**Stratégie de mots de passe Windows**

**TABLE DES MATIERES**

[1. Détail de la stratégie Windows 3](#_Toc30347536)

[a) Conserver l’historique des mots de passe 3](#_Toc30347537)

[b) Durée de vie maximale du mot de passe : 3](#_Toc30347538)

[c) Durée de vie minimale du mot de passe : 3](#_Toc30347539)

[d) Enregistrer les mots de passe en utilisant un chiffrement réversible : 4](#_Toc30347540)

[e) Le mot de passe doit respecter des exigences de complexité : 4](#_Toc30347541)

[f) Longueur minimale du mot de passe : 4](#_Toc30347542)

[2. Autres options disponibles (par utilisateur) 5](#_Toc30347543)

[a) Particularité administrateur 5](#_Toc30347544)

[3. Stratégies de mots de passe 6](#_Toc30347545)

[a) Mot de passe complexe 6](#_Toc30347546)

[b) Passphrase 6](#_Toc30347547)

[c) Fréquence de changement 6](#_Toc30347548)

# Détail de la stratégie Windows (hors applications métiers et autres logiciels)



## Conserver l’historique des mots de passe

Ce paramètre de sécurité détermine le nombre de nouveaux mots de passe uniques devant être associés à un compte d’utilisateur avant qu’un ancien mot de passe puisse être réutilisé. La valeur doit être comprise entre 0 et 24 mots de passe.

Cette stratégie permet aux administrateurs d’améliorer la sécurité en garantissant que d’anciens mots de passe ne sont pas réutilisés continuellement.

Pour maintenir l’efficacité de l’historique des mots de passe, ne permettez pas que les mots de passe soient changés immédiatement après avoir été changés en activant également le paramètre de stratégie de sécurité Durée de vie minimale du mot de passe. Pour plus d’informations sur le paramètre de stratégie de sécurité de durée de vie minimale du mot de passe, voir Durée de vie minimale du mot de passe.

## Durée de vie maximale du mot de passe :

Ce paramètre de sécurité détermine la période (en jours) pendant laquelle un mot de passe peut être utilisé avant que le système oblige l’utilisateur à le changer. Vous pouvez prévoir que les mots de passe expirent après une période comprise entre 1 et 999 jours, ou vous pouvez spécifier que les mots de passe n’expirent jamais en choisissant la valeur 0. Si la durée de vie maximale du mot de passe est comprise entre 1 et 999 jours, la durée de vie minimale du mot de passe doit être inférieure à la durée de vie maximale. Si la durée de vie maximale du mot de passe a la valeur 0, la durée de vie minimale peut être comprise entre 0 et 998 jours.

*Remarque : la meilleure pratique consiste à choisir un délai d’expiration compris entre 30 et 90 jours, selon votre environnement. De cette manière, un attaquant dispose d’une période limitée pour trouver le mot de passe d’un utilisateur et avoir accès aux ressources de votre réseau.*

## Durée de vie minimale du mot de passe :

Ce paramètre de sécurité détermine la période minimale (en jours) d’utilisation d’un mot de passe avant que l’utilisateur puisse le changer. Vous choisissez une valeur comprise entre 1 et 998 jours, ou vous pouvez permettre des changements immédiats en spécifiant la valeur 0.

La durée de vie minimale du mot de passe doit être inférieure à la durée de vie maximale, sauf si la durée de vie maximale du mot de passe est définie à 0, indiquant que les mots de passe n’expirent jamais. Si la durée de vie maximale du mot de passe est de 0, la durée de vie minimale peut être réglée à une valeur comprise entre 0 et 998.

Configurez la durée de vie minimale du mot de passe à une valeur supérieure à 0 pour garantir l’efficacité du paramètre Appliquer l’historique des mots de passe. Sans une durée de vie minimale du mot de passe, les utilisateurs peuvent effectuer des tentatives répétées d’entrée de mot de passe jusqu’à ce qu’ils obtiennent un ancien mot de passe favori. Le réglage par défaut ne respecte pas cette recommandation, afin qu’un administrateur puisse spécifier un mot de passe pour un utilisateur et obliger ce dernier à changer le mot de passe défini par l’administrateur lorsque l’utilisateur se connecte. Si l’historique du mot de passe est défini à 0, l’utilisateur n’a pas besoin de choisir un nouveau mot de passe. Pour cette raison, le paramètre Appliquer l’historique des mots de passe est défini à 1 par défaut.

## Enregistrer les mots de passe en utilisant un chiffrement réversible :

Ce paramètre de sécurité détermine si le système d’exploitation stocke les mots de passe en utilisant un chiffrement réversible.

Cette stratégie est destinée aux applications qui utilisent des protocoles nécessitant la connaissance du mot de passe de l’utilisateur à des fins d’authentification. Le stockage des mots de passe avec un chiffrement réversible est fondamentalement identique au stockage des versions des mots de passe en texte clair. Pour cette raison, cette stratégie ne doit être activée que si les impératifs de l’application prévalent sur la nécessité de protéger les informations des mots de passe.

## Le mot de passe doit respecter des exigences de complexité :

Ce paramètre de sécurité détermine si les mots de passe doivent respecter des exigences de complexité.

Si cette stratégie est activée, les mots de passe doivent respecter les exigences minimales suivantes :

Ne pas contenir le nom de compte de l’utilisateur ou des parties du nom complet de l’utilisateur comptant plus de deux caractères successifs

Comporter au moins six caractères

Contenir des caractères provenant de trois des quatre catégories suivantes :

Caractères majuscules anglais (A à Z)

Caractères minuscules anglais (a à z)

Chiffres en base 10 (0 à 9)

Caractères non alphabétiques (par exemple, !, $, #, %)

Les exigences de complexité sont appliquées lors du changement ou de la création de mots de passe.

## Longueur minimale du mot de passe :

Ce paramètre de sécurité détermine le nombre minimal de caractères que doit contenir le mot de passe d’un compte d’utilisateur. Vous pouvez choisir une valeur comprise entre 1 et 14 caractères, ou vous pouvez établir qu’aucun mot de passe n’est requis en choisissant la valeur 0.

# Autres options disponibles (par utilisateur)



## Particularité administrateur



# Stratégies de mots de passe

Il existe plusieurs stratégies de mot de passe détaillées ci-dessous, il faut choisir celle qui sera la plus adaptée à vos besoins (complexité et fréquence de changement).

## Mot de passe complexe

Il est possible d’obliger les utilisateurs à utiliser un mot de passe complexe composé de caractères spéciaux, majuscules et chiffres.

C’est très sécurisé mais souvent compliqué pour les utilisateurs de gérer ses mots de passe s’ils sont alliés à des changements fréquents.

## Passphrase

Il est aussi possible de créer un mot de passe sous forme d’une phrase (sans espace et sans caractères spéciaux) qui est une phrase commune simple à se souvenir. Cela permet d’avoir un bon compromis entre la longueur et la complexité.

Par contre la saisie du mot de passe est plus longue qu’un mot de passe complexe qui sera composé de moins de caractères. Mais cette longueur de mot de passe est très difficile à pirater via des systèmes dit « Brute Force » qui essayent de « deviner » votre mot de passe.

## Fréquence de changement

Il est important de définir plusieurs changements de mots de passe annuels (la bonne pratique d’usage est environ tous les 90 jours). Il faut trouver le bon compromis entre la complexité du mot de passe et la fréquence de changement.