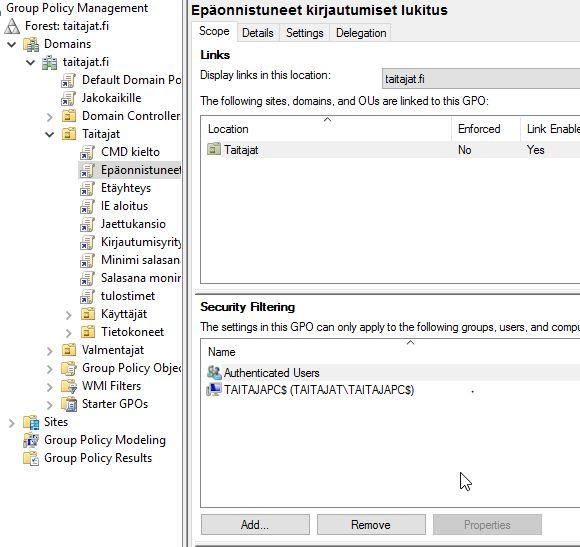
A screenshot of a computer

Description automatically generated

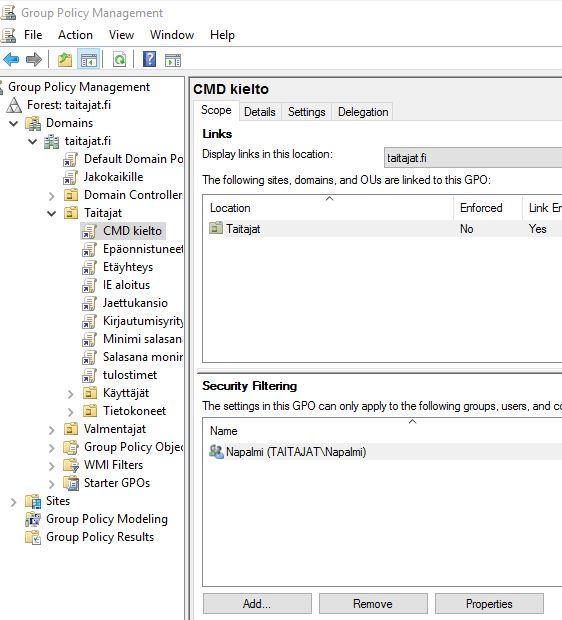
# Esimerkki Security Filtering käytöstä

Tässä määritetään, että command promptiin ei ole oikeutta Napalmi ryhmän käyttäjillä.

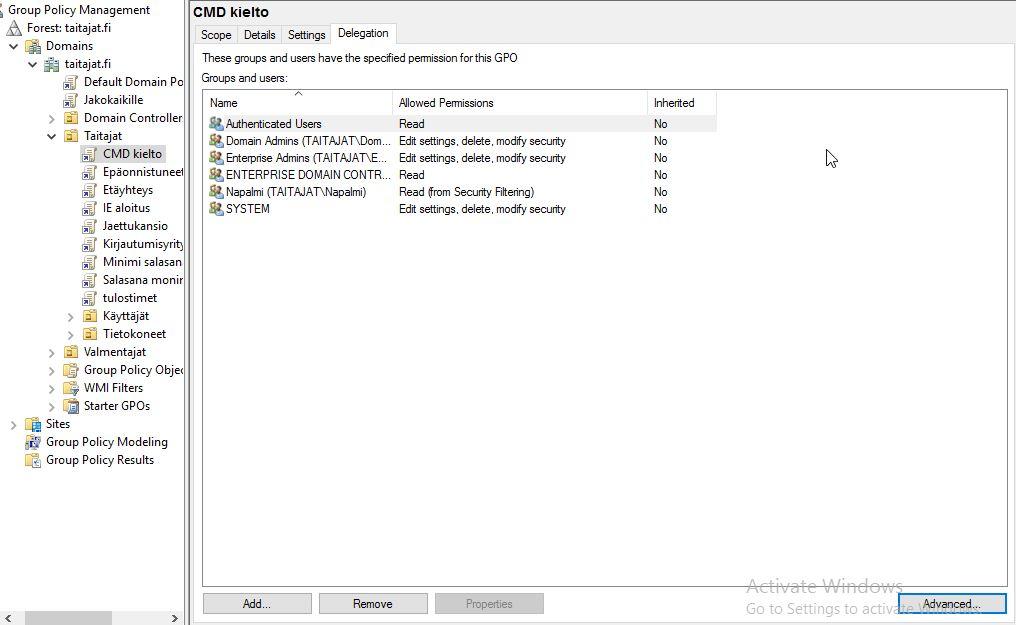
Oletuksena Security Filtering näyttäisi tältä Scope välilehdeltä:



Poistetaan Authenticated Users Remove kohdasta ja lisätään haluttu ryhmä, eli Napalmi, Add… kohdasta.

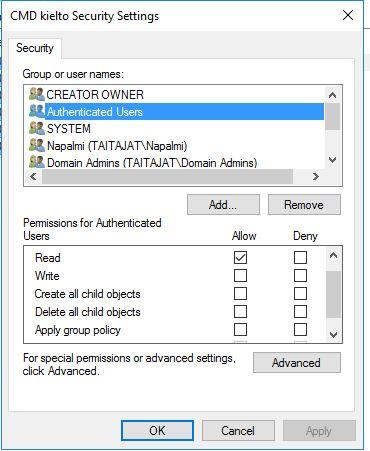
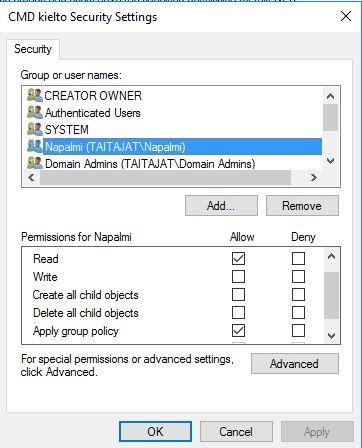


Seuraavaksi Delegation välilehdeltä muokataan oikeuksia. Paina Advanced… kohtaa.



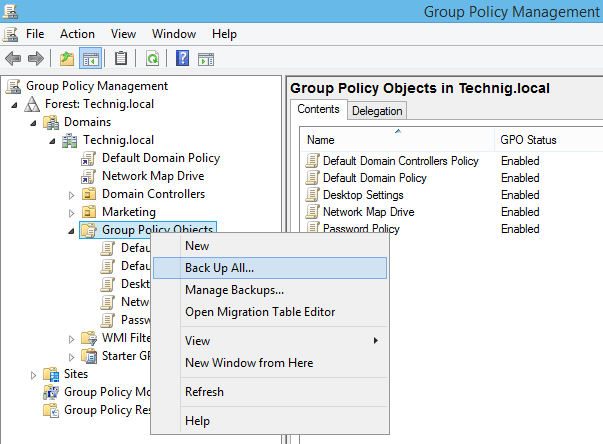
Authenticated Users tulee olla Read oikeus, mutta ei Apply group policy oikeutta. (Vasen kuva)

Napalmi ryhmällä tulee olla Read ja Apply group policy oikeudet. (Oikea kuva)

# Varmuuskopionti

Kuvan mukaisella tavalla saat otettua varmuuskopiot ryhmäkäytännöistä seuraavalla tavalla:



# Central Store

Central Store on toiminto, jonka avulla toimialueelle voi tuoda ulkopuolisia ryhmäkäytäntöjä. Usein näitä käytetään esimerkiksi Edge, Chrome ja Firefox selainten hallintaan.

Central Store tehdään luomalla kansio nimeltään PolicyDefinitions polkuun C:\Windows\SYSVOL\domain\Policies\. Tämän jälkeen polkuun C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions kopioitaisiin olemassa olevat ryhmäkäytännöt sekä uudet ulkopuoliset ryhmäkäytännöt.

Olemassa olevat ryhmäkäytännöt löytyvät palvelimelta kansiosta C:\Windows\PolicyDefinitions. (Tai ne voidaan ladata Microsoftin sivuilta). Täältä kopioitaisiin en-US kansio sekä KAIKKI .admx päätteiset tiedostot. Ne kopioitaisiin kansioon C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions

Tämän jälkeen ulkopuoliset ryhmäkäytännöt ladattaisiin ja ne purettaisiin C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions kansioon. Tähän kansioon tulisi .admx päätteinen tiedosto.

Kansioon C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions\en-US kopioitaisiin .adml päätteinen tiedosto.

Esimerkki Microsoftin osoitteesta <https://learn.microsoft.com/en-us/deployedge/configure-microsoft-edge#add-the-administrative-template-to-active-directory>