Réinitialisation du SID Windows

- Procédure de réinitialisation du SID d'un PC

Procédure de réinitialisation du SID d'un PC

Contexte et utilité

Le SID (Security Identifier) est un identifiant unique attribué à chaque ordinateur Windows. Cette procédure permet de réinitialiser le SID d'un PC, ce qui est utile dans les cas suivants :

- Problèmes de connexion SMB entre deux postes
- Suite à un clonage de disque ou d'ordinateur
- Erreurs de connexion au domaine ou aux partages réseau
- Conflits de SID identiques sur le réseau

> **Note :** Cette procédure modifie le SID de l'ordinateur, pas celui d'un utilisateur. Assurez-vous de sauvegarder vos données importantes avant de commencer.

Étape 1 : Récupération du SID actuel

Cette étape permet de noter le SID actuel pour vérifier après la modification que le changement a bien été effectué.

1.1 Téléchargement de l'outil PsGetSid

Téléchargez l'outil PsGetSid depuis le site officiel de Microsoft : https://learn.microsoft.com/en-us/sysinternals/downloads/psgetsid

1.2 Extraction et exécution

1. Dézippez l'archive téléchargée dans un dossier de votre choix
2. Ouvrez un terminal PowerShell ou CMD dans ce dossier (clic droit > Ouvrir dans le terminal)
3. Exécutez la commande suivante :

```
.\psgetsid64.exe
```

4. Notez le SID affiché (il commence généralement par `S-1-5-21-...`). Cette information sera nécessaire pour vérifier que la modification a bien fonctionné.

Étape 2 : Changement du SID

> ⚠ **ATTENTION :** Cette étape modifie le système. Assurez-vous de bien suivre toutes les instructions.

2.1 Désactivation de l'antivirus (TRÈS IMPORTANT)

Avant de procéder au changement de SID, vous devez impérativement désactiver **tous** les antivirus présents sur le système :

- **ESET** (si installé) : Si c'est pour un particulier ou sur du Nod32 vous pouvez le faire directement sur le produit de sécurité. Si c'est du MSP alors il faut crée une politique de désactivation dans la console.
- **Windows Defender** : Paramètres > Confidentialité et sécurité > Sécurité Windows > Protection contre les virus et menaces > Gérer les paramètres > Désactiver la protection en temps réel

> ⚠ **Important :** Le non-respect de cette étape peut entraîner l'échec de la procédure ou des dysfonctionnements du système. Même si les deux antivirus sont installés, la désactivation d'ESET seul ne suffira pas.

2.2 Téléchargement de l'outil SIDCHG

Téléchargez l'outil SIDCHG64 depuis le site officiel : https://www.stratesave.com/html/sidchg.html

> **Important :** Téléchargez bien la version **SIDCHG64** (version 64 bits).

2.3 Exécution de l'outil

1. Ouvrez un terminal **en tant qu'administrateur** (PowerShell ou CMD) dans le dossier contenant l'exécutable
2. Exécutez la commande suivante :

```
.\sidchg64-3.0n.exe /R
```

3. L'outil va vous demander une clé de licence

2.4 Saisie de la clé de licence

La clé de licence gratuite est disponible sur le site de Stratesave.

> **Note :** La clé peut changer périodiquement. Consultez toujours le site officiel pour obtenir la clé actuelle.

2.5 Redémarrage du système

1. Après avoir saisi la clé, vérifiez qu'une ligne vous demande de redémarrer avec une validation `Y/N`
2. Tapez `Y` et appuyez sur Entrée
3. Le PC va redémarrer automatiquement

> ⚠ **IMPORTANT :** Pendant le redémarrage, un message peut s'afficher indiquant que le SID est en cours de modification. **Ne touchez à rien** et attendez que le redémarrage soit complètement terminé. Toute interruption pourrait corrompre le système.

Étape 3 : Vérification

3.1 Vérification du changement de SID

Une fois le PC redémarré, vérifiez que le SID a bien été modifié :

1. Ouvrez à nouveau un terminal dans le dossier contenant PsGetSid
2. Exécutez à nouveau la commande :

```
.\psgetsid64.exe
```

3. Comparez le nouveau SID avec celui que vous aviez noté à l'étape 1. Ils doivent être différents.

3.2 Test de connexion

Testez la connexion réseau ou l'accès au partage SMB qui posait problème.

- **Si la connexion fonctionne :** La procédure est terminée avec succès. Vous pouvez réactiver vos antivirus.
- **Si la connexion ne fonctionne toujours pas :**
  - Vérifiez d'abord que le SID a bien été modifié (étape 3.1)
  - Si le SID n'a pas changé, recommencez la procédure en vous assurant d'avoir bien désactivé les antivirus
  - Si le SID a changé mais le problème persiste, le souci peut provenir d'une autre cause

---

Dépannage

Le SID n'a pas changé

- Vérifiez que vous avez bien désactivé **tous** les antivirus (ESET et Windows Defender)
- Assurez-vous d'avoir exécuté le terminal en tant qu'administrateur
- Vérifiez que la clé de licence saisie est correcte et à jour

Le PC ne démarre plus après le redémarrage

- Redémarrez le PC en mode sans échec
- Si vous avez une sauvegarde système, envisagez de restaurer le système
- Contactez le support technique si le problème persiste

Notes importantes

Sujet	Détail
Sauvegarde	Effectuez toujours une sauvegarde complète avant de modifier le SID
Domaine Active Directory	Si le PC est joint à un domaine, retirez-le du domaine avant de changer le SID, puis rejoignez-le après
Applications	Certaines applications liées au SID peuvent nécessiter une réinstallation ou une réactivation
Licences	Les licences logicielles liées au SID peuvent être affectées

---

Sources : https://docs.safeharboursupport.com/books/windows/page/65051-changing-the-sid-of-a-windows-device

Document créé le 12/03/2025