SPECOPS BREACHED PASSWORD PROTECTION

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 BREACHED PASSWORD PROTECTION

Specops Breached Password Protection est un service qui vérifie vos mots de passe Active Directory par rapport à une liste de mots de passe compromis mise à jour en permanence. La liste contient plus de 3 milliards de mots de passe provenants de fuites de données majeures, ainsi que des mots de passe utilisés actuellement dans des attaques réelles. Lors d'un changement de mot de passe dans Active Directory, le service bloque et avertit les utilisateurs si le mot de passe qu'ils ont choisi se trouve dans la liste de mots de passe bannis.

Comment cela fonctionne-t-il ?

Il existe deux versions du service Breached Password Protection, Complete et Express. Les deux sont incluses lorsque vous activez Breached Password Proteciton dans Specops Password Policy.

- Breached Password Protection Complete contient plus de 3 milliards de mots de passe et se connecte à votre réseau via une clé API. Lorsqu'il est activé, le service vérifie les mots de passe de vos utilisateurs lors d'un changement ou d'une réinitialisation de mot de passe et les avertit par e-mail ou par SMS si ce mot de passe s'avère être un mot de passe compromis connu et peut leur demander de le changer lors de leur prochaine connexion.

- Breached Password Protection Express est un sous-ensemble optimisé de la liste complète. Lorsqu'il est activé, le service vérifie les mots de passe de vos utilisateurs lors d'un changement de mot de passe et les empêche immédiatement d'utiliser ce mot de passe. Les administrateurs peuvent également configurer des analyses nocturnes basée sur la liste Express. La liste Express est également utilisée lors de l'exécution d'une analyse de Specops Password Auditor.

Vous pouvez activer l'une ou l'autre selon vos préférences en matière de sécurité, mais nous vous recommandons d'activer les deux si vous le pouvez.

Pour en savoir plus sur les exigences techniques de Specops Breached Password Protection, consultez notre fiche de référence.

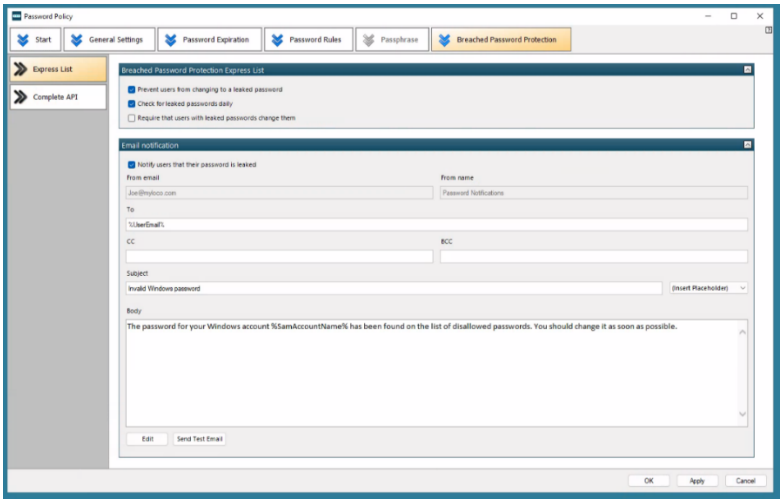
Fonctionnalités

FONCTIONNALITÉS CLÉS	ACTIVE DIRECTORY	AZURE AD PASSWORD PROTECTION	SPECOPS BREACHED PASSWORD PROTECTION
La liste bloquée inclut les mots de passe mots de passe compromis	n/a	Non (pas une liste de tiers, confirmé par Microsoft)	Oui

FONCTIONNALITÉS CLÉS	ACTIVE DIRECTORY	AZURE AD PASSWORD PROTECTION	SPECOPS BREACHED PASSWORD PROTECTION
(comme recommandé par des organismes comme le NIST et NCSC)			
Protège contre l'utilisation de plus de 3 milliards de mots de passe connus comme ayant été compromis	n/a	Non (correspondances floues supérieures à 1 million)	Oui
Bloque les mots de passe utilisés dans les attaques par pulvérisation de mot de passe (password spraying) qui se produisent actuellement.	n/a	Partiellement (utilise uniquement les termes de base de la liste globale)	Oui
Les mises à jour de la liste bloquée offrent une protection immédiate	n/a	Oui	Oui
Offre une protection sur les contrôleurs de domaine non connectés à un réseau internet externe	n/a	Non	Oui (avec Express)
Explication à l'écran de la raison pour laquelle le mot de passe est rejeté	n/a	Non (pas pour on-prem)	Oui
Notifications hors écran des mots de passe compromis	n/a	Non	Oui (SMS et email)

À quoi cela ressemble-t-il ?

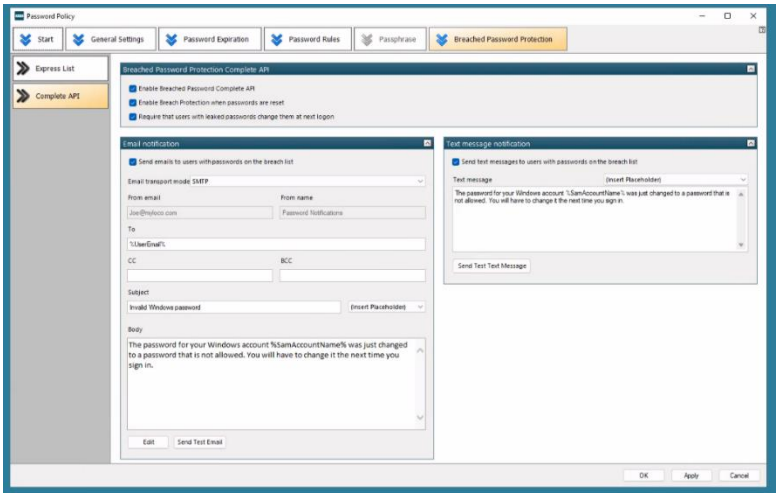
Vous configurez les paramètres de Specops Breached Password Protection dans votre écran d'administration Specops Password Policy.



Configurez le moment où les utilisateurs sont obligés de changer de mot de passe, ainsi que le contenu de vos notifications par e-mail et par SMS.

Utilisez cc ou cci pour alerter le personnel informatique ou le helpdesk.

Activez la vérification journalière des mots de passe compromis pour l'application Express.



Configurez le moment où les utilisateurs sont obligés de changer de mot de passe ainsi que le contenu de vos notifications par e-mail.

Choisissez si vous souhaitez utiliser votre propre serveur de messagerie ou le service Specops pour envoyer vos notifications par email.

Questions fréquemment posées

À quelle fréquence la liste est-elle mise à jour ?

Notre équipe travaille constamment à la mise à jour de la liste utilisée dans Specops Breached Password Protection. Breached Password Protection Complete, notre liste connectée par API, est mise à jour immédiatement dès que notre équipe trouve de nouveaux ajouts (au moins une fois par jour). Breached Password Protection Express, la liste condensée téléchargeable, est mise à jour tous les deux mois environ.

Quelles sont vos sources pour la liste ?

Pour des raisons de sécurité, nous ne révélons pas le contenu intégral de Specops Breach Password Protection. Cependant, nous pouvons partager que la liste de plus de 3 milliards de mots de passe comprend la liste

HaveIBeenPwned, les dernières listes de la Collection, ainsi que les listes de fuites connues, comme le recommandent les organismes de réglementation tels que l'ANSSI, la CNIL et d'autres…

En plus des brèches connues, notre équipe de recherche surveille également activement les mots de passe utilisés dans des attaques réelles par pulvérisation des mots de passe qui se produisent en ce moment même. Le système de collecte des données de surveillance des attaques de notre équipe met le service à jour quotidiennement et veille à ce que les utilisateurs de l'organisation soient immédiatement bloqués dans le choix de ces mots de passe lors de la modification/réinitialisation.

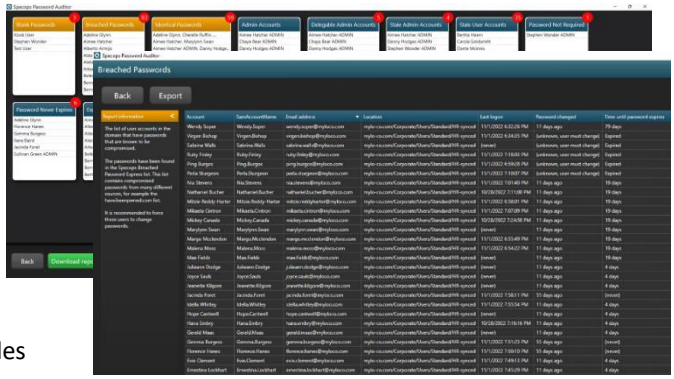
Les mots de passe sont-ils envoyés à l'extérieur avec Specops Breached Password Protection ?

Non. Le filtre de mot de passe Sentinel génère un hachage bcrypt du nouveau mot de passe de l'utilisateur. Ni le mot de passe ni le hachage bcrypt ne sont exposés. Les premiers octets du hachage bcrypt sont utilisés pour interroger un ensemble de hachages correspondants. La correspondance a lieu sur le contrôleur de domaine, au sein du réseau de l'organisation.

J'ai une autre question…

Vous avez une question à laquelle vous ne trouvez pas de réponse ici ? Nous serions heureux d'y répondre. Contactez votre représentant Specops ou contactez-nous.

Découvrez combien de mots de passe de vos utilisateurs sont vulnérables



Specops Password Auditor est un outil gratuit qui scanne et vérifie les mots de passe des comptes utilisateurs Active Directory par rapport à notre liste de mots de passe compromis. L'Auditeur fournit également une vue complète des comptes d'administrateur dans le domaine d'une organisation, y compris les comptes d'administrateur bloqués/inactifs. À partir d'une vue unique, vous pouvez identifier les vulnérabilités qui peuvent vous aider dans votre plan de sécurité.

Il suffit d'un seul mot de passe divulgué pour créer un risque et une compromission potentielle. Téléchargez gratuitement Specops Password Auditor.

Demandez une démo de Specops Breached Password Protection

Vous êtes prêt à voir comment Specops Breached Password Protection fonctionne dans votre environnement ? Specops Breached Password Protection fait partie de Specops Password Policy, un outil Active Directory qui étend les fonctionnalités de la politique de groupe et simplifie la gestion des politiques de mot de passe à granularité fine.

Demandez dès aujourd'hui une version d'essai de Specops Password Policy et de Breached Password Protection.

Avis d'Expert

INCONTESTABLEMENT PLUS SÉCURISÉ

"Les nouvelles fonctionnalités de dictionnaire et de liste de refus sont conçues pour donner aux administrateurs encore plus de contrôle sur les mots de passe des utilisateurs et permettre des mots de passe qui sont incontestablement plus sécurisés."

- Brien Posey, 15-times Microsoft MVP