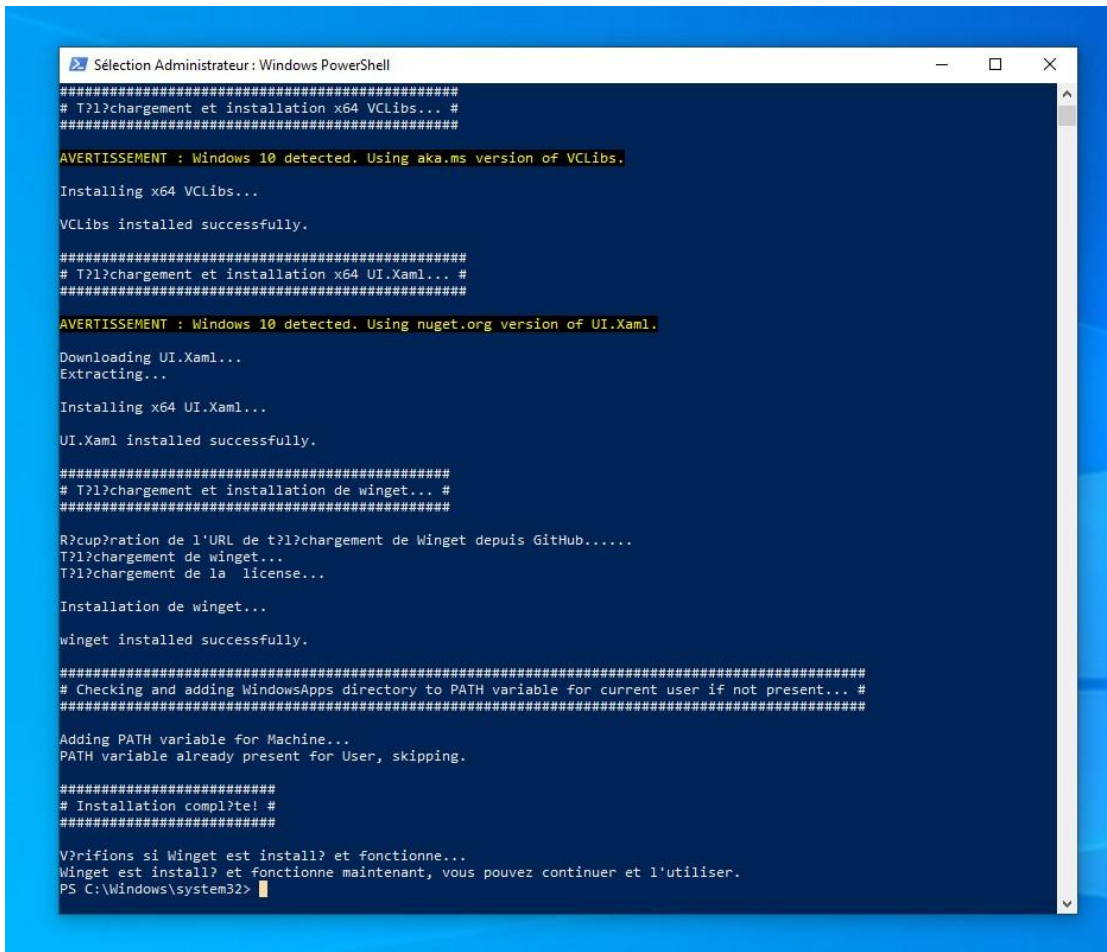


Documentation W10 Projet Cyber

Installation de WinGet

iwr -useb <https://raw.githubusercontent.com/sbeteta42/winget/main/winget-install.ps1> | iex



```
Sélection Administrateur : Windows PowerShell
#####
# T?l?chargement et installation x64 VCLibs... #
#####
AVERTISSEMENT : Windows 10 detected. Using aka.ms version of VCLibs.
Installing x64 VCLibs...
VCLibs installed successfully.
#####
# T?l?chargement et installation x64 UI.Xaml... #
#####
AVERTISSEMENT : Windows 10 detected. Using nuget.org version of UI.Xaml.
Downloading UI.Xaml...
Extracting...
Installing x64 UI.Xaml...
UI.Xaml installed successfully.
#####
# T?l?chargement et installation de winget... #
#####
R?cup?ration de l'URL de t?l?chargement de Winget depuis GitHub.....
T?l?chargement de winget...
T?l?chargement de la license...
Installation de winget...
winget installed successfully.
#####
# Checking and adding WindowsApps directory to PATH variable for current user if not present... #
#####
Adding PATH variable for Machine...
PATH variable already present for User, skipping.
#####
# Installation compl?te! #
#####
V?rifions si Winget est install? et fonctionne...
Winget est install? et fonctionne maintenant, vous pouvez continuer et l'utiliser.
PS C:\Windows\system32>
```

Winget est un outil sur Windows qui aide à installer et à mettre à jour des logiciels plus facilement, sans avoir à chercher sur internet.

1. Paramètres Biométriques et d'écran de Verrouillage

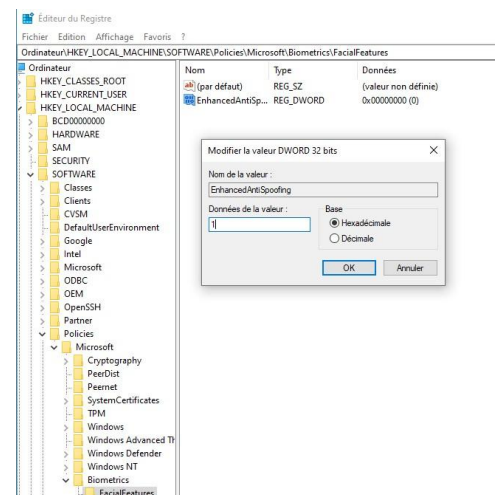
1.1 Amélioration de la protection Anti-Spoofing pour la reconnaissance faciale

L'amélioration de la protection anti-spoofing pour la reconnaissance faciale renforce la sécurité en réduisant le risque d'accès non autorisé par des méthodes de falsification d'images ou de vidéos.

1. Tapez "regedit" dans la boîte de dialogue et appuyez sur Entrée. Cela ouvrira l'Éditeur du Registre.
2. Naviguez jusqu'à la clé suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Biometrics\FacialFeatures

3. Si la clé "FacialFeatures" n'existe pas, vous devrez la créer. Faites un clic droit sur "Microsoft", choisissez "Nouveau" > "Clé" et nommez-la "Biometrics". Ensuite, créez une nouvelle clé sous "Biometrics" et nommez-la "FacialFeatures".
4. Une fois que vous êtes dans la clé "FacialFeatures", faites un clic droit dans le volet droit, choisissez "Nouveau" > "Valeur DWORD (32 bits)".
5. Nommez cette valeur "EnhancedAntiSpoofing".
6. Double-cliquez sur "EnhancedAntiSpoofing" et attribuez-lui une donnée de valeur "1" pour l'activer.
7. Fermez l'Éditeur du Registre.



1.2 Désactivation de l'utilisation de la caméra sur l'écran de verrouillage

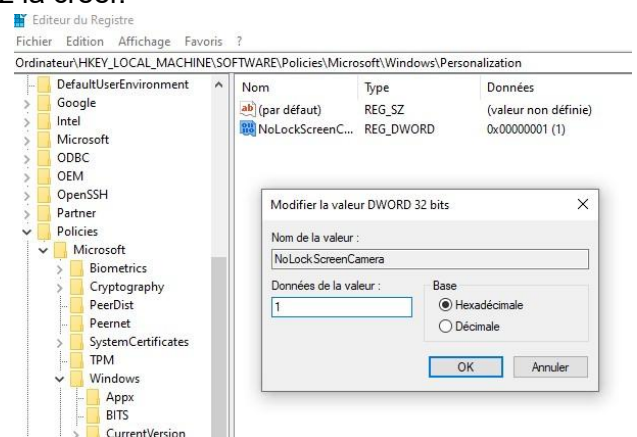
La désactivation de l'utilisation de la caméra sur l'écran de verrouillage renforce la confidentialité en empêchant l'accès non autorisé à la caméra de l'appareil, réduisant ainsi le risque de surveillance indésirable ou d'exploitation de la vie privée.

1. Accédez à la clé suivante dans l'Éditeur du Registre :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Personalization

2. Si la clé "Personalization" n'existe pas, vous devrez la créer.

3. Créez une nouvelle valeur DWORD (32 bits) nommée "NoLockScreenCamera" si elle n'existe pas déjà.
4. Définissez sa valeur sur 1 pour désactiver l'utilisation de la caméra sur l'écran de verrouillage.
5. Redémarrez votre ordinateur pour appliquer les modifications.



1.3 Empêchement de l'activation vocale des applications sur un appareil verrouillé

La désactivation de l'activation vocale des applications sur un appareil verrouillé renforce la confidentialité en limitant l'accès aux fonctionnalités vocales sensibles lorsque l'appareil est sécurisé, réduisant ainsi le risque d'utilisation non autorisée ou de divulgation de données personnelles.

1. Accédez à la clé suivante dans l'Éditeur du Registre :

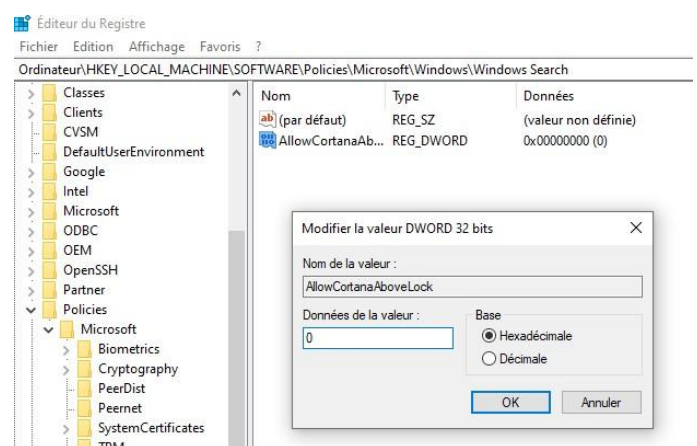
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search

2. Si la clé "Windows Search" n'existe pas, vous devrez la créer.

3. Créez une nouvelle valeur DWORD (32 bits) nommée "AllowCortanaAboveLock" si elle n'existe pas déjà.

4. Définissez sa valeur sur 0 pour empêcher l'activation vocale des applications sur un appareil verrouillé.

5. Redémarrez votre ordinateur pour appliquer les modifications.



2. DNS et Sécurité Réseau

2.1 Désactivation de la diffusion DNS Multicast et des requêtes parallèles A et AAAA

La désactivation de la diffusion DNS multicast renforce la sécurité en limitant la visibilité des requêtes DNS, réduisant ainsi le risque d'exposition involontaire d'informations sensibles et de potentielles attaques.

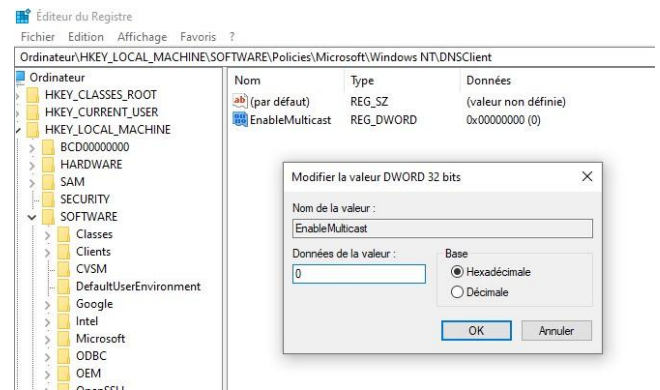
1. Ouvrez l'Éditeur du Registre (regedit).

2. Accédez à la clé suivante :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters

3. Créez une nouvelle valeur DWORD (si elle n'existe pas déjà) nommée "EnableMulticast" et définissez sa valeur sur 0 pour désactiver la diffusion DNS multicast.

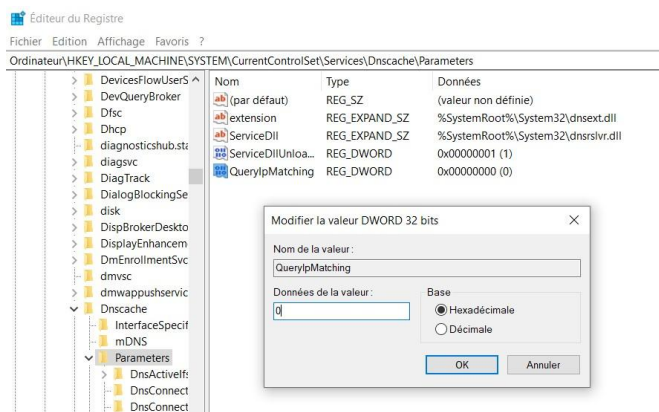
4. Redémarrez votre ordinateur pour que les modifications prennent effet.



Il est aussi possible de désactiver QueryLpMatching ce qui permet de renforcer la confidentialité en empêchant la correspondance basée sur les emplacements locaux dans les requêtes DNS, réduisant ainsi le risque de divulgation d'informations sensibles sur la localisation.

1. Accédez à la clé suivante dans l'Éditeur du Registre :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters



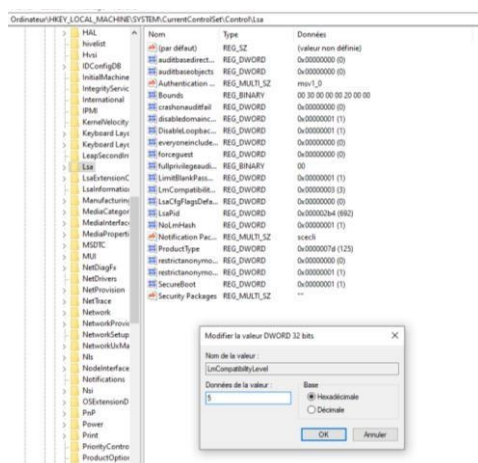
2. Créez une nouvelle valeur DWORD nommée "QueryLpMatching" si elle n'existe pas déjà.

3. Définissez sa valeur sur 0 pour désactiver la correspondance basée sur les emplacements locaux.

4. Redémarrez votre ordinateur pour appliquer les modifications.

2.2 Désactivation de NTLM v1

La désactivation de NTLMv1 via le Registre Windows renforce la sécurité en éliminant une méthode de hachage de mot de passe moins sécurisée, réduisant ainsi le risque d'exploitation par des attaques de type relais NTLM.



1. Accédez à la clé suivante dans l'Éditeur du Registre :

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

2. Créez une nouvelle valeur DWORD 32 bits nommée "LmCompatibilityLevel" si elle n'existe pas déjà.

3. Définissez sa valeur sur 5 pour désactiver NTLMv1.

4. Redémarrez votre ordinateur pour appliquer les modifications.

2.3 Désactivation de SMB v1

La désactivation de SMBv1 via le Registre Windows renforce la sécurité en éliminant un protocole réseau obsolète et vulnérable, réduisant ainsi le risque d'exploitation par des attaques telles que WannaCry et d'autres menaces similaires.

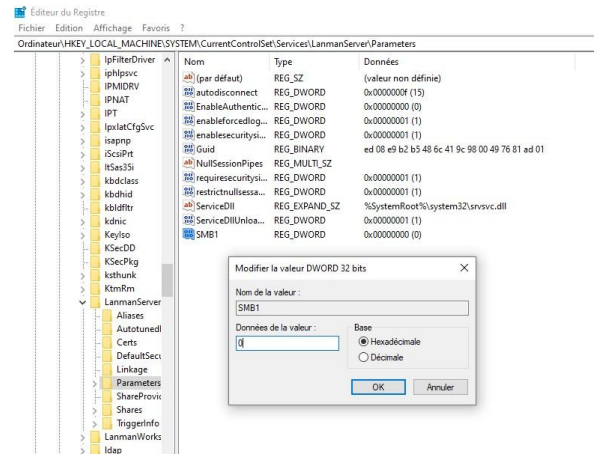
1. Accédez à la clé suivante dans l'Éditeur du Registre :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

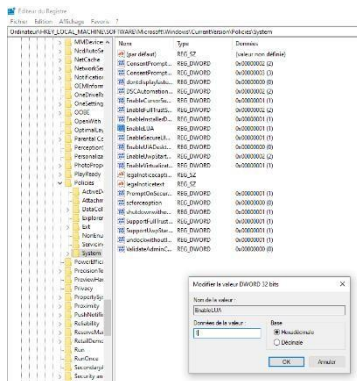
2. Créez une nouvelle valeur DWORD nommée "SMB1" si elle n'existe pas déjà.

3. Définissez sa valeur sur 0 pour désactiver SMBv1.

4. Redémarrez votre ordinateur pour appliquer les modifications.



2.4 Activation de l'UAC et configuration des paramètres associés



L'activation de l'UAC (Contrôle de compte d'utilisateur) renforce la sécurité en demandant une confirmation de l'utilisateur avant d'autoriser les actions nécessitant des privilèges administratifs, réduisant ainsi le risque d'exécution involontaire de logiciels malveillants ou de modifications non autorisées du système.

1. Accédez à la clé suivante dans l'Éditeur du Registre :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

2. Modifiez ou créez une valeur DWORD nommée "EnableLUA".

3. Définissez sa valeur sur 1 pour activer l'UAC.

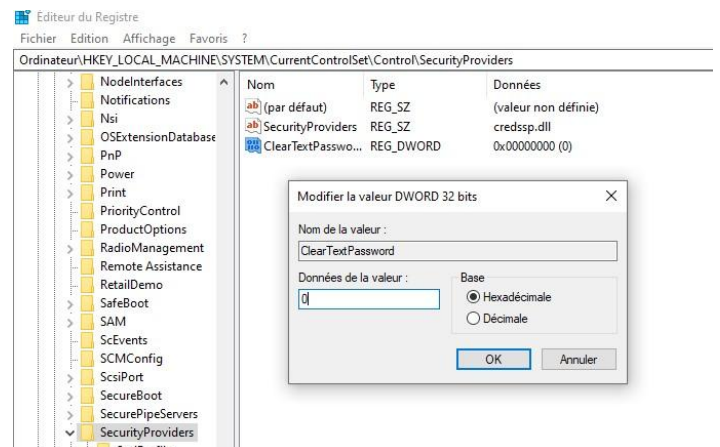
4. Redémarrez votre ordinateur pour appliquer les modifications.

3. Sécurité des mots de passe et de l'authentification

3.1 Désactivation de l'enregistrement des mots de passe en clair en mémoire

La désactivation de l'enregistrement des mots de passe en clair en mémoire renforce la sécurité en empêchant la rétention non cryptée des mots de passe sensibles, réduisant ainsi le risque de compromission des informations d'identification.

1. Ouvrez l'Éditeur du Registre en appuyant sur Windows + R, puis en tapant "regedit" dans la boîte de dialogue et en appuyant sur Entrée.
2. Accédez à la clé suivante dans l'Éditeur du Registre
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders
3. Faites un clic droit sur la zone vide à droite, pointez sur "Nouveau", puis sélectionnez "Valeur chaîne".
4. Nommez cette nouvelle valeur "ClearTextPassword".
5. Double-cliquez sur la valeur nouvellement créée et attribuez-lui une donnée de valeur vide ou supprimez-la.
6. Cliquez sur "OK" pour enregistrer les modifications.
7. Fermez l'Éditeur du Registre.
8. Redémarrez votre ordinateur pour que les modifications prennent effet.



3.2 Restriction des types de chiffrement Kerberos

Kerberos est un protocole d'authentification réseau sécurisé qui permet aux utilisateurs de prouver leur identité sur un réseau non sécurisé à l'aide d'échanges de tickets chiffrés, évitant ainsi la transmission de mots de passe en clair.

1. Appuyez sur la touche Windows + R pour ouvrir la boîte de dialogue Exécuter.
2. Tapez regedit et appuyez sur Entrée pour ouvrir l'Éditeur du Registre.
3. Accédez à l'emplacement suivant dans l'arborescence de l'Éditeur du Registre :
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters
4. Dans le volet droit de l'Éditeur du Registre, recherchez ou créez les valeurs suivantes :
 - Pour restreindre les types de chiffrement des tickets Kerberos, créez ou modifiez la valeur DWORD (32 bits) nommée SupportedEncryptionTypes.
 - Pour restreindre les types de chiffrement pour l'authentification Kerberos preauthentification, créez ou modifiez la valeur DWORD (32 bits) nommée SupportedPreauthAlgorithms.

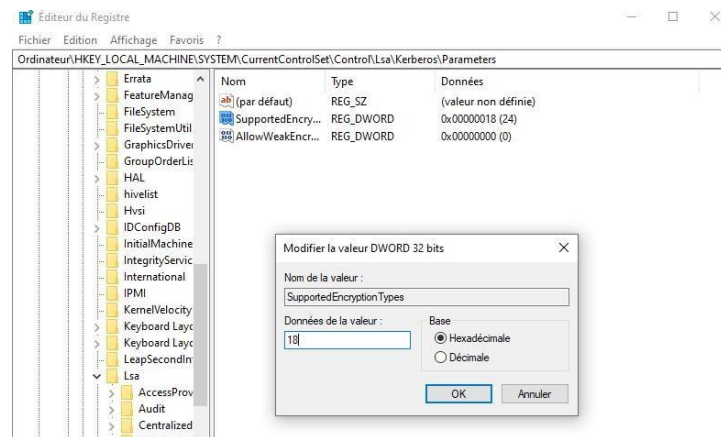
5. Double-cliquez sur la valeur créée ou modifiée pour ouvrir la boîte de dialogue Modifier la valeur DWORD.

6. Dans la boîte de dialogue Modifier la valeur DWORD, saisissez la valeur correspondant à la combinaison des types de chiffrement que vous souhaitez autoriser, en utilisant des valeurs hexadécimales :

- Pour les types de chiffrement des tickets Kerberos, vous pouvez utiliser des combinaisons de :
 - 0x1 pour DES_CBC_CRC (Désuet et peu sécurisé)
 - 0x2 pour DES_CBC_MD5 (Désuet et peu sécurisé)
 - 0x4 pour RC4_HMAC_MD5 (Désuet et peu sécurisé)
 - 0x8 pour AES128_CTS_HMAC_SHA1_96
 - 0x10 pour AES256_CTS_HMAC_SHA1_96
- Pour les types de chiffrement pour l'authentification Kerberos pré-authentification, les valeurs possibles dépendent de la version de Windows que vous utilisez. Les valeurs incluent généralement 0x1 pour AES128-CTS-HMAC-SHA1-96 et 0x2 pour AES256CTS-HMAC-SHA1-96.

7. Cliquez sur OK pour enregistrer la valeur.

8. Fermez l'Éditeur du Registre.

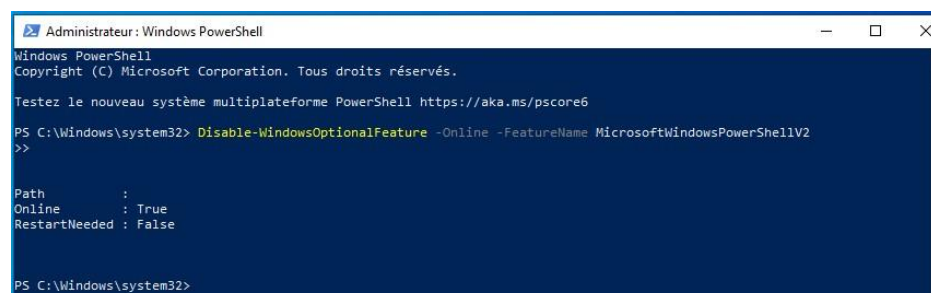
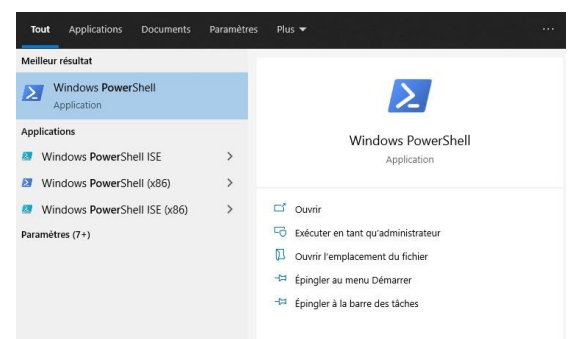


3.3 Désactivation de PowerShell V2

Désactiver PowerShell V2 renforce la sécurité en éliminant les vulnérabilités potentielles, tout en favorisant la compatibilité et les performances optimales avec les versions plus récentes du logiciel. Pour désactiver PowerShell V2 à l'aide de PowerShell, vous pouvez suivre ces étapes :

1. Ouvrez PowerShell en tant qu'administrateur. Pour ce faire, recherchez "PowerShell" dans le menu Démarrer, faites un clic droit sur "Windows PowerShell" et sélectionnez "Exécuter en tant qu'administrateur".

2. Une fois dans PowerShell, exécutez la



commande suivante pour désactiver PowerShell V2 :

Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2

Une fois la commande exécutée avec succès, PowerShell V2 sera désactivé sur votre système.

3.4 Désactivation de l'AutoRun

La désactivation de l'AutoRun empêche les programmes malveillants d'être exécutés automatiquement à partir de périphériques de stockage amovibles tels que les clés USB, réduisant ainsi le risque d'infection par des logiciels malveillants.

1. Dans l'Éditeur du Registre, naviguez jusqu'à la clé suivante :

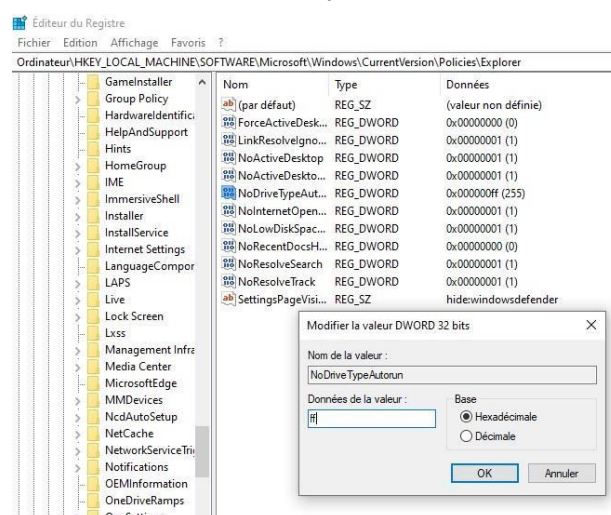
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

2. Si vous ne trouvez pas la clé "Explorer", vous pouvez la créer. Pour cela, faites un clic droit sur "Policies", sélectionnez "Nouveau" puis "Clé" et nommez-la "Explorer".

3. Dans la clé "Explorer", faites un clic droit sur un espace vide du volet droit, sélectionnez "Nouveau" puis "Valeur DWORD (32 bits)".

4. Nommez cette valeur "NoDriveTypeAutoRun".

5. Double-cliquez sur "NoDriveTypeAutoRun" pour modifier sa valeur.



6. Dans la boîte de dialogue qui s'ouvre, entrez la valeur correspondante à vos besoins. Pour désactiver complètement l'autorun, vous devez saisir "FF" en hexadécimal.

7. Fermez l'Éditeur du Registre.

8. Redémarrez votre ordinateur pour que les modifications prennent effet.

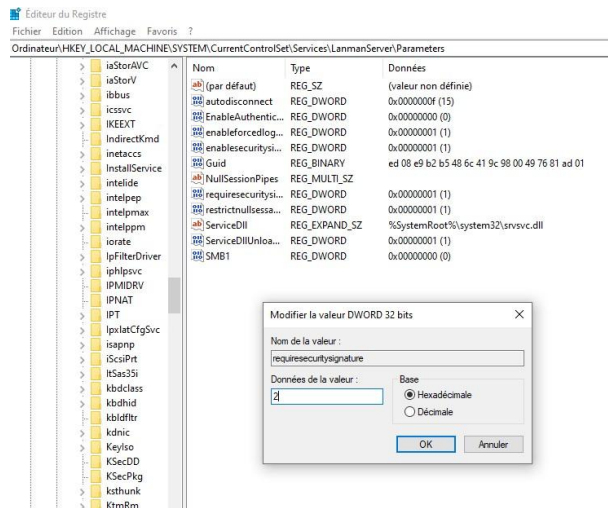
4. Protection Réseau

4.1. Activation de la signature SMB/LDAP

1. Accédez à la clé suivante dans l'Éditeur du Registre :

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters

2. Si la clé "Parameters" n'existe pas, vous devrez la créer.
3. Créez une nouvelle valeur DWORD (32 bits) nommée "RequireSecuritySignature" si elle n'existe pas déjà.



4. Définissez sa valeur sur 2 pour activer la signature SMB/LDAP.

- 0 : Désactive la signature de sécurité SMB/LDAP.
- 1 : Active la signature de sécurité SMB/LDAP pour les connexions sortantes, mais n'oblige pas les autres ordinateurs à signer les paquets.
- 2 : Active la signature de sécurité SMB/LDAP pour les connexions sortantes et exige que les autres ordinateurs signent les paquets.

5. Redémarrez votre ordinateur pour appliquer les modifications.

4.2 Configuration des paramètres de sécurité des membres de domaine

1. Accédez à la clé suivante dans l'Éditeur du Registre :

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters`

2. Créez ou modifiez les valeurs DWORD appropriées pour configurer les paramètres de sécurité des membres de domaine :

- `RequireSignOrSeal` : 1 pour exiger la signature ou le scellement des communications.
- `RequireStrongKey` : 1 pour exiger l'utilisation de clés Kerberos sécurisées.
- `SealSecureChannel` : 1 pour sceller le canal de communication entre les membres du domaine.
- `SignSecureChannel` : 1 pour signer le canal de communication entre les membres du domaine.

3. Redémarrez votre ordinateur pour appliquer les modifications.

4.3 Activation de SmartScreen

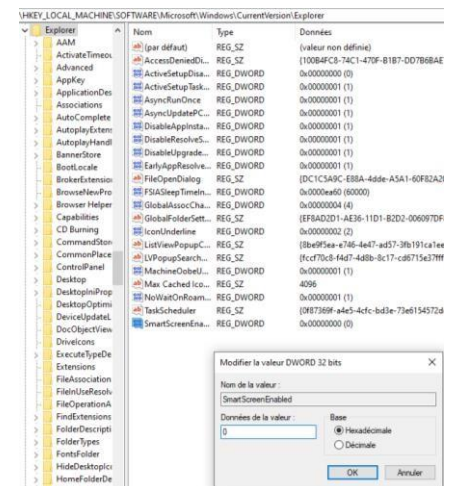
L'activation de SmartScreen renforce la sécurité en fournissant une protection contre les logiciels malveillants et les sites Web dangereux en analysant les fichiers et les URL téléchargés, réduisant ainsi le risque d'infection par des logiciels malveillants ou de navigation sur des sites potentiellement nuisibles.

Pour activer SmartScreen via le Registre Windows :

1. Accédez à la clé suivante dans l'Éditeur du Registre :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

2. Créez ou modifiez une valeur DWORD (32 bits) nommée "SmartScreenEnabled" si elle n'existe pas déjà.
3. Définissez sa valeur sur 1 pour activer SmartScreen.
4. Redémarrez votre ordinateur pour que les modifications prennent effet.



5. Paramètres de Windows Defender

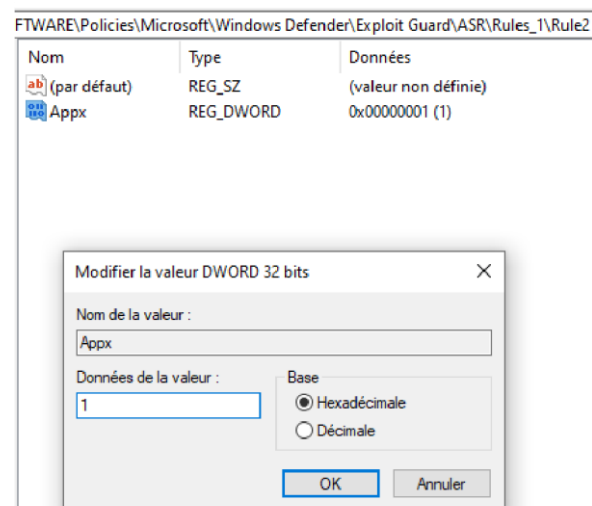
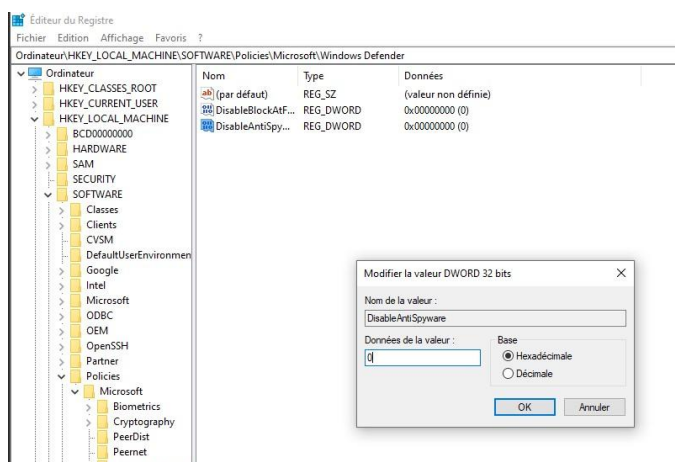
5.1 Activation de diverses protections dans Windows Defender

La modification du paramètre "disableantispware" dans le Registre Windows en le définissant sur 0 permet d'activer la fonctionnalité d'antispware de Windows Defender, renforçant ainsi la protection contre les logiciels espions et les menaces liées à la sécurité.

1. Accédez à la clé suivante dans l'Éditeur du Registre :

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender

2. Trouvez ou créez une valeur DWORD (32 bits) nommée "disableantispware".



3. Double-cliquez sur "disableantispyware" et définissez sa valeur sur 0 pour activer l'antispyware.
4. Redémarrez votre ordinateur pour que les modifications prennent effet.

5.2 Configuration des fonctionnalités cloud et des protections contre les exploits système.

Ces modifications dans le registre permettent de configurer les règles spécifiques de protection contre les exploits dans Windows Defender Exploit Guard, renforçant ainsi la sécurité en prévenant les attaques d'exploitation système sur votre système d'exploitation Windows.

1. Ouvrez l'Éditeur du Registre en appuyant sur Windows + R, puis en tapant "regedit" dans la boîte de dialogue et en appuyant sur Entrée.

Accédez à la première clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Defender\ExploitGuard\ASR\Rules_1\Rule1

2. Trouvez la valeur DWORD nommée "Appx". Si elle n'existe pas, vous devrez la créer.
3. Double-cliquez sur cette valeur pour la modifier.
4. Mettez la valeur à 1 pour activer
5. Répétez les étapes 2 à 5 pour la deuxième clé :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Defender\ExploitGuard\ASR\Rules_1\Rule2

6. Une fois que vous avez modifié les valeurs selon vos besoins, fermez l'Éditeur du Registre.

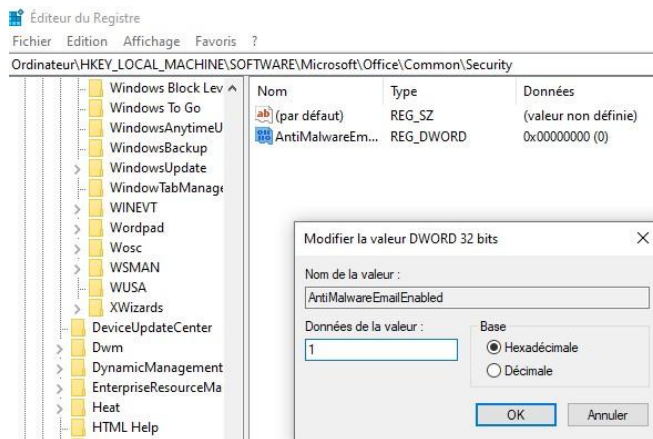
6. Sécurité MS Office

6.1 Sécurisation de diverses versions de MS Office contre les attaques de malspam.

Voici les étapes pour activer le paramètre "AntiMalwareEmailEnabled" en utilisant le nouveau chemin dans le Registre Windows :

1. Dans l'Éditeur du Registre, naviguez jusqu'à la clé suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Office\Common\Security



2. Si la clé "Security" n'existe pas, vous pouvez la créer. Cliquez avec le bouton droit sur "Common", choisissez

"Nouveau" > "Clé" et nommez-la "Security".

3. Assurez-vous que vous êtes dans la clé "Security". Cliquez avec le bouton droit dans le volet droit, choisissez "Nouveau" > "Valeur DWORD (32 bits)".

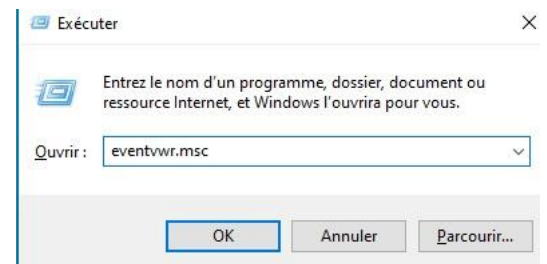
4. Nommez cette nouvelle valeur "AntiMalwareEmailEnabled".

5. Double-cliquez sur "AntiMalwareEmailEnabled" et attribuez-lui une donnée de valeur "1" pour activer la fonctionnalité.

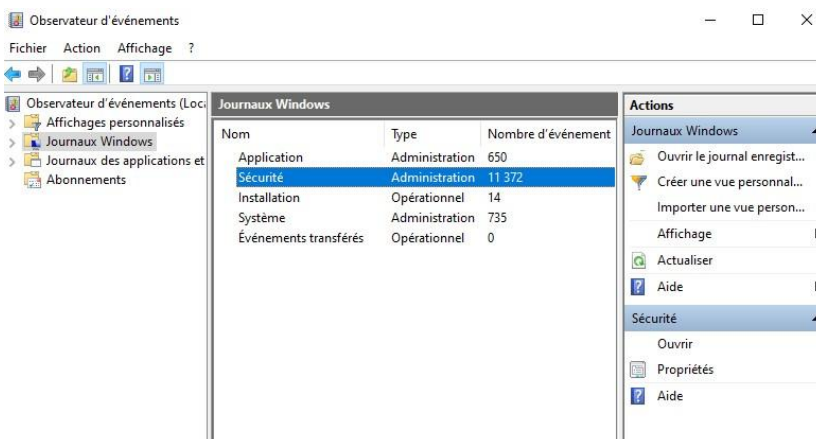
7. Journalisation des Événements Windows

7.1 Augmentation de la taille des journaux d'événements de sécurité

L'augmentation de la taille des journaux d'événements de sécurité permet de stocker davantage d'événements de sécurité, assurant une surveillance continue des activités critiques du système et facilitant l'analyse des incidents de sécurité.



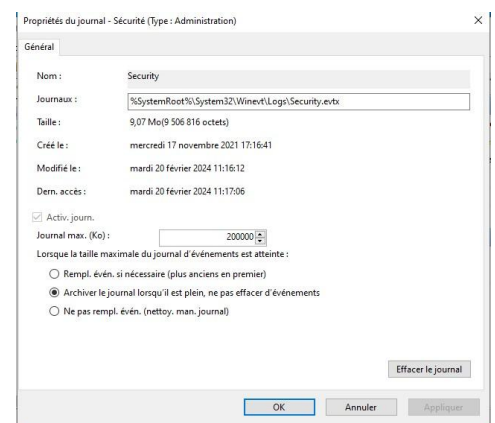
Pour augmenter la taille des journaux d'événements de sécurité :



1. Ouvrez l'Observateur d'événements en appuyant sur Windows + R, tapez "eventvwr.msc" dans la boîte de dialogue et appuyez sur Entrée.

2. Dans

l'Observateur d'événements, cliquez avec le bouton droit sur "Journal" dans le volet de gauche, puis sélectionnez "Propriétés".



3. Sous l'onglet "Général", vous pouvez ajuster la taille maximale du journal en utilisant le champ "Taille maximale du journal (KB)".
4. Augmentez la taille maximale selon vos besoins. Vous pouvez entrer la taille en kilo-octets (KB) ou en mégaoctets (MB).

7.2.A Activation de la journalisation des événements

L'activation de la journalisation du suivi des processus permet de surveiller et d'enregistrer les événements liés à l'exécution des processus sur le système. Cela aide à détecter et à analyser les activités suspectes ou malveillantes, fournissant ainsi une sécurité accrue en permettant une réponse plus rapide aux menaces potentielles.

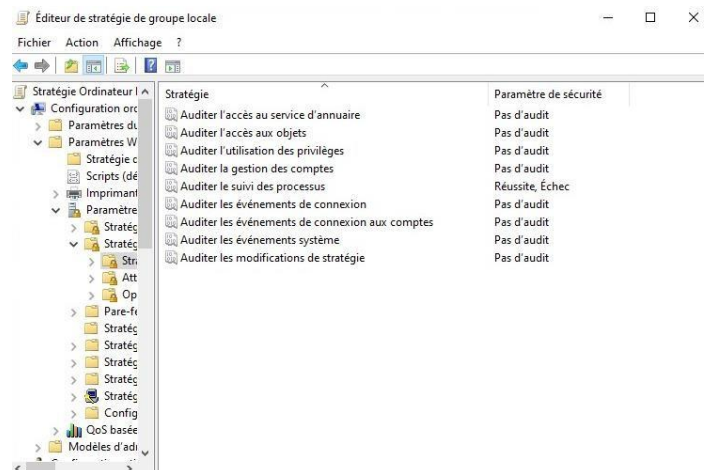


1. Ouvrez l'Éditeur de stratégie de groupe en appuyant sur Windows + R, tapez "gpedit.msc" dans la boîte de dialogue, puis appuyez sur Entrée.

2. Naviguez jusqu'à l'option suivante :

Configuration de l'ordinateur > Paramètres de sécurité > Stratégies locales > Stratégie d'audit
Dans le volet de droite, double-cliquez sur "Auditer le suivi des processus".

3. Sélectionnez "Activé" pour activer la journalisation du suivi des processus.



7.2.B Activation de la journalisation des données de ligne de commande

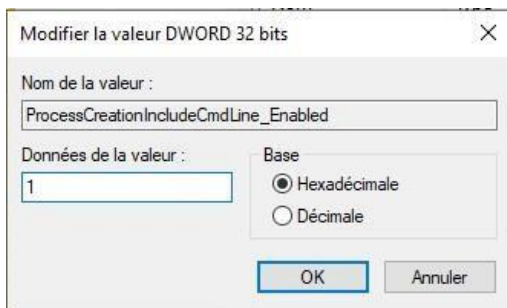
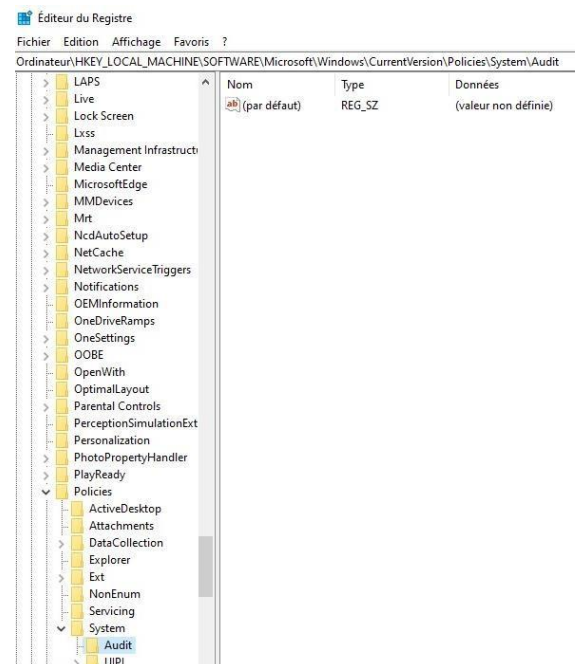
Activer l'inclusion de la ligne de commande lors de la journalisation de la création des processus permet de capturer les commandes exactes utilisées lors du lancement de processus, offrant ainsi une visibilité accrue sur les activités système et facilitant la détection des comportements malveillants ou suspects.

Voici les étapes pour modifier la clé de Registre mentionnée :

1. Dans l'Éditeur du Registre, naviguez jusqu'à la clé suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit

2. Si la clé "Audit" n'existe pas, vous pouvez la créer.
Cliquez avec le bouton droit sur "System", choisissez "Nouveau" > "Clé" et nommez-la "Audit".



3. Assurez-vous que vous êtes dans la clé "Audit". Cliquez avec le bouton droit dans le volet droit, choisissez "Nouveau" > "Valeur DWORD (32 bits)".

4. Nommez cette nouvelle valeur "ProcessCreationIncludeCmdLine_Enabled".

5. Double-cliquez sur "ProcessCreationIncludeCmdLine_Enabled" pour

modifier sa valeur.

6. Définissez la valeur sur "1" pour activer l'inclusion de la ligne de commande lors de la journalisation de la création des processus.

8. Mesures de Sécurité Avancées

8.1 Activation des paramètres de sécurité avancés

1. Dans l'Éditeur du Registre, naviguez jusqu'à la clé suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SecurityManager\CapabilityManager

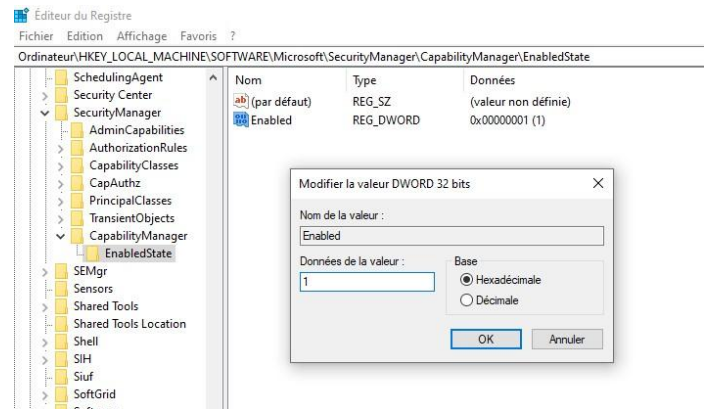
2. Si la clé "CapabilityManager" n'existe pas, vous pouvez la créer. Cliquez avec le bouton droit sur "SecurityManager", choisissez "Nouveau" > "Clé" et nommez-la "CapabilityManager".

3. Assurez-vous que vous êtes dans la clé "CapabilityManager". Cliquez avec le bouton droit dans le volet droit, choisissez "Nouveau" > "Valeur DWORD (32 bits)".

4. Nommez cette nouvelle valeur "EnabledState".

5. Double-cliquez sur "EnabledState" pour modifier sa valeur.

6. Définissez la valeur sur "1" pour activer les fonctionnalités de sécurité avancées.



L'activation de cette clé dans le Registre permet d'activer des fonctionnalités de sécurité avancées sur le système, renforçant ainsi sa protection contre les menaces et améliorant ses capacités de gestion et de contrôle d'accès.

8.2 Activation de la journalisation des modules PowerShell et des blocs de scripts

1. Accédez à la clé suivante dans l'Éditeur du Registre :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ScriptBlockLogging

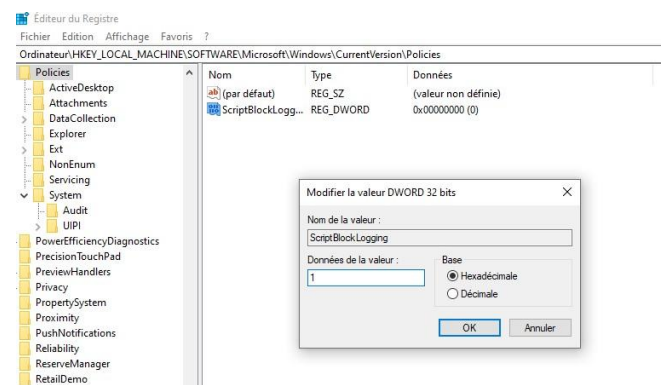
2. Si la clé "ScriptBlockLogging" n'existe pas, vous pouvez la créer. Cliquez avec le bouton droit sur "Policies", choisissez "Nouveau" > "Clé" et nommez-la "ScriptBlockLogging".

3. Assurez-vous que vous êtes dans la clé "ScriptBlockLogging". Cliquez avec le bouton droit dans le volet droit, choisissez "Nouveau" > "Valeur DWORD (32 bits)".

4. Nommez cette nouvelle valeur "EnableScriptBlockLogging".

5. Double-cliquez sur "EnableScriptBlockLogging" pour modifier sa valeur.

6. Définissez la valeur sur "1" pour activer la journalisation des blocs de scripts.



8.3 Configuration des politiques d'audit

1. Naviguez jusqu'au chemin suivant dans l'Éditeur du Registre :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security

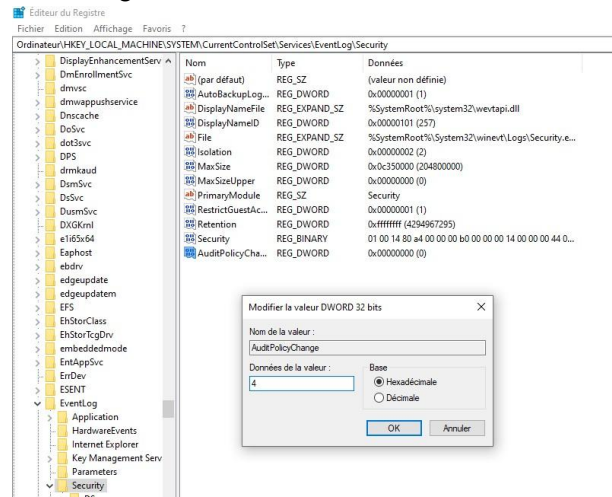
2. Cliquez avec le bouton droit sur la clé "System" dans le volet de gauche.

3. Choisissez "Nouveau" > "Valeur DWORD (32 bits)" dans le menu contextuel.

4. Nommez la nouvelle valeur DWORD

5. Double-cliquez sur la nouvelle valeur que vous venez de créer.

6. Dans la fenêtre "Modifier la valeur", saisissez "4" dans le champ "Données de la valeur".



9. Sécurité Issas

9.1 Renforcement de Issas contre le vol d'information d'identification

1. Naviguez jusqu'au chemin suivant dans l'Éditeur du Registre :

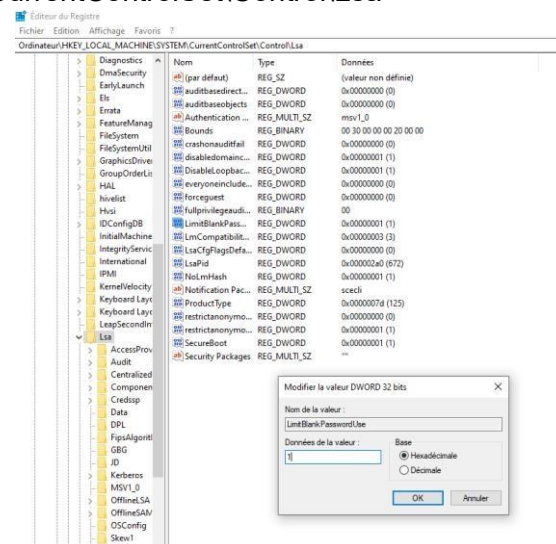
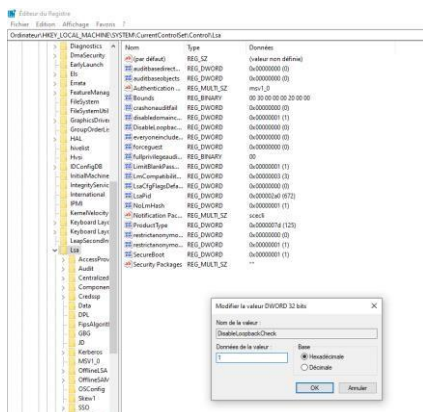
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

2. Double-cliquez sur la clé "DisableLoopbackCheck" dans le volet de droite.

3. Dans la fenêtre "Modifier la valeur DWORD", changez la valeur de "Données de la valeur" à "1".

4. Cliquez sur "OK" pour enregistrer la modification.

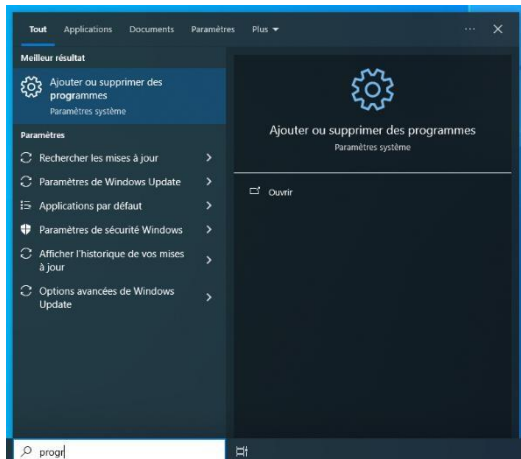
5. Répétez les étapes 4-6 pour la clé "LimitBlankPasswordUse".



10. Désinstallation des Applications Indésirables

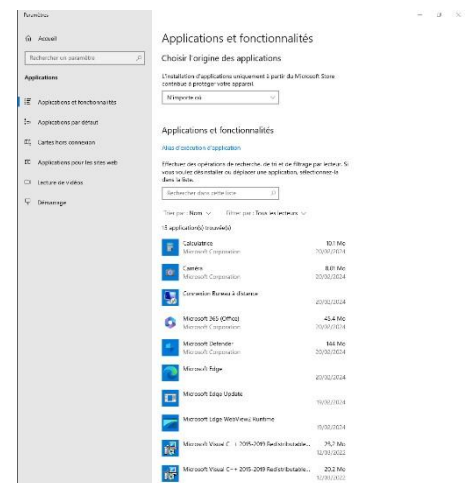
10.1 Suppression des applications intégrées inutiles

La démarche pour désinstaller une application :



1. Cliquez sur le bouton "Démarrer" dans la barre des tâches (icône de Windows).
2. Sélectionnez l'icône "Paramètres" (représentée par un engrenage) dans le menu Démarrer, ou appuyez sur Windows + I pour ouvrir les Paramètres.
3. Dans la fenêtre Paramètres, sélectionnez la catégorie "Applications".
4. Dans la barre latérale gauche, cliquez sur "Applications et fonctionnalités".

5. Attendez que la liste des applications installées sur votre système se charge.
6. Parcourez la liste des applications pour trouver celle que vous souhaitez désinstaller.
7. Sélectionnez l'application que vous souhaitez désinstaller en cliquant dessus.
8. Cliquez sur le bouton "Désinstaller" et suivez les instructions à l'écran pour confirmer la désinstallation de l'application.



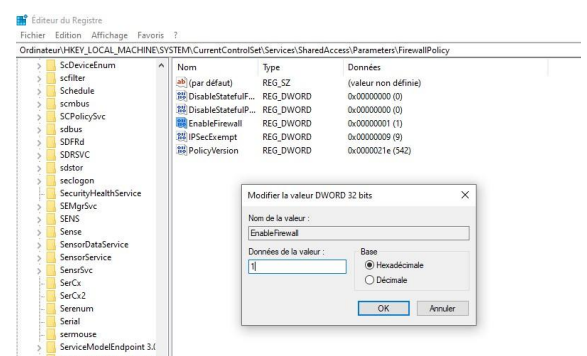
11. Pare-feu et Blocage des Connexions

11.1 Activation du Pare-feu Windows

1. Dans l'Éditeur du Registre, naviguez jusqu'au chemin suivant :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy

2. Assurez-vous d'être dans la clé "FirewallPolicy". Si la sous-clé "StandardProfile" existe, vous pouvez également naviguer jusqu'à elle.



3. Dans le volet droit de l'Éditeur du Registre, recherchez la valeur nommée "EnableFirewall".

4. Double-cliquez sur "EnableFirewall" pour modifier sa valeur.

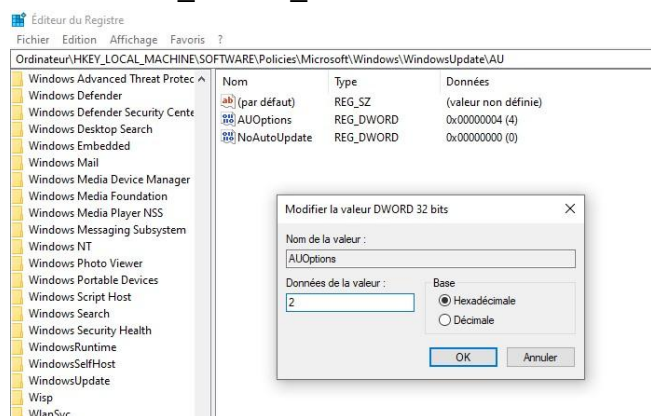
5. Dans la fenêtre "Modifier la valeur DWORD", changez la "Donnée de la valeur" à "1" pour activer le pare-feu Windows.

12. Mises à jour Windows et AutoRun

12.1 Activation des mises à jour automatiques de Windows

1. Naviguez jusqu'au chemin spécifié :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU



2. Dans le volet de droite, recherchez la valeur "AUOptions".

3. Double-cliquez sur "AUOptions" pour modifier sa valeur.

4. Dans la fenêtre qui s'ouvre, changez la "Donnée de la valeur" à "2".

Mot de passe pour accéder au BIOS

Mettre un mot de passe pour accéder au BIOS renforce la sécurité en empêchant les modifications non autorisées de la configuration matérielle, protégeant ainsi les données sensibles. De plus, cela limite le démarrage à partir de périphériques externes, réduisant ainsi les risques d'exécution de logiciels malveillants. En somme, cette mesure renforce la protection globale de l'ordinateur contre les menaces potentielles.

Dans un premier temps mettez le PassWord on boot en Enabled afin de l'activer.

Dans un second temps, définissez un mot de passe sur le paramètre Set Supervisor PassWord, ce qui ajoutera un mot de passe pour se connecter au bios de votre machine.

Il est aussi possible de définir un mot de passe sur Set User Password afin de définir un mot de passe au lancement de votre machine.

