Windows 11 : la protection de l'autorité de sécurité locale

Table des matières

1. Qu'est-ce que la protection de l'autorité de sécurité locale est désactivée

L'autorité de sécurité locale ou Local Security Authority Process (LSASS) est l'une des fonctions critiques du sous-système de sécurité Windows qui authentifie l'identité d'un utilisateur au cours
du processus d'ouverture de session sur un ordinateur local.

Elle vérifie les changements de mot de passe et les tentatives de connexion, crée des jetons d'accès pour les sessions de connexion unique et exécute d'autres tâches liées à l'authentification
et à l'autorisation de Windows.

Cela se traduit par le processus lsass.exe qui tourne en permanence dans Windows 11.

La protection du sous-système de l'autorité de sécurité locale est l'une des principales mesures
que vous pouvez prendre pour protéger votre système et vos comptes contre les cybercriminels.

C'est une fonctionnalité de protection apparue dans Windows 11 dans la sécurité de l'appareil et isolation du noyau.

Elle utilise la virtualisation matérielle et la sécurité basée sur la virtualisation (VBS) pour créer un processus LSAIso isolé du système.

Une fois que l'on aura activé la protection de l'autorité de sécurité locale, on pourrait mieux contrôler la vulnérabilité des mots de passe en texte clair et les attaques par vidage de mot de passe.

Celle-ci se règle dans **Sécurité Windows > Sécurité des appareils > détails de l'isolation du noyau**.

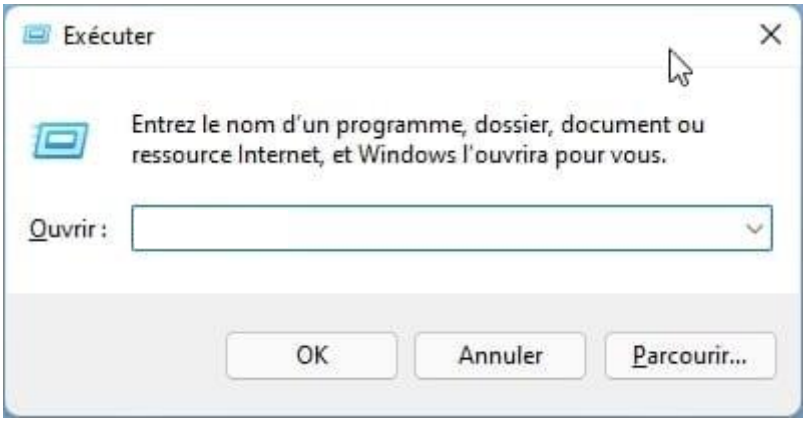
2. Activer la protection de l'autorité de sécurité locale

La protection de l'autorité de sécurité locale est désactivée après un redémarrage. Si le message s'affiche même après l'avoir activé et redémarré l'ordinateur, créer d'abord un point de restauration du système, puis essayer ceci.

2.1 Activer la protection depuis le registre Windows après un redémarrage

a) Sur votre clavier, appuyer sur les touches **Windows + R**

b) Dans la pop-up **Exécuter** qui s'ouvre, saisir **regedit** et valider



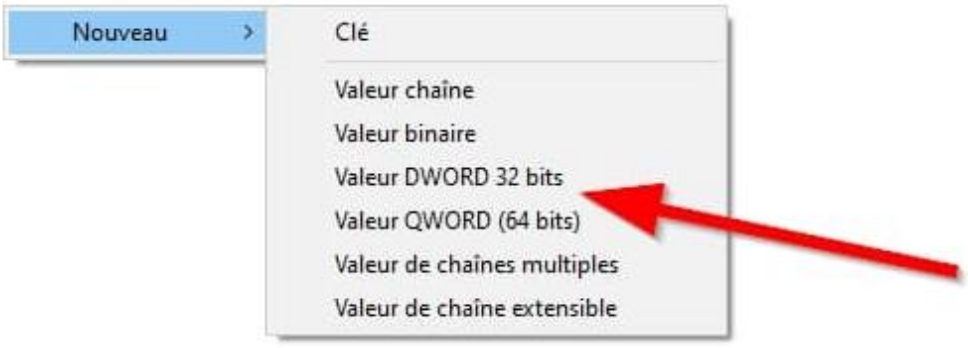
c) Dans l'éditeur du registre Windows, déroulez l'arborescence suivante :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

d) Sur le volet de droite, s'assurer que **RunAsPPLBoot** et **RunAsPPL** ont une **valeur de 2**. Si ce n'est pas le cas, double-cliquer dessus et corriger la valeur avec 2

Si on ne voit pas **RunAsPPLBoot**, il faut créer la valeur. Pour cela, dans le volet de droite :

a) Faire un clic droit **Nouveau > Valeur D-Word 32 bits**

b) Créer une valeur **DWORD 32 bits** dans le registre Windows



c) Nommer la valeur en **RunAsPPLBoot**

d) Double-cliquer dessus pour saisir la valeur 2

e) Enfin redémarrer l'ordinateur pour prendre en compte les changements, vérifier si La protection de l'autorité de sécurité locale est maintenant activé.

2.2 Activer la protection depuis le registre Windows

Pour activer la protection l'autorité de sécurité locale, procéder comme suit

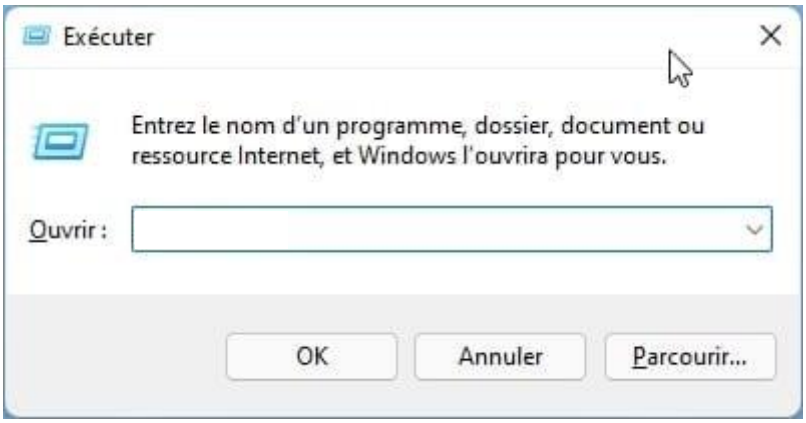
a) Cliquez sur Oui à l'invite du contrôle des comptes utilisateurs (UAC)
b) Dans l'éditeur du registre, accédez au chemin d'accès ci-dessous
HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > Lsa
c) Dans le panneau de droite, double-cliquer sur **RunAsPPL**
d) Remplacer la valeur par **1** et cliquez sur OK
e) Redémarrer le PC pour appliquer les modifications

2.3 Activer la protection depuis l'éditeur de stratégie de groupe locale

Gpedit.msc est l'éditeur de stratégie de groupe locale pour activer ou désactiver des modèles de configuration ou de restrictions administrateur.
Ce dernier n'est pas disponible dans les éditions familles de Windows 11 et Windows 10.

Si l'on veut utiliser ces éditions, on doit l'activer à l'aide du script Activer-gpedit-Win10-11.zip

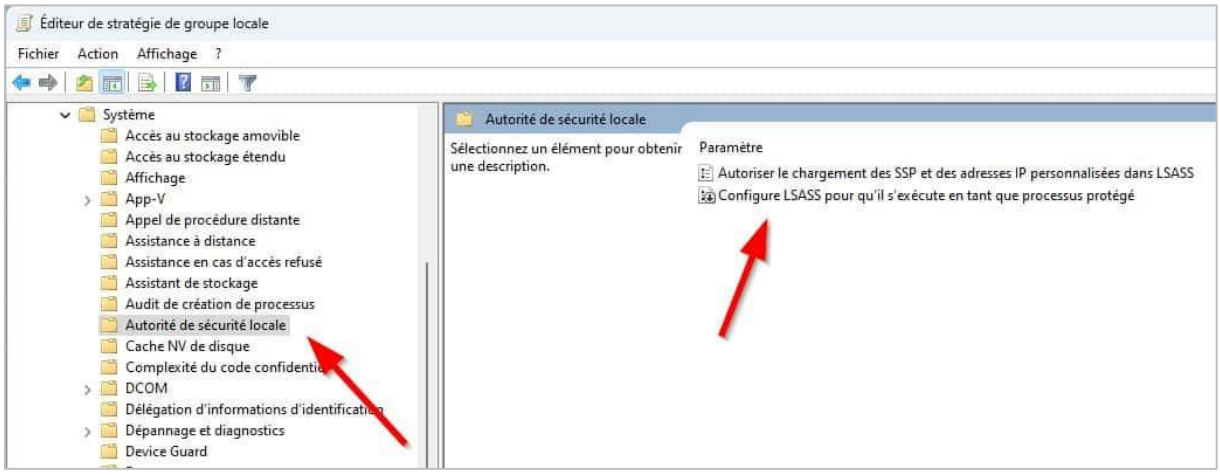
a) Sur le clavier, appuyez sur les touches **Windows + R**
b) Saisir **gpedit.msc** pour l'ouvrir



c) Dérouler **Stratégies de l'ordinateur local > Configuration ordinateur > Modèles d'administration > Composants Windows**

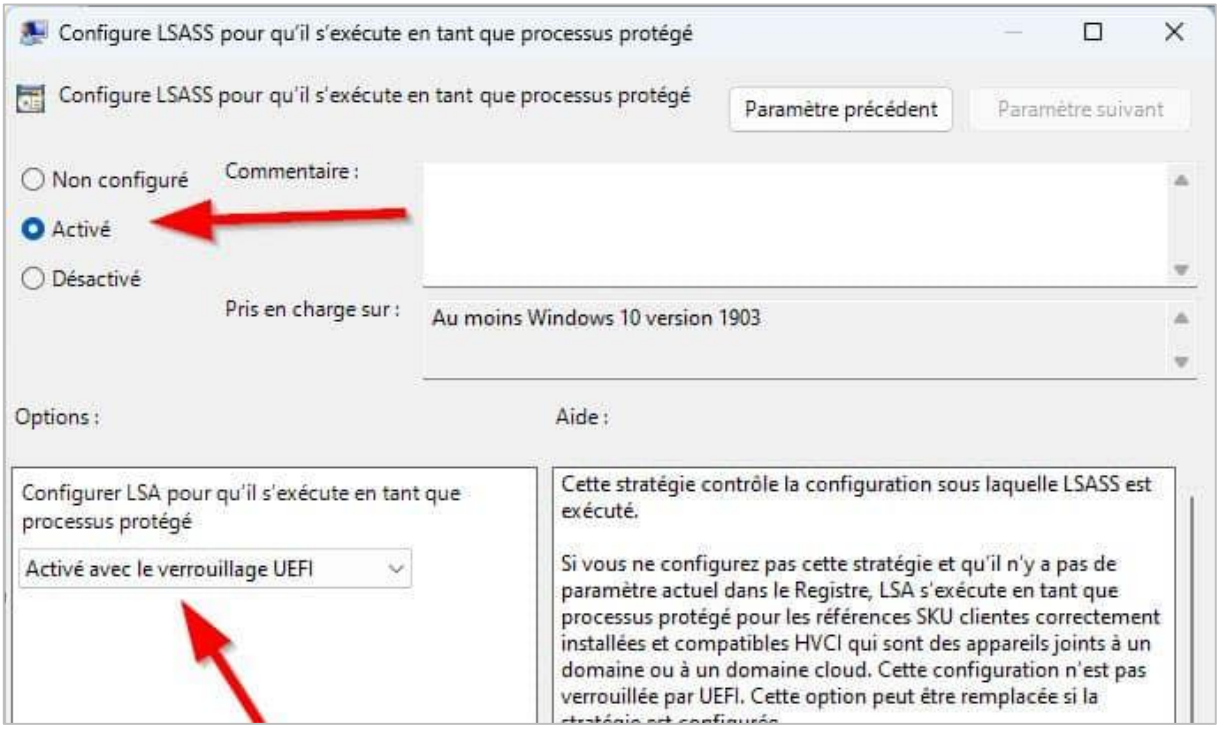
d) Ensuite sélectionner **Système > Autorité de sécurité locale**

e) Dans le volet de droite, double cliquez sur **Configurer LSASS** pour qu'il s'exécute en tant que processus protégé



f) En haut à gauche, cocher la case **Activé**

g) Ensuite en dessous, dans Configurer LSA pour qu'il s'exécute en tant que processus protégé, sélectionnez Activé avec le verrouillage (UEFI)



h) Cliquez sur Appliquer et OK

i) Enfin redémarrez l'ordinateur pour prendre en compte les modifications. Cela va solutionner, le message la protection de l'autorité de sécurité locale est désactivée