SPECOPS PASSWORD POLICY
Datasheet

A PROPOS DE SPECOPS Specops Software est le leader de solutions de gestion des mots de passe et d'authentification. Specops protège les données de votre entreprise en bloquant les mots de passe faibles et en sécurisant l'authentification des utilisateurs. Chaque jour, des milliers d'organisations utilisent le logiciel Specops pour protéger leurs données professionnelles. Visitez https://www.specopssoft.com/fr/ pour plus d'informations.

SPECOPS PASSWORD POLICY

Specops Password Policy vous aide à renforcer la sécurité des mots de passe dans votre environnement Microsoft Active Directory. L'outil étend la fonctionnalité de la politique de groupe et simplifie la gestion des politiques de mot de passe à granularité fine (Fine Grained Password Policy ou FGPP). Specops Password Policy peut cibler n'importe quel niveau de GPO, groupe, utilisateur ou ordinateur avec des paramètres de complexité de mot de passe, de liste de mots de passe compromis, de dictionnaires et de phrases de passe.

Adoptez une approche segmentée et personnalisez vos paramètres en fonction des besoins de sécurité des différentes populations d'utilisateurs. Attribuez aux utilisateurs qui ont accès à des données sensibles une plus grande complexité de mot de passe, sans pour autant entraver la convivialité pour les utilisateurs moins privilégiés. Ou bien, remplacez la complexité en autorisant les phrases de passe pour appliquer des politiques sécurisées sans accabler les utilisateurs.

Renforcez la sécurité en bloquant l'utilisation de mots de dictionnaire personnalisés propres à votre organisation. Avec le service Specops Breached Password Protection, Specops Password Policy peut bloquer l'utilisation de plus de 4 milliards de mots de passe compromis connus. Le service vérifie les mots de passe trouvés dans les fuites de données, les botnets de logiciels malveillants, ainsi que les mots de passe trouvés par notre vaste système de pots de miel qui surveille les mots de passe utilisés dans les attaques par force brute qui se produisent en ce moment même.

FONCTIONNALITÉS CLÉS	SPECOPS	MICROSOFT FGPP	AZURE AD PASSWORD PROTECTION
Dictionnaire et listes de mots de passe compromis Vous pouvez utiliser un dictionnaire de mots de passe, un fichier contenant des mots de passe couramment utilisés et/ou compromis, pour empêcher les utilisateurs de créer des mots de passe susceptibles d'être attaqués par dictionnaire.			
Création de listes de dictionnaires personnalisées	Oui (sans limite)	Non	Oui (jusqu'à 1000 termes, minimum 4 caractères)
Bloque les mots de passe utilisés dans les attaques par pulvérisation de mots de passe qui se produisent actuellement	Oui	Non	Partiellement (utilise uniquement les termes de base dans la liste globale)

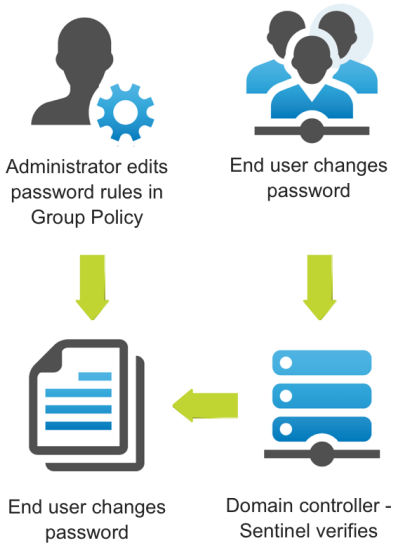
FONCTIONNALITÉS CLÉS	SPECOPS	MICROSOFT FGPP	AZURE AD PASSWORD PROTECTION
La liste des mots de passe bloqués comprend les mots de passe de tiers ayant fait l'objet d'une violation (comme le recommandent des organismes tels que l'ANSSI, la CNIL NIST et le NCSC).	Oui (plus de 4 milliards de mots de passe uniques compromis)	Non	Non (la liste "interdite" n'est pas une liste de mots de passe divulgués)
Recherche et supprime les mots de passe divulgués déjà utilisés	Oui	Non	Non
Interdiction de l'utilisation partielle d'un mot de la liste du dictionnaire	Oui (complet ou partiel)	N/A	Non
Interdiction de l'utilisation du prénom ou du nom de l'utilisateur	Oui (complet ou partiel)	Non	Pas d'interdiction partielle
Bloque les mots de 3 lettres, les abréviations et les acronymes	Oui	N/A	Non (minimum 4 caractères)
Interdiction de la substitution de caractères communs	Oui	Non	Plusieurs manquants
Complexité du mot de passe / de la phrase de passe La complexité correspond généralement aux types de caractères (minuscules, majuscules, numériques et spéciaux) utilisés dans un mot de passe. Cependant, la complexité est inefficace si elle est prévisible.			
5/5 types de caractères	Oui	Seulement 3/5 types de caractères	N/A
Interdiction des caractères identiques consécutifs	Oui	Non	N/A

FONCTIONNALITÉS CLÉS	SPECOPS	MICROSOFT FGPP	AZURE AD PASSWORD PROTECTION
Interdiction des types de caractères communs au début	Oui	Non	N/A
Prise en charge des passphrases	Oui	Non	N/A
Expiration des mots de passe / Historique des mots de passe			
Rappels d'expiration du mot de passe	Email, Infobulles	Infobulles uniquement	N/A
Interdiction d'une partie du mot de passe actuel	Oui	Non	N/A
Nombre minimum de caractères modifiés	Oui	Non	N/A
Durée de vie du mot de passe en fonction de sa longueur	Oui	Non	N/A
Autres			
Outil de reporting dédié à la politique de mot de passe	Oui	Non	Non
Affichage dynamique de la politique de mot de passe	Oui	Non	N/A
Modèles de politique de mot de passe OOTB NIST et NCSC	Oui	Non	N/A

FONCTIONNALITÉS CLÉS	SPECOPS	MICROSOFT FGPP	AZURE AD PASSWORD PROTECTION
Personnalisation du message d'échec de changement de mot de passe pour l'utilisateur final	Oui	Non	N/A

Comment cela fonctionne-t-il ?

Specops Password Policy s'appuie sur le moteur de stratégie de groupe d'Active Directory et fonctionne conjointement avec les fonctions de stratégie de mot de passe existantes. Elle se compose des éléments suivants et ne nécessite pas de serveurs ou de ressources supplémentaires dans votre environnement.



Outils d'administration : Configurent les aspects centraux de la solution, et permettent la création des paramètres de Specops Password Policy dans les GPOs.

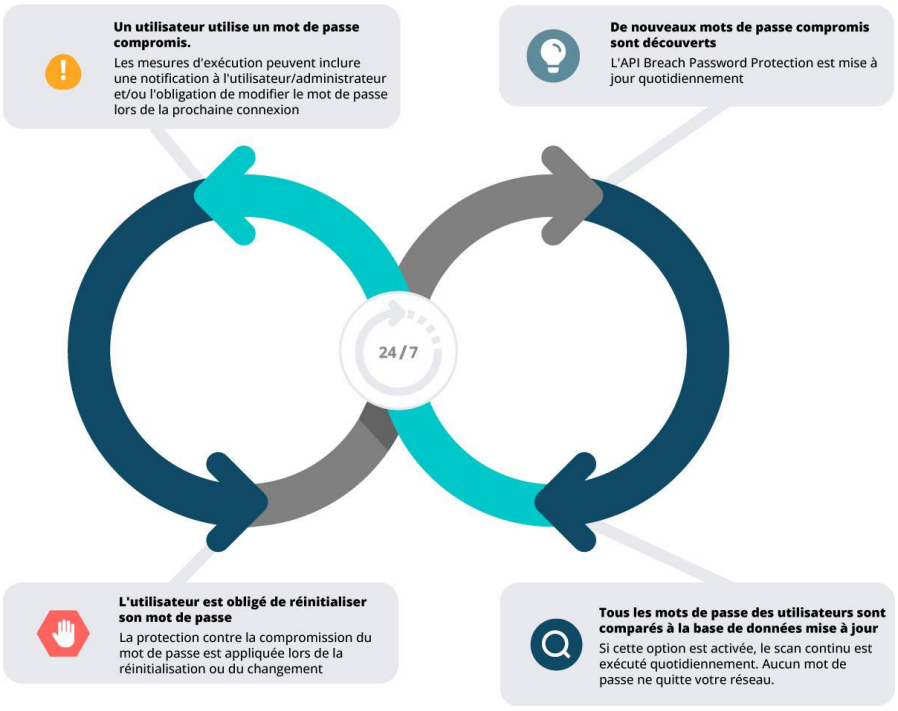
Sentinel: Vérifie si un nouveau mot de passe correspond aux paramètres de la Specops Password Policy attribués à l'utilisateur. Le Sentinel est un filtre de mot de passe au niveau des contrôleurs de domaine.

Client (facultatif): Affiche les règles de la stratégie de mot de passe à l'utilisateur final lors de la modification de son mot de passe. Notifie également les utilisateurs lorsque leur mot de passe est sur le point d'expirer.

Scan continu avec Specops Breached Password Protection

La fonction de scan continu vérifie tous les mots de passe Active Directory par rapport à l'API Breached Password Protection pour la compromission une fois par jour pendant le scan périodique programmé. Si elle est activée, l'API est mise à jour quotidiennement avec les mots de passe compromis nouvellement découverts à partir de notre système de pot de miel de mots de passe, en plus des fuites de mots de passe nouvellement découvertes ou des mots de passe volés à partir de botnets de logiciels malveillants, lorsqu'ils se produisent.

Aucun mot de passe ne quitte le réseau local.

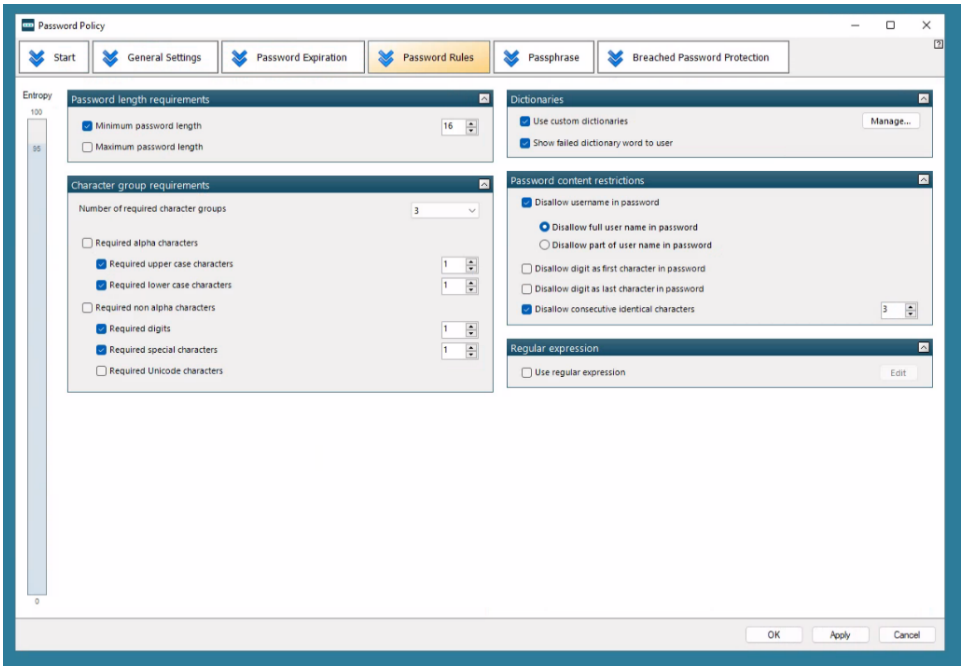


Les actions correctives optionnelles comprennent l'application du changement lors de la prochaine connexion ou la notification par texte ou par courrier électronique. La notification par e-mail peut être configurée pour notifier tout utilisateur souhaité (y compris les administrateurs).

Les derniers résultats du scan peuvent être consultés dans les journaux d'événements ainsi que sur la page de rapport du scan périodique dans l'interface d'administration.

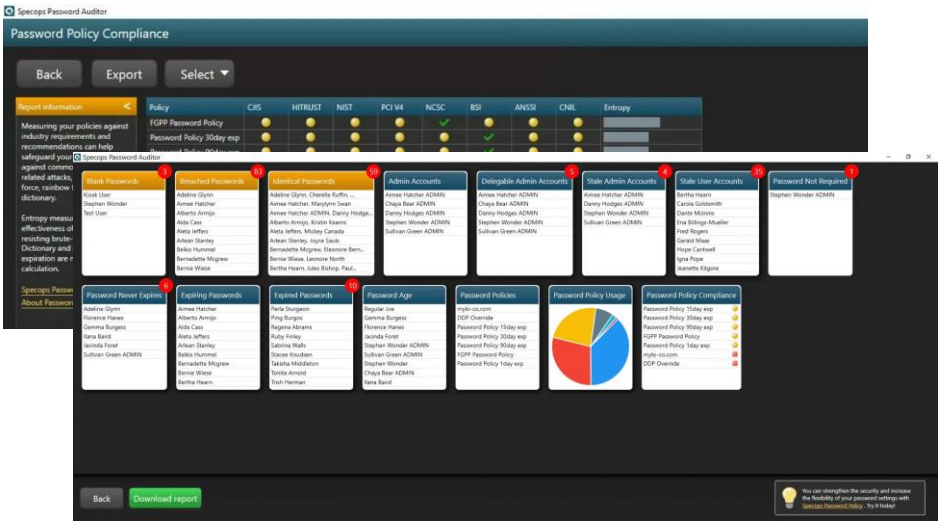
À quoi cela ressemble-t-il ?

Expérience en tant qu'administrateur



Les paramètres des mots de passe peuvent être configurés à partir de l'éditeur de gestion des stratégies de groupe.

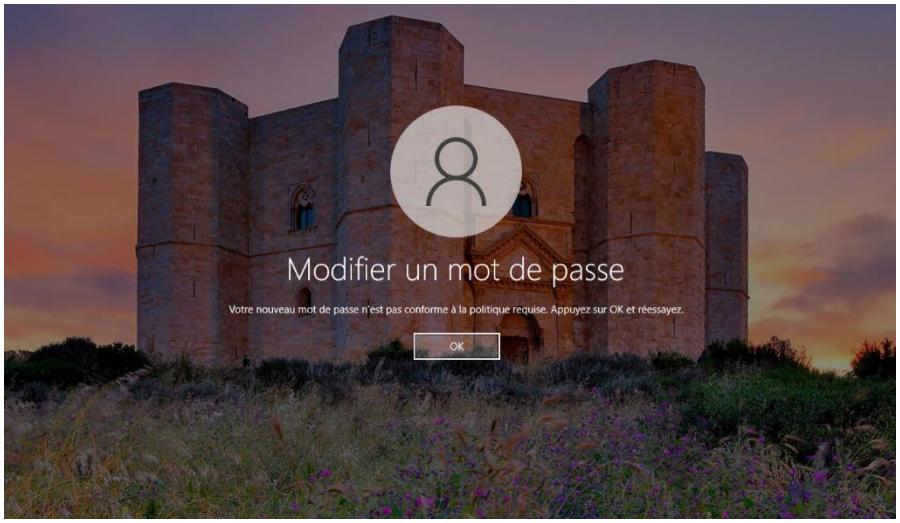
Vous pouvez configurer une stratégie de mot de passe pour utiliser des règles classiques ou des passphrases.



L'outil Password Auditor analyse et détecte les vulnérabilités liées aux mots de passe.

Les résultats comprennent plusieurs rapports interactifs avec des informations sur les utilisateurs et les politiques, ainsi qu'un rapport PDF exportable.

Expérience de l'utilisateur final



Specops Password Policy vous permet de personnaliser les messages que les utilisateurs voient au-delà du message standard de Windows.

Les options d'affichage comprennent l'affichage du mot du dictionnaire trouvé ou des règles sur lesquelles l'utilisateur a réussi ou échoué..

L'affichage dynamique lors du changement de mot de passe signifie que les utilisateurs finaux voient un message dynamique lorsqu'ils tapent leur nouveau mot de passe.

Un meilleur feedback de l'utilisateur final signifie des utilisateurs plus heureux et moins d'appels au helpdesk.

Demandez une démo de Specops Password Policy

Vous souhaitez savoir comment Specops Password Policy et Breached Password Protection peuvent fonctionner dans votre environnement ? Cliquez ici pour demander une démo ou un essai aujourd'hui.

Avis client

Satisfaits du produit et l'accompagnement à la mise en place par Specops

Le renforcement de la politique des mots de passes de l'annuaire Active Directory est toujours un sujet d'actualité. Le déploiement de Specops Password Policy nous a apporté des options plus fines sur nos politiques, et un contrôle en temps réel des mots de passes vis-à-vis de bases contenant des milliards de mots de passe volés. Après un an d'utilisation, nous sommes satisfaits du produit et l'accompagnement à la mise en place par Specops.

Nicolas Boulet, RSSI, Asobo Studio

C'est un outil très intuitif et le support chez Specops est top

Côté clients, nos collaborateurs sont désormais autonomes pour modifier leur mot de passe (plus la peine d'appeler le support technique) grâce aux explications détaillées sur le mot de passe demandé (nombre de caractères, types de caractères...). Ils peuvent aussi choisir la longueur de leur mot de passe afin d'allonger sa durée de vie. Côté administration, l'outil est très simple et nous avons été suivi tout au long de la mise en place et de la configuration de l'outil. En plus de cet outil très intuitif, le support chez Specops est top, ils sont très réactifs et répondent à nos interrogations très rapidement, quitte à faire une réunion avec un spécialiste.

Audrey H., Ingénieure Système et Sécurité, Altaprofits

Je recommande vivement Specops Password Policy

La solution Specops Password Policy est facile à mettre en œuvre et à utiliser. Elle garantit que notre système ne sera pas facilement compromis par des mots de passe divulgués. L'équipe de Specops a été très réactive lors des premiers contacts et nous a accompagnés dans tout le processus de déploiement. Je recommande vivement Specops Password Policy.

Jérôme N., IT Manager, Une entreprise leader dans le domaine des dispositifs médicaux implantables