GPO's

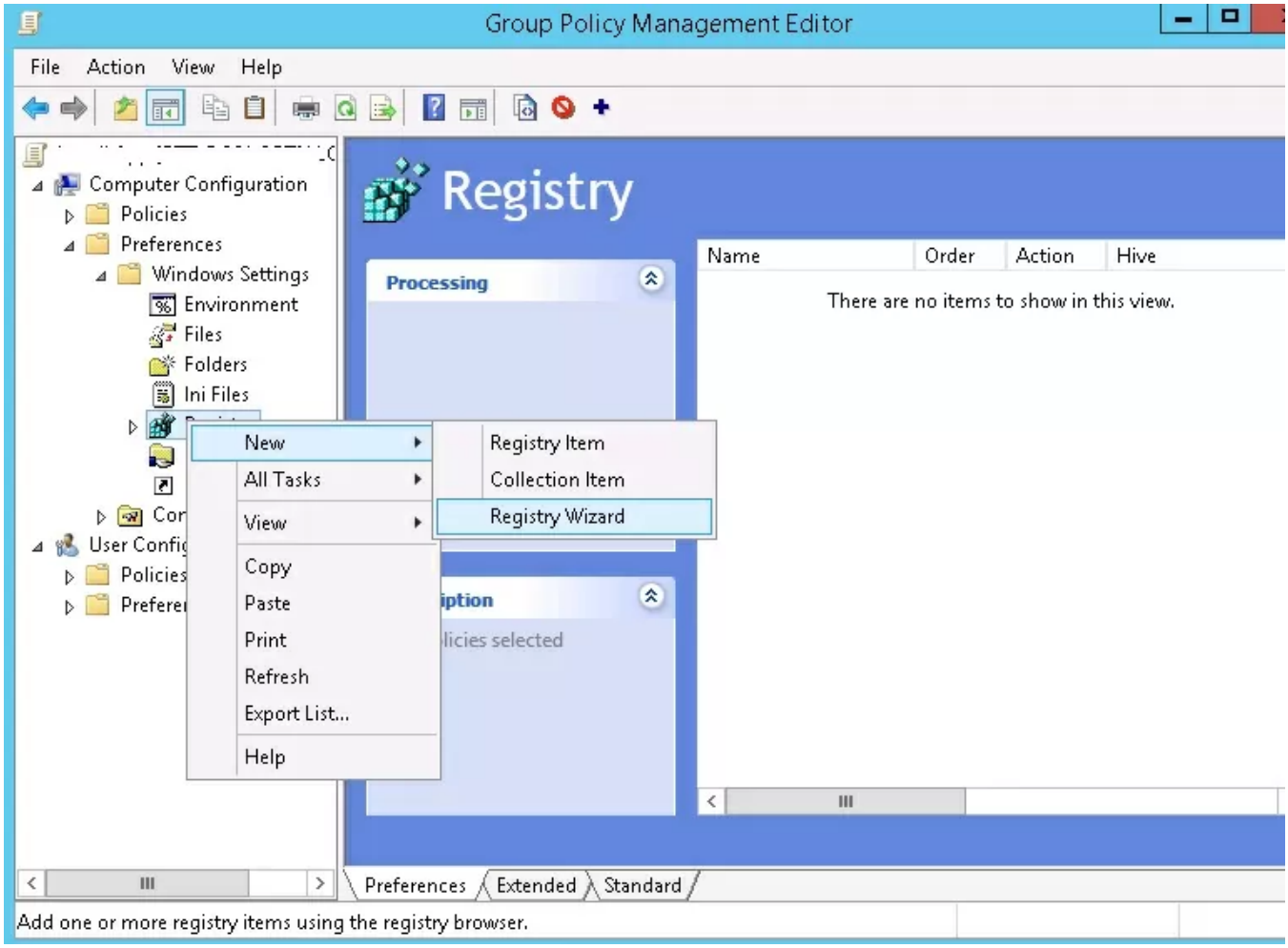
- Modifier le registre par GPO
- LAPS
- Exclure un groupe d’une gpo / utilisateur
- Erreur avec la relation d'approbation
- COMMANDES AD UTILES
- Déploiement EXE par GPO et installation silencieuse
- Filtrage WMI
- Acrobat Reader optimisation

Modifier le registre par GPO

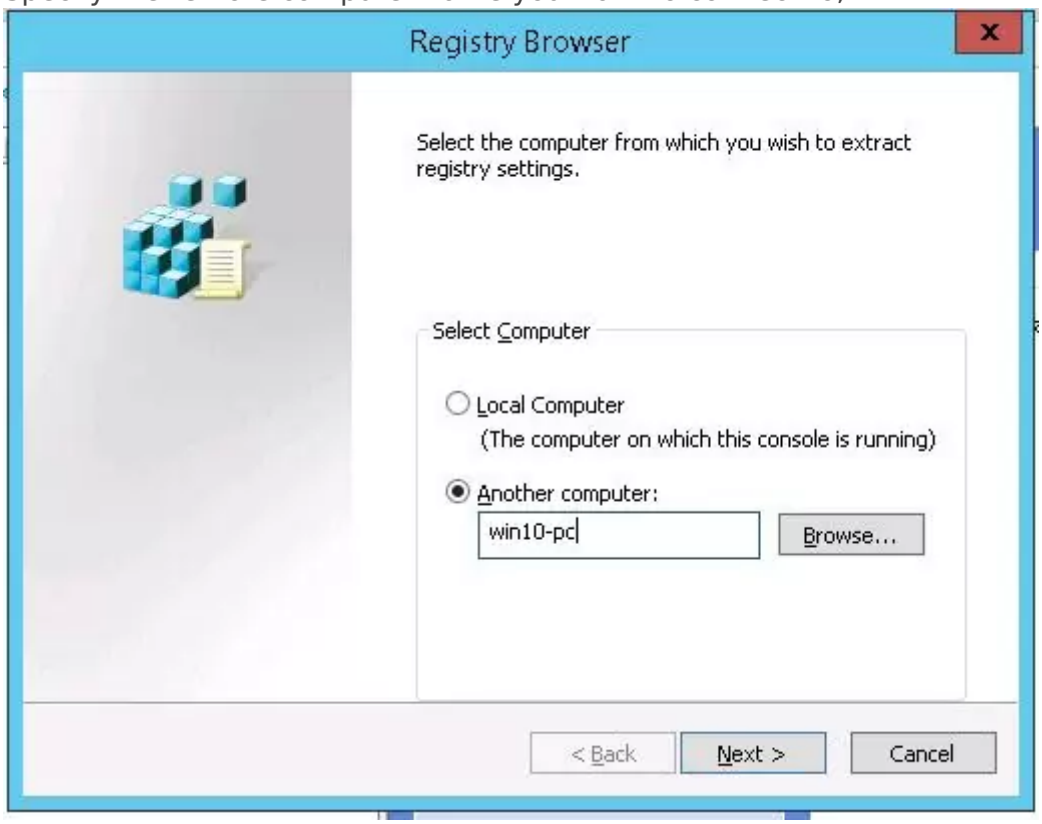
Deploy Registry Items Using the Registry Wizard in GPO

The Registry Wizard in the GPO is the easiest way to make changes to the registry.

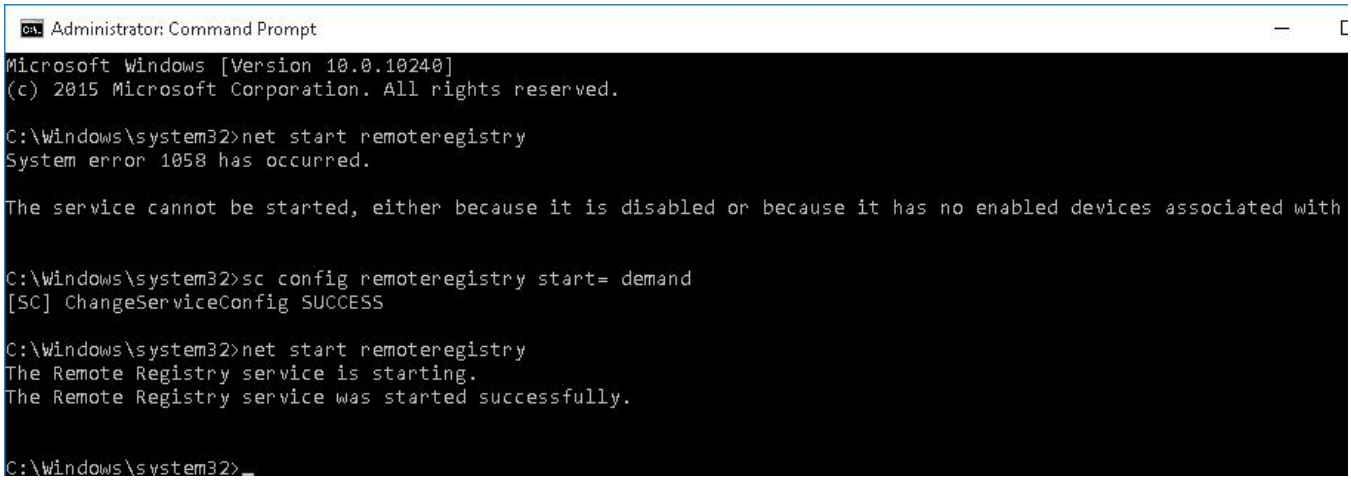
1. Run the Group Policy Management console (`gpmc.msc`);
2. Create a new GPO (or edit the existing one), link it to the required container (OU) in AD with the computers (or users) on which you want to apply the registry key, and switch to the policy edit mode;
3. Expand the GPO section **Computer** (or **User**) **Configuration** -> **Preferences** -> **Windows Settings** -> **Registry** and select **New** -> **Registry Wizard** in the context menu;



4. The **Registry Wizard** allows you to connect to the registry on a remote computer and select the existing registry key;
5. Specify the remote computer name you want to connect to;



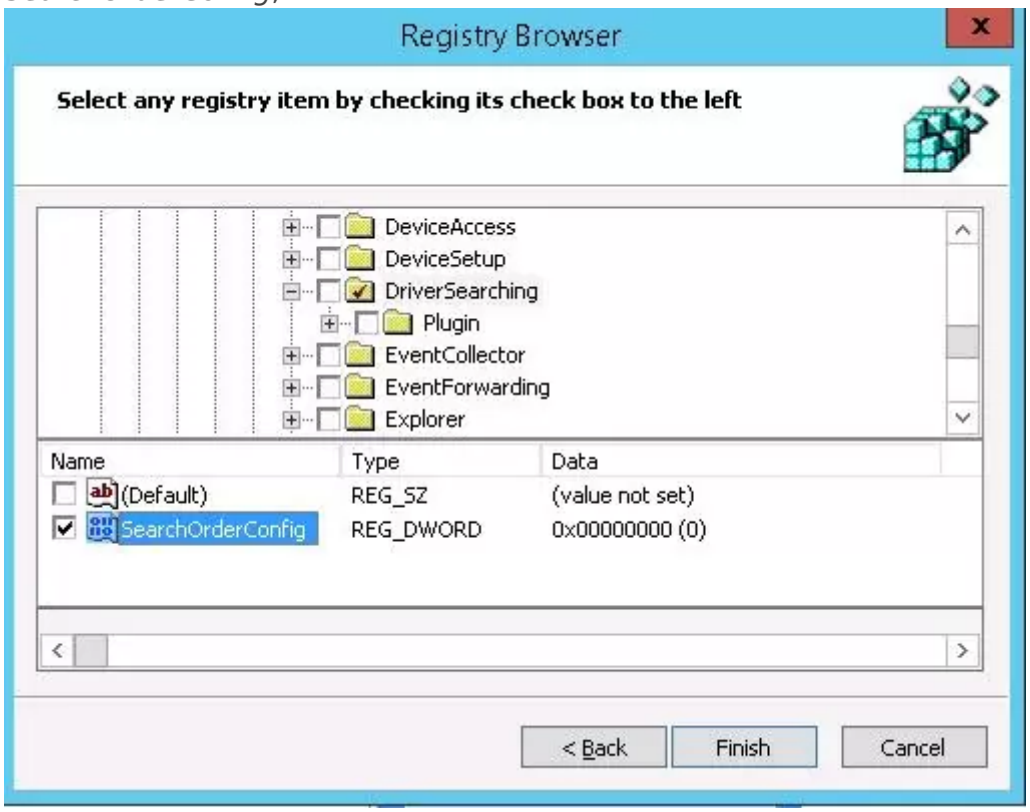
Note. If the error *The network path was not found* appears when you try to connect to a computer through the Registry Browser, it most likely this remote computer is turned off, access to it is blocked by a firewall or the Remote Registry service is not started on it. ****To start the service manually, run these commands on the remote computer: `sc config remoteregistry start= demandnet start remoteregistry`



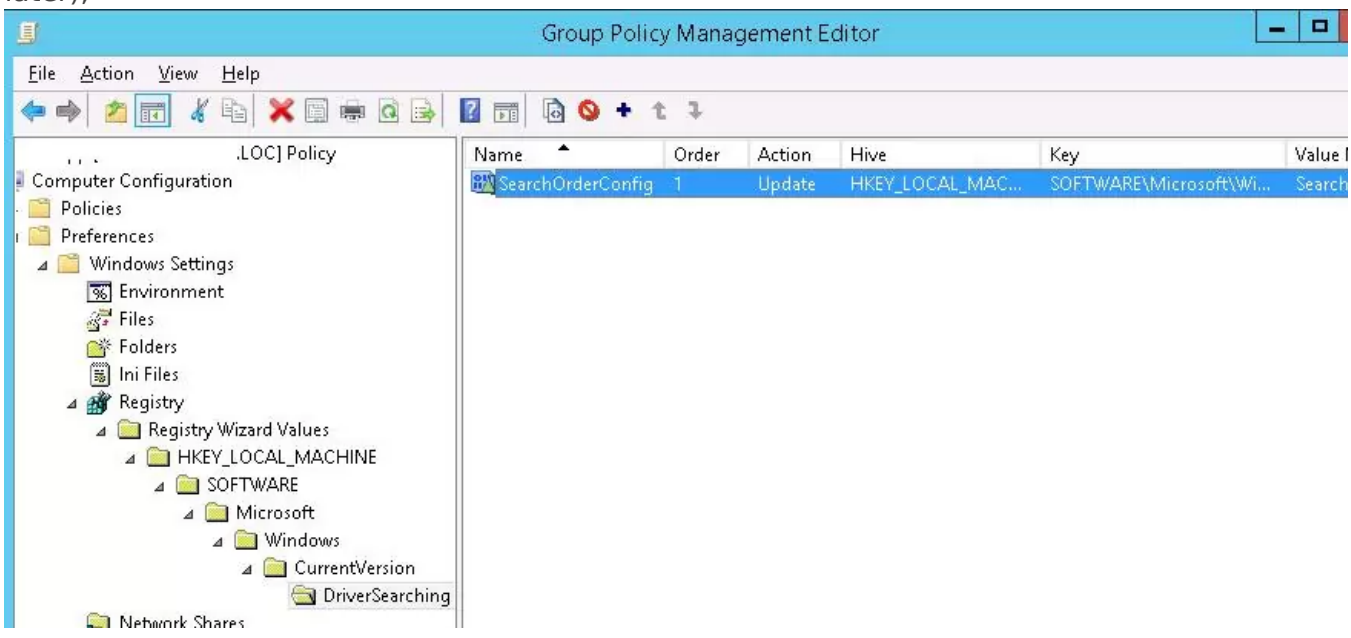
6. Use the Remote Registry Browser to find and select all the registry parameters that you want to deploy through the GPO;
   Note. This registry browser allows you to select only registry keys from the HKEY_LOCAL_MACHINE and HKEY_USERS hives on a remote computer. If you need to set the keys contained in other registry hives, you need to install RSAT on the remote computer. Then run the gpmc.msc console on this computer and use the same procedure

to select the registry keys you need.

7. In this example, I want to import only one registry parameter to the GPP — *SearchOrderConfig*;



8. The specified registry entry is imported into the GPP console along with the path and current value (0). You can change its value and the desired action (this will be considered later);



9. Thus, you have created a Group Policy to deploy your registry key. The next time the Group Policy settings are updated on the target computers, the value of the SearchOrderConfig registry key will change to 0.

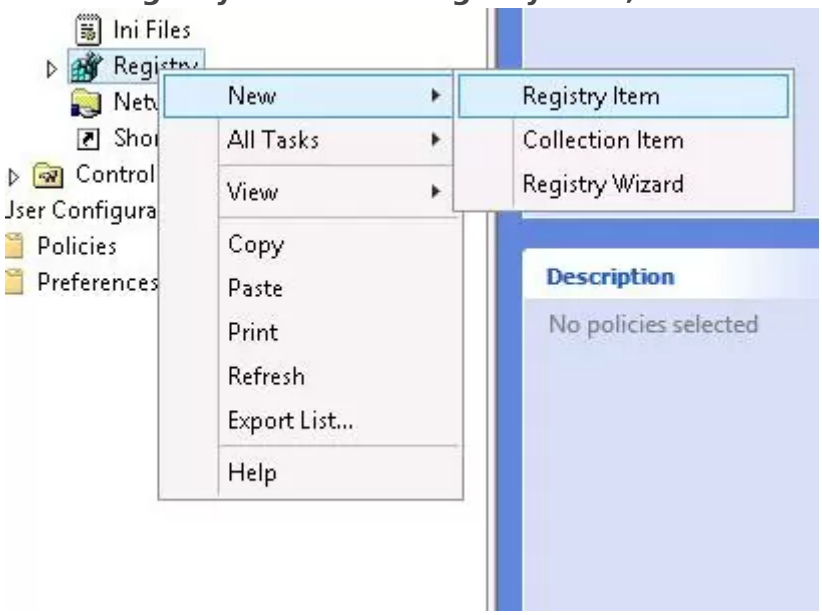
   If the policy doesn't apply to the client, you can use the GPResult tool for diagnostics.

If this GPO is removed, unlinked from an AD container, or a target computer is moved to another OU, then the value of the registry parameter won`t return to its original (default) value.

How to Manually Create, Edit or Delete a Registry Key using Group Policy?

You can use GPP to create, modify, or delete a specific parameter or registry key by manually specifying the path and value of the registry item.

1. Select **Registry -> New -> Registry Item;**



2. Configure your registry item settings:

   Action: Update

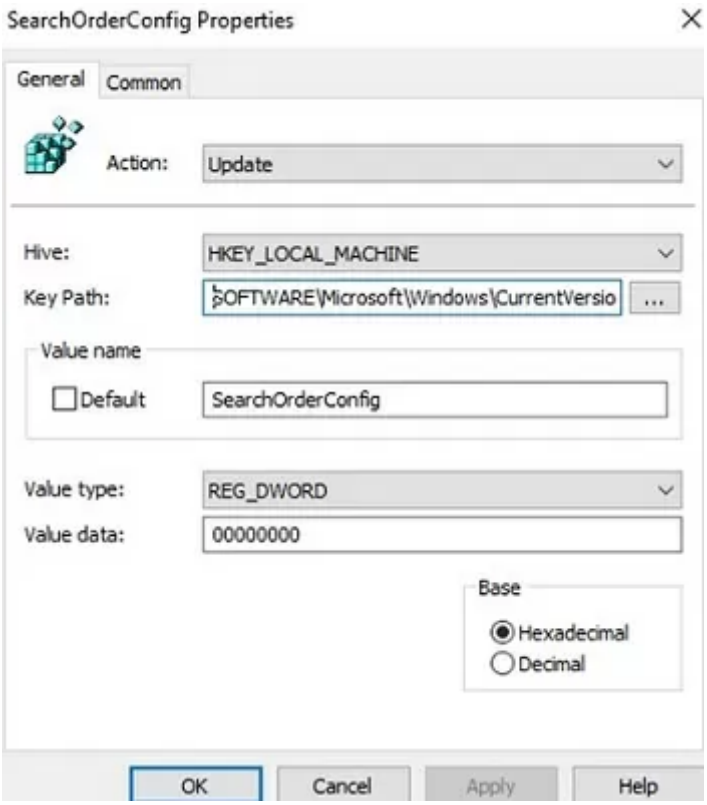
   Hive: HKEY_LOCAL_MACHINE

   Key Path: SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\DriverSearching

   Value name: SearchOrderConfig

   Value type: REG_DWORD

   Value date: 00000000



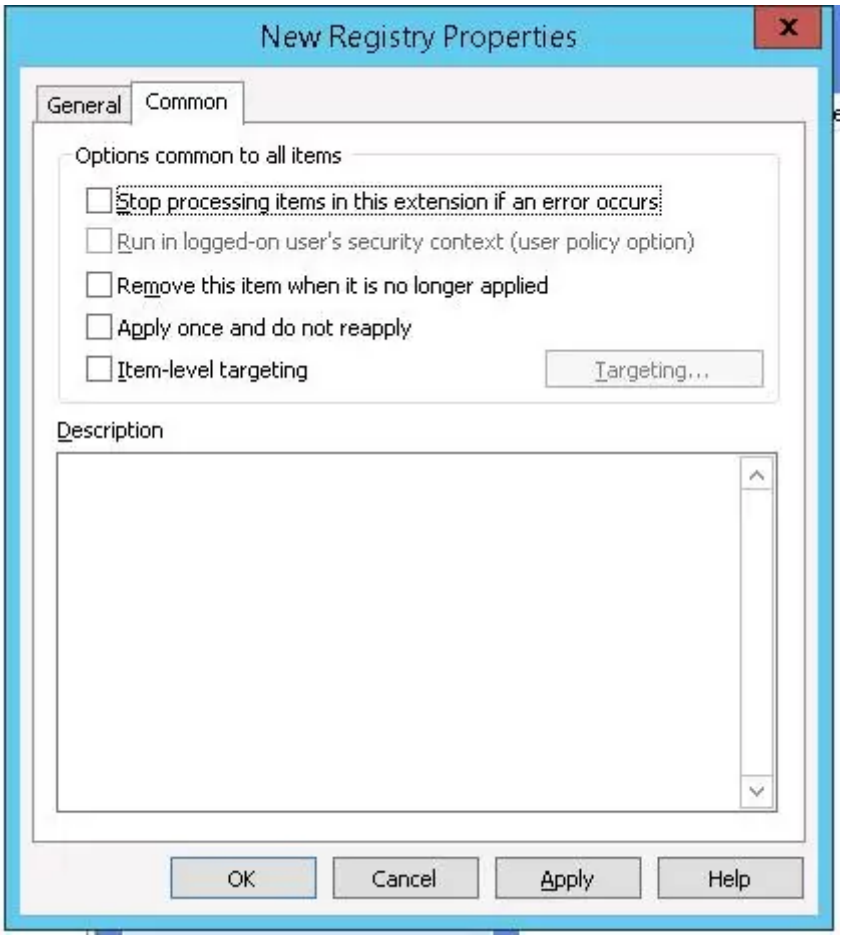
Do not enter the name of the HIVE in the key path, or an additional subkey will be created in the registry (such as HKEY_HKEY_XXX).

3. By default, the registry items that are configured by the GPO are set to **Update** mode.

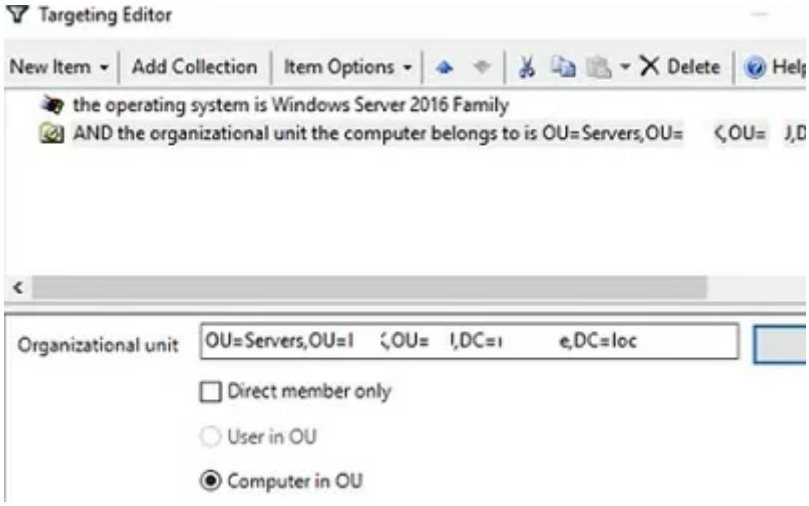
4 types of actions are available in GPO for registry keys:

- **Create** – creates a registry key/parameter. If the parameter already exists, its value is not changed;
- **Update** (by default) – updates the value of an existing parameter according to the GPP. If the registry parameter doesn't exist, it will be created automatically (as well as the registry key where it should be located);
- **Replace** – if the registry parameter/key already exists, it will be deleted and recreated (rarely used);
- **Delete** – deletes a registry item.

There is a number of other useful options on the **Common** tab:



- **Run in logged-on user's security context (user policy option)** — a registry key is created only in the current user context (it is possible only for GPP in the User Configuration section of the GPO). If a user doesn't have administrator privileges, the policy won't be able to write anything to the protected system registry keys;
- **Remove this item when it is no longer applied** – if the policy no longer applies to a client, the registry change will be automatically deleted;
- **Apply once and do not reapply** – a policy is applied to a client (user or computer) only once. Later it won't be reapplied. If after applying the GPO, the user manually changes the value of the registry item, the policy won't override its value on the next policy update cycle;
- **Item-level targeting** – allows you to more accurately target policy to clients (you can target the policy to a specific IP, network mask, computer name, or computers with certain characteristics, similar to how you use WMI filters in GPO). For example, you can specify that the registry parameter should be applied to computers running Windows Server 2016 in the AD OU named Servers.



This is how the resulting Group Policy settings will look in the GPMC console (on the Settings tab).

Preferences hide

Windows Settings hide

Registry hide

Collection: Registry Wizard Values/ HKEY_LOCAL_MACHINE/ SOFTWARE/ Microsoft/ Windows/ CurrentVersion/ DriverSearching hide

Common hide

Options

Stop processing items on this extension if an error occurs on this item	No
Apply once and do not reapply	No

Registry item: SearchOrderConfig hide

General hide

Action: Update

Properties

Hive	HKEY_LOCAL_MACHINE
Key path	SOFTWARE\Microsoft\Windows\CurrentVersion\DriverSearching
Value name	SearchOrderConfig
Value type	REG_DWORD
Value data	0x0 (0)

Common hide

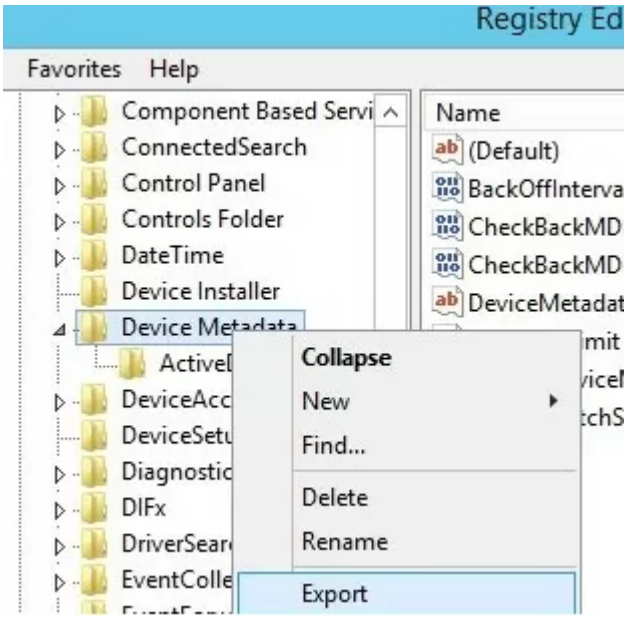
Options

Stop processing items on this extension if an error occurs on this item	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

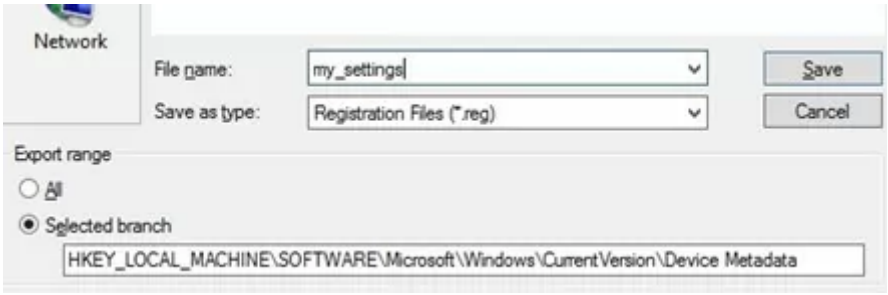
GPO: Import Registry Data from a REG File

The Registry Group Policy Preference allows an administrator to import a .REG file containing multiple registry entries into Group Policy at once. For this, the REG file must be converted to XML (Group Policy Editor allows you to import files in XML format only).

For example, you have a reference computer on which some settings are configured through the registry. You can export these settings to a REG file by right-clicking on the reg key name in the regedit.exe and selecting **Export**.



Save the registry key entries to the REG file.



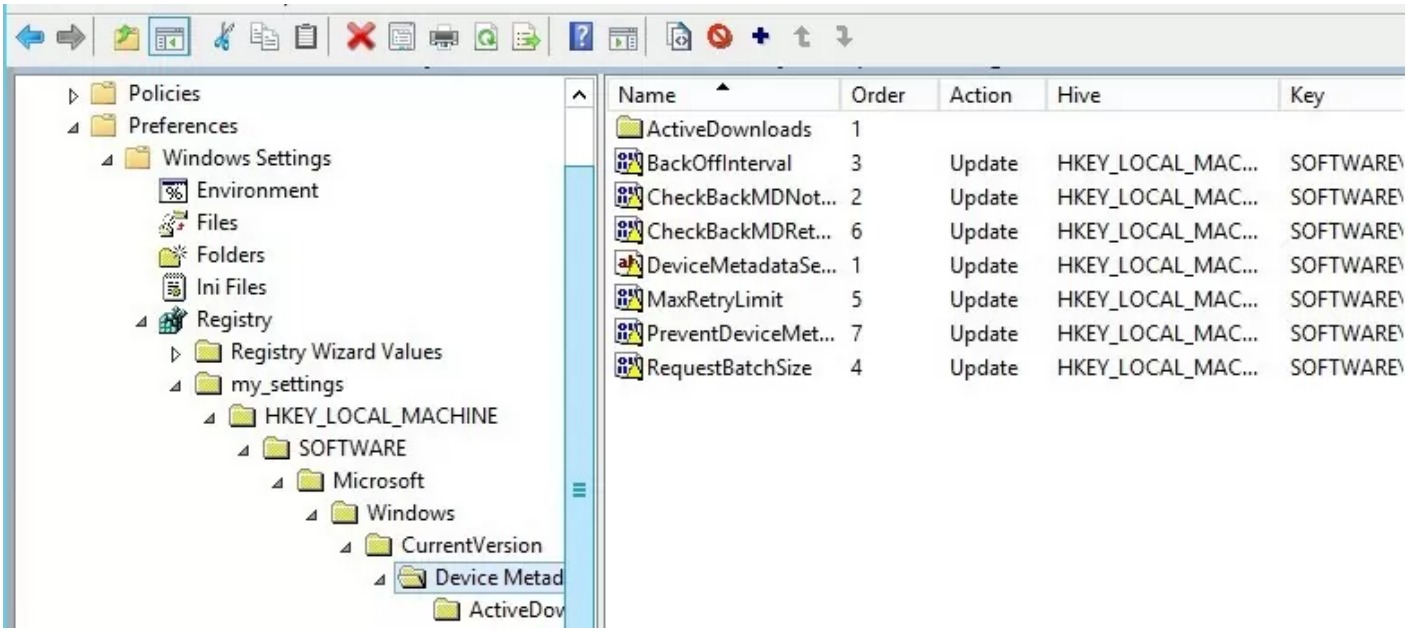
If your REG file contains data from different registry hives (HKLM, HKCU, HKEY_CLASSES_ROOT, HKEY_USERS), you need to divide them into separate REG files.

Next, you need to convert this REG file to XML format. You can perform the reg->xml conversation using the online service **Reg2GPP** https://www.runecasters.com.au/reg2gpp with the PowerShell

script **RegToXML.ps1**.

Copy the resulting XML file in File Explorer and paste it into the Registry section of the Group Policy Editor.

As a result, all the registry settings from your REG file will appear in the Group Policy console and will be applied to the target domain computers.

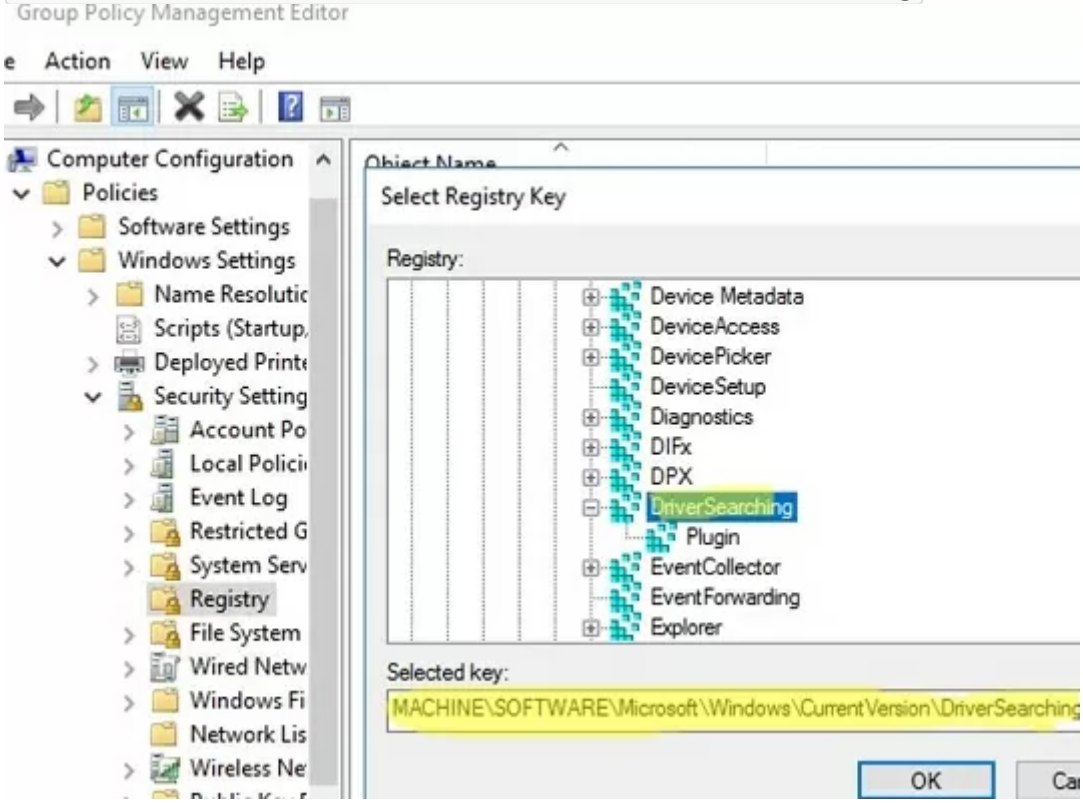


Set Registry Key Permissions with Group Policy

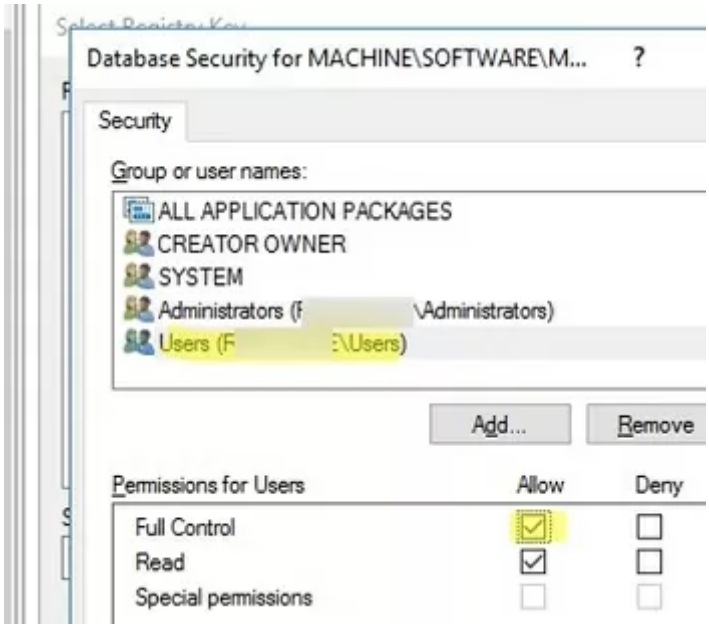
You can use Group Policy to change access permissions (ACL) for specific registry keys. You can use this feature to prevent non-admin users from accessing protected registry keys or to allow regular users the right to modify system keys.

You can configure the registry ACL settings in the GPO section **Computer Configuration** -> **Windows Settings** -> **Security Settings** -> **Registry**

1. Select **Add key**;
2. Use the built-in Registry Browser to find the registry key you need (or specify the path manually in the following format `MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\DriverSearching`);



3. Set the new ACL settings for your registry key that you want to apply in the Database Security window. In this example, I want to allow users to make any changes to the system-protected registry key. You need to select the **Users** group and grant **Full Control** permission for it. You can enable the inheritance of permissions to the sub-keys by using the **Advanced** -> **Enable inheritance** option;



You can add or remove any other security groups, users, and other principals from the local computer or Active Directory.

4. Save your changes. The new registry key permissions will apply to clients after the GPO is updated.

How to Modify Registry Entries with a GPO Logon Script?

Prior to Windows Server 2008, only logon script BAT files can be used to modify the registry settings by using the GPO. You must use the **reg add** or **reg import** commands in such a .bat file to make changes to the registry.

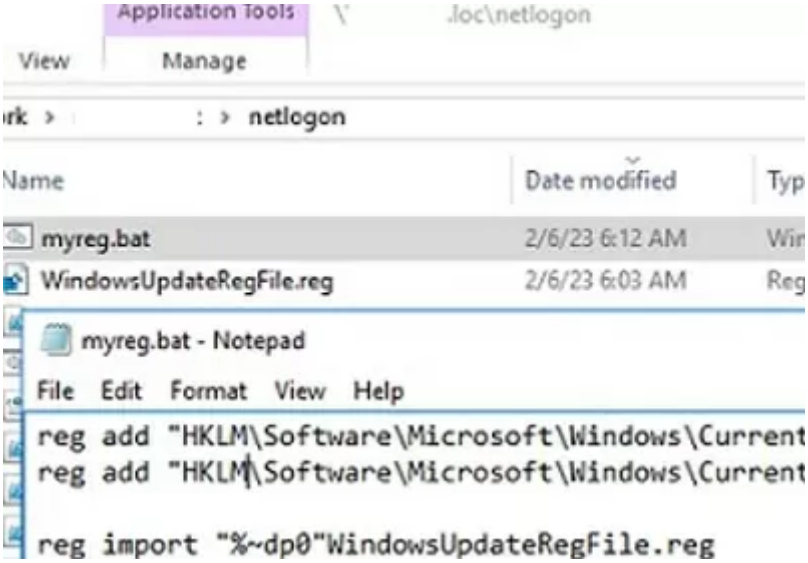
To make changes to the registry using the GPO logon script, you need to create a text file **myreg.bat** with the necessary commands. For example:

- These two commands allow you to configure proxy settings in Windows (run via Startup script in Computer Configuration): `reg add "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings" /v ProxyEnable /t REG_DWORD /d 1 /freg add "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings" /v ProxyServer /t REG_SZ /d yourproxyadress:proxyport /f`
- The following two commands clear the client's RDP connection history. In this example, the script must be run from the Logon script section in the User Configuration because we are accessing a user registry hive: `reg delete "HKEY_CURRENT_USER\\Software\\Microsoft\\Terminal Server Client\\Default" /va /freg delete "HKEY_CURRENT_USER\\Software\\Microsoft\\Terminal Server Client\\Servers" /f`
- The last command lets you import an entire registry key from a REG file (in order to export the local registry key, use the following command: *reg export*

HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate c:\WindowsUpdateRegFile.reg
): `reg import "%~dp0"WindowsUpdateRegFile.reg`

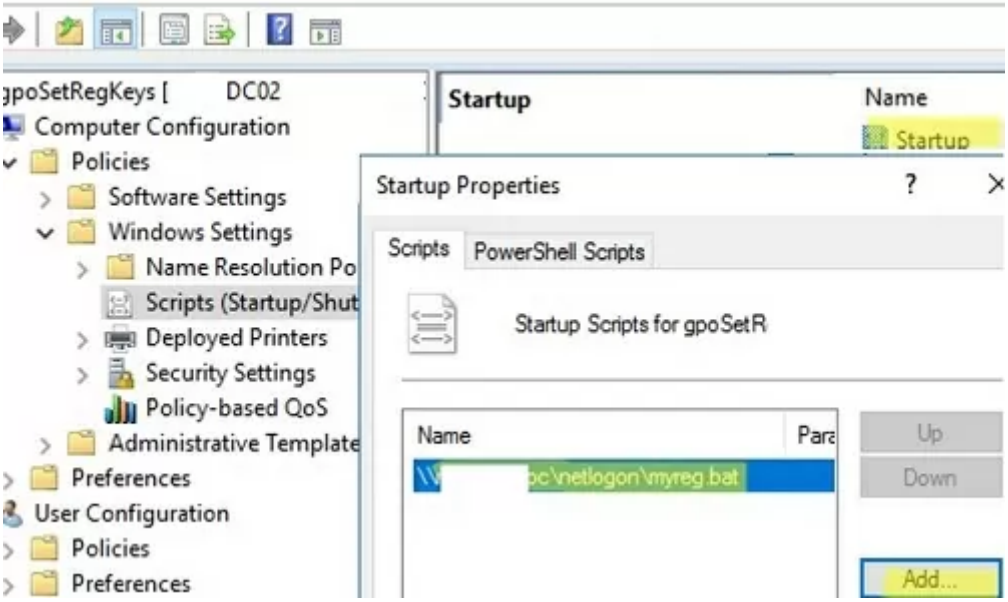
To use the path to the current directory where the BAT script is located, the special `%~dp0` parameter is used.

Copy your *.bat (and *.reg if you need to import) to the Netlogon directory on the domain controller (`\\\\woshub.loc\\netlogon`).



Open your GPO and navigate go to **Computer Configuration** -> **Windows Settings** -> **Scripts** -> **Startup**.

Click **Add** and specify the UNC path to your bat file in NETLOGON.



The next time you restart Windows, your BAT file will run and make changes to the registry.

By default, this bat file is run every time you restart your computer. You can configure the GPO to run the script only once.

LAPS

Le mot de passe administrateur local : un vrai problème de sécurité

Bien souvent, pour faciliter la gestion des postes de travail notamment lors des opérations de maintenance, **on définit le même mot de passe pour le compte "Administrateur" local de toutes les machines**. Ce mot de passe est définit à l'installation de Windows, ou automatiquement lorsque la machine est déployée à partir d'une solution de déploiement d'images (comme le couple WDS/MDT).

Même si l'on peut avoir conscience que cela est problématique d'un point de vue de la sécurité, il est difficilement envisageable de **gérer un mot de passe par machine sans solution adaptée**. Comme vous l'avez compris suite à la lecture des premiers paragraphes de ce chapitre, Microsoft propose une vraie solution à cette problématique avec LAPS.

Utiliser le même mot de passe administrateur local est une aubaine pour les pirates informatiques. Pour bien comprendre, prenons un exemple où une société utilise le même mot de passe sur toutes les machines (ou un ensemble de machines) de son parc. Si un pirate informatique parvient à récupérer le mot de passe Administrateur local et prendre le contrôle d'une machine, il peut effectuer **des déplacements latéraux de machine en machine puisque le même mot de passe est utilisé**. De cette façon, il peut progresser plus facilement au sein de votre système d'information afin d'atteindre son objectif final... D'où l'intérêt de protéger les comptes locaux des machines !

Attention : LAPS (Legacy) est désormais remplacé par Windows LAPS, qui fonctionne sur le même principe mais qui apporte des fonctionnalités supplémentaires (dont le chiffrement du mot de passe et le stockage du mot de passe dans Azure Active Directory). Pour en savoir plus sur la configuration de Windows LAPS pour l'Active Directory, suivez ce tutoriel Windows LAPS. Autrement dit, Windows LAPS doit être utilisé en priorité vis-à-vis de LAPS (Legacy).

Exclure un groupe d’une gpo / utilisateur

https://www.it-connect.fr/chapitres/comment-bloquer-une-gpo-pour-un-groupe-specifique/

Application : j'ai du exclure le compte administrateur d’une gpo appliquant des restrictions dans des sessions RDS les rendant compliquées à dépanner.

Cas : j'ai exclu un utilisateur d’une GPO mais pas d'effet.

Rsop.msc depuis le poste pour identifier les paramètres modifiés par gpo.

Ça ne fonctionnait pas car GPO ordinateur > il faut exécuter la commande en tant qu'administrateur local du poste.

Runas /user:domaine\administrateur cmd

Puis rsop.msc

Récupérer le nom de la gpo responsable

Erreur avec la relation d'approbation

https://www.it-connect.fr/windows-comment-corriger-erreur-de-relation-approbation-voici-plusieurs-methodes/

COMMANDES AD UTILES

Repadmin /replsummary > Identifies domain controllers that are failing inbound replication or outbound replication, and summarizes the results in a report.

netdom query dc > Identifier le contrôleur de domaine

netdom query fsmo > identifier le serveur qui a le rôle FSMO

dcdiag > diagnostiquer un problème avec le contrôleur de domaine

quser /server:vm-dc1.amfd.local > utilisateurs connectés à un serveur, depuis quand etc ...

logoff /server:vm-dc1.amfd.local 2

tester l’accès à \\domaine > tester l'accès FTP au dossier sysvol

Déploiement EXE par GPO et installation silencieuse

Comment déployer un logiciel au format EXE par GPO ? | IT-Connect

Au final ça n’a pas fonctionné pour moi > mais en BATCH oui :

La GPO ne s’applique pas, un fichier avec certificat semble attendu.

Déploiement du client Watchguard.

Script :

\\racetools.local\SysVol\racetools.local\Policies\{196DF44A-2EB6-4889-93CE-C81AD9AEC07B}\Machine\Scripts\Startup\install.exe /silent /verysilent /Components=main,tapdriver /tasks=desktopicon

Emplacement des fichiers :

\\racetools.local\SysVol\racetools.local\Policies\{196DF44A-2EB6-4889-93CE-C81AD9AEC07B}\Machine\Scripts\Startup

Filtrage WMI

Filtrer une GPO en fonction d'un OS en utilisant les filtres WMI

Pour filtrer sur tous les OS serveur

```
SELECT * from Win32_OperatingSystem where ProductType="3"
```

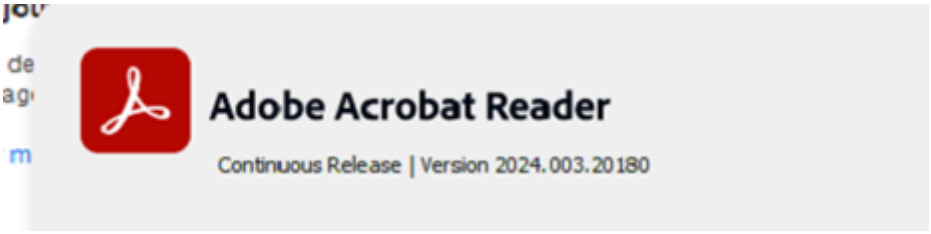
Pour filtrer sur tous les OS client

```
SELECT * from Win32_OperatingSystem where ProductType="1"
```

Acrobat Reader optimisation

Attention à la version. Cela influx sur la valeur de la clé : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\xxxxx\xxx

Les clés suivantes sont valables pour la version :



Configuration ordinateur (activée)

Stratégies

Modèles d’administration

Définitions de stratégies (fichiers ADMX) récupérées à partir du magasin central.

Système/Stratégie de groupe

Stratégie Paramètre Commentaire

Configurer le mode de traitement par bouclage de la stratégie de groupe utilisateur Activé

Mode : Remplacer

Configuration utilisateur (activée)

Préférences > Paramètres Windows > Registre

bProtectedMode (ordre : 1)

Général

Action Mettre à jour

Propriétés

Ruche HKEY_LOCAL_MACHINE

Chemin d’accès à la clé SOFTWARE\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown

Nom de la valeur bProtectedMode

Type de la valeur REG_DWORD

Données de la valeur 0x0 (0)

bSDIMode (ordre : 2)

Général

Action Mettre à jour

Propriétés

Ruche HKEY_CURRENT_USER

Chemin d’accès à la clé Software\Adobe\Acrobat Reader\DC\AVgeneral

Nom de la valeur bSDIMode

Type de la valeur REG_DWORD

Données de la valeur 0x1 (1)

bEnhancedSecurityInBrowser (ordre : 4)

Général

Action Mettre à jour

Propriétés

Ruche HKEY_CURRENT_USER

Chemin d’accès à la clé Software\Adobe\Acrobat Reader\DC\TrustManager

Nom de la valeur bEnhancedSecurityInBrowser

Type de la valeur REG_DWORD

Données de la valeur 0x0 (0)

bEnhancedSecurityStandalone (ordre : 5)

Général

Action Mettre à jour

Propriétés

Ruche HKEY_CURRENT_USER

Chemin d’accès à la clé Software\Adobe\Acrobat Reader\DC\TrustManager

Nom de la valeur bEnhancedSecurityStandalone

Type de la valeur REG_DWORD

Données de la valeur 0x0 (0)

iProtectedView (ordre : 6)

Général

Action Mettre à jour

Propriétés

Ruche HKEY_CURRENT_USER

Chemin d’accès à la clé Software\Adobe\Acrobat Reader\DC\TrustManager

Nom de la valeur iProtectedView

Type de la valeur REG_DWORD

Données de la valeur 0x0 (0)

bProtectedMode (ordre : 7)

Général

Action Mettre à jour

Propriétés

Ruche HKEY_CURRENT_USER

Chemin d’accès à la clé Software\Adobe\Acrobat Reader\DC\Privileged

Nom de la valeur bProtectedMode

Type de la valeur REG_DWORD

Données de la valeur 0x0 (0)

bShowMagAtLaunch (ordre : 8)

Général

Action Mettre à jour

Propriétés

Ruche HKEY_CURRENT_USER

Chemin d’accès à la clé Software\Adobe\Acrobat Reader\DC\IPM

Nom de la valeur bShowMagAtLaunch

Type de la valeur REG_DWORD

Données de la valeur 0x0 (0)

bDontShowMagWhenViewingDoc (ordre : 9)

Général

Action Mettre à jour

Propriétés

Ruche HKEY_CURRENT_USER

Chemin d’accès à la clé Software\Adobe\Acrobat Reader\DC\IPM

Nom de la valeur bDontShowMagWhenViewingDoc

Type de la valeur REG_DWORD

Données de la valeur 0x0 (0)

bToggleCustomOpenExperience (ordre : 10)

Général

Action Mettre à jour

Propriétés

Ruche HKEY_CURRENT_USER

Chemin d’accès à la clé Software\Adobe\Acrobat Reader\DC\AVgeneral

Nom de la valeur bToggleCustomOpenExperience

Type de la valeur REG_DWORD

Données de la valeur 0x1 (1)

bToggleCustomSaveExperience (ordre : 11)

Général

Action Mettre à jour

Propriétés

Ruche HKEY_CURRENT_USER

Chemin d’accès à la clé Software\Adobe\Acrobat Reader\DC\AVgeneral

Nom de la valeur bToggleCustomSaveExperience

Type de la valeur REG_DWORD

Données de la valeur 0x1 (1)

bToggleCustomOpenExperience (ordre : 12)

Général

Action Mettre à jour

Propriétés

Ruche HKEY_CURRENT_USER

Chemin d’accès à la clé software\Adobe\Acrobat Reader\DC\FeatureLockDown

Nom de la valeur bToggleCustomOpenExperience

Type de la valeur REG_DWORD

Données de la valeur 0x1 (1)

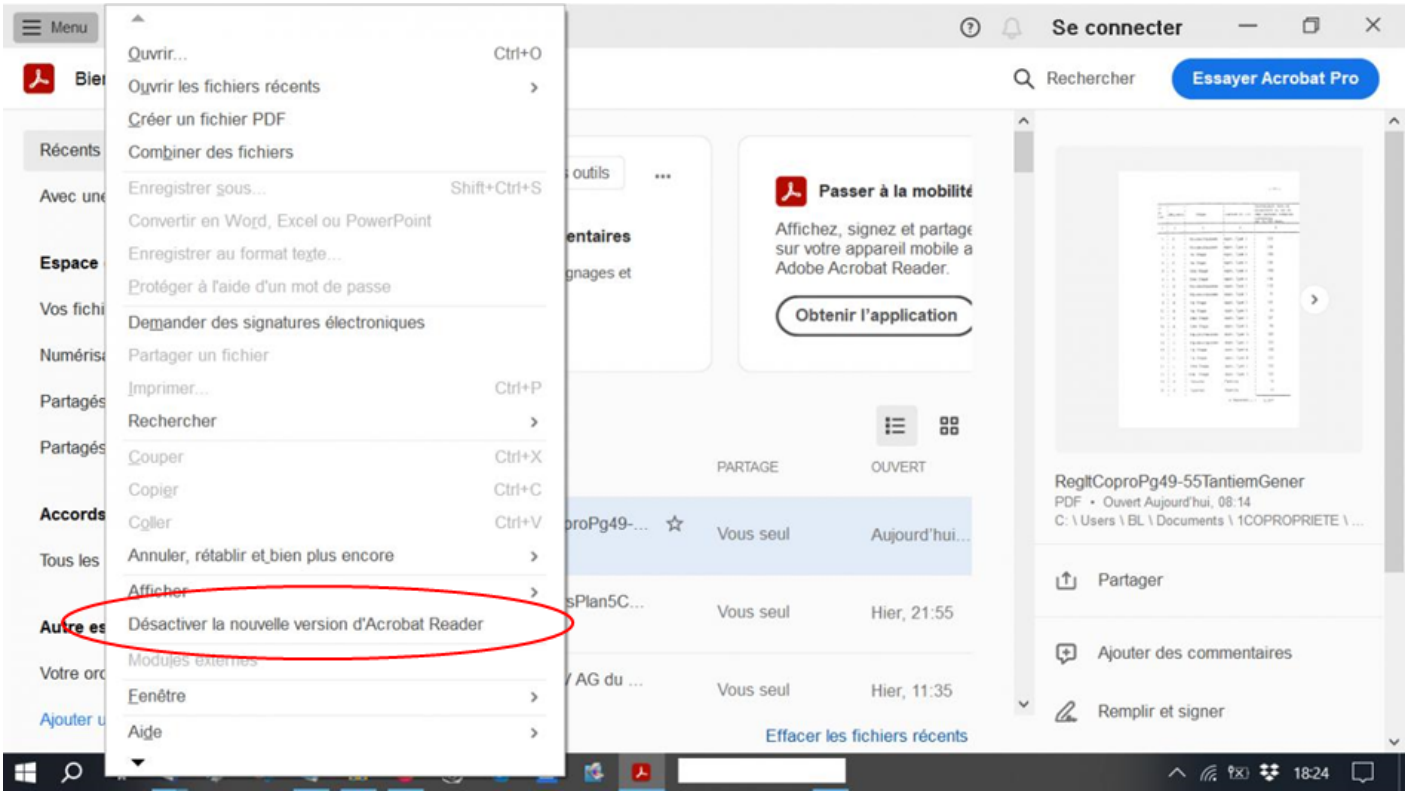
bEnableAV2

Mettre à jour

HKEY_CURRENT_USER

Software\Adobe\Adobe Acrobat\DC\AVGeneral

bEnableAV2 REG_DWORD 00000000


Menu
Se connecter
Rechercher
Essayer Acrobat Pro
Ouvrir... Ctrl+O
Ouvrir les fichiers récents
Créer un fichier PDF
Combiner des fichiers
Enregistrer sous... Shift+Ctrl+S
Convertir en Word, Excel ou PowerPoint
Enregistrer au format texte...
Protéger à l'aide d'un mot de passe
Demander des signatures électroniques
Partager un fichier
Imprimer... Ctrl+P
Rechercher
Couper Ctrl+X
Copier Ctrl+C
Coller Ctrl+V
Annuler, rétablir et bien plus encore
Afficher
Désactiver la nouvelle version d'Acrobat Reader
Modules externes
Fenêtre
Aide
Passer à la mobilité
Affichez, signez et partage
sur votre appareil mobile a
Adobe Acrobat Reader.
Obtenir l'application
PARTAGE
OUVERT
Vous seul
Aujourd'hui...
Vous seul
Hier, 21:55
Vous seul
Hier, 11:35
Effacer les fichiers récents
RegltCoproPg49-55TantiemGener
PDF • Ouvert Aujourd'hui, 08:14
Partager
Ajouter des commentaires
Remplir et signer
18:24