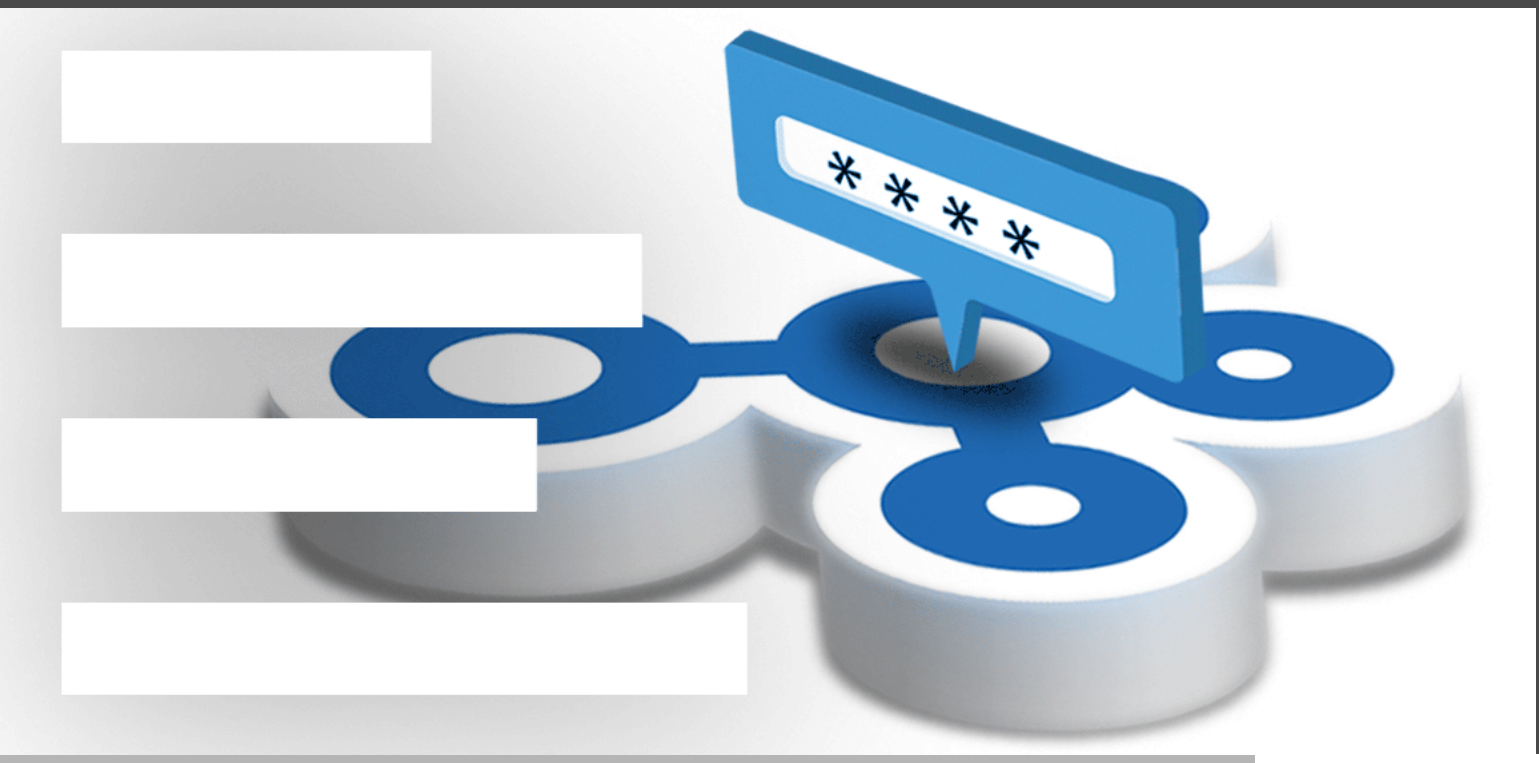
[Nouvelle fonctionnalité en vedette] Rapport de l'analyseur des mots de passe dans Password Hub Business 2021.1.



LE NOUVEAU RAPPORT DE L'ANALYSEUR DE MOTS DE PASSE

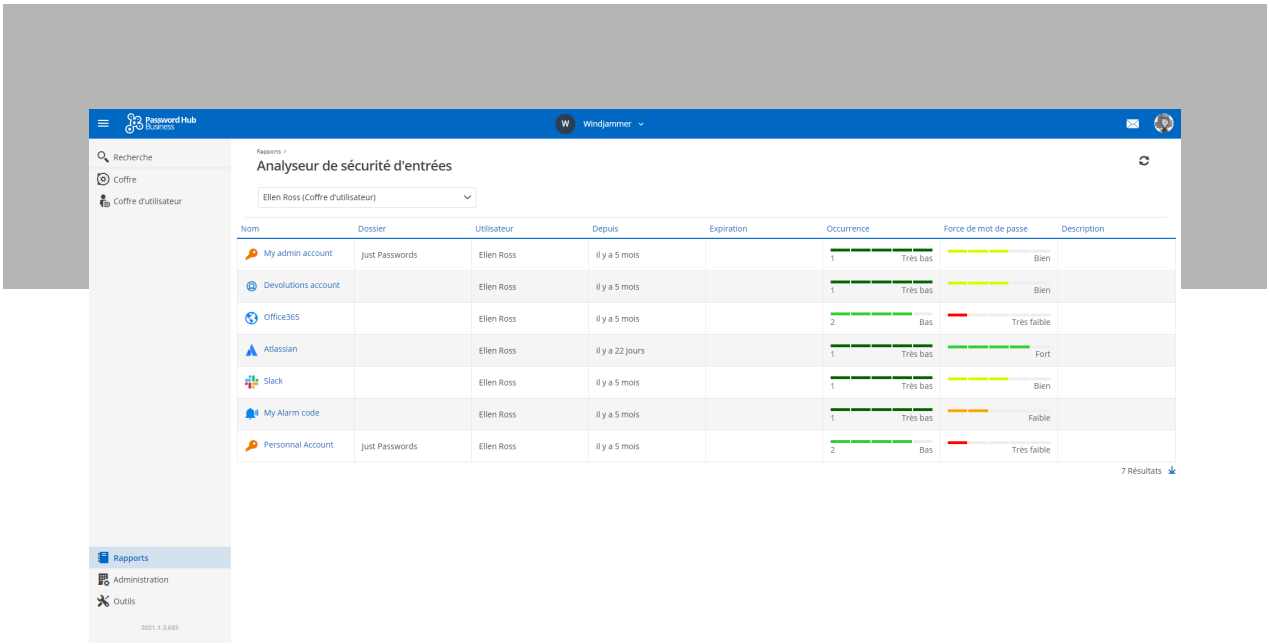
Nous lancions récemment la très attendue version 2021.1 de Password Hub Business avec ses nombreux ajouts et améliorations. Aujourd'hui, nous examinons de plus près l'une des nouvelles fonctionnalités les plus importantes : le nouveau rapport de l'analyseur de mots de passe. Comme vous pourrez le constater dans quelques instants, ce rapport est conçu pour vous aider à adopter les bonnes pratiques en matière de sécurité à tous les niveaux de votre entreprise, chose essentielle pour prévenir des violations ou fuites de données.

L’analyseur de sécurité des entrées

Avant d’aller plus loin, regardons d’abord l’une des fonctionnalités de Password Hub Business qui s’appelait « analyseur de mots de passe », mais qui s’appelle désormais « analyseur de sécurité des entrées ». (À noter que cette fonctionnalité s’appelle toujours « analyseur de mots de passe » dans Remote Desktop Manager et Devolutions Server.)

Cette fonctionnalité apporte des informations de sécurité sur les entrées, comme :

- La dernière fois qu’une entrée a été modifiée.
- Combien de fois un mot de passe a été réutilisé pour le même coffre.
- Si un mot de passe utilisé dans une entrée est considéré comme très fort, fort, bon, faible ou très faible.



Même si l’analyseur de sécurité des entrées est très utile pour améliorer les bonnes pratiques de sécurité, il est avant tout conçu pour se concentrer sur les entrées. Dans ce cas, qu’arrive-t-il lorsque vous souhaitez vous concentrer sur les mots de passe? Et bien, c’est là qu’entre en jeu le nouveau rapport d’analyseur de mots de passe!

À propos du rapport d'analyseur de mots de passe

Cette fonctionnalité disponible uniquement dans Password Hub Business (vous ne le retrouverez pas encore dans Remote Desktop Manager ou Devolutions Server) ajoute un niveau substantiel de sécurité aux mots de passe.

Comme mentionné précédemment, le rapport se concentre sur les mots de passe et non sur les entrées. Il révèle entre autres :

- Combien de mots de passe sont associés à un coffre.
- Combien parmi ces mots de passe sont considérés comme très forts, forts, bons, faibles ou très faibles.
- Combien de fois un mot de passe est utilisé pour toutes les entrées d'un coffre.

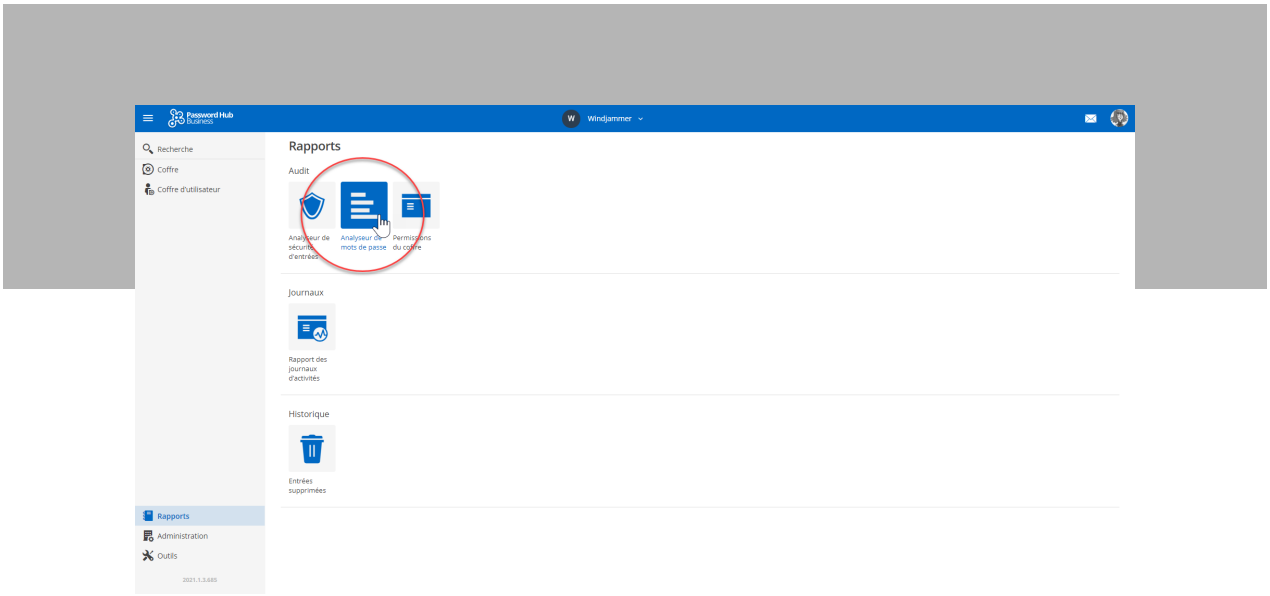
Le plus grand avantage du rapport d'analyseur de mots de passe, c'est qu'il met en évidence les vulnérabilités pour qu'elles puissent être ciblées et corrigées sur-le-champ. Par exemple, si vous avez 30 mots de passe réutilisés, l'analyseur de sécurité des entrées vous demande de les rechercher individuellement, ce qui peut entrainer une lourde charge administrative. Avec le rapport d'analyseur de mots de passe, vous savez exactement là où chacun des trente mots de passe réutilisés se trouvent. Mieux encore : vous pouvez y accéder directement, comme nous pourrons le voir plus loin. **Avant cela, voyons comment créer un rapport.**

Comment générer un rapport d'analyse de mots de passe

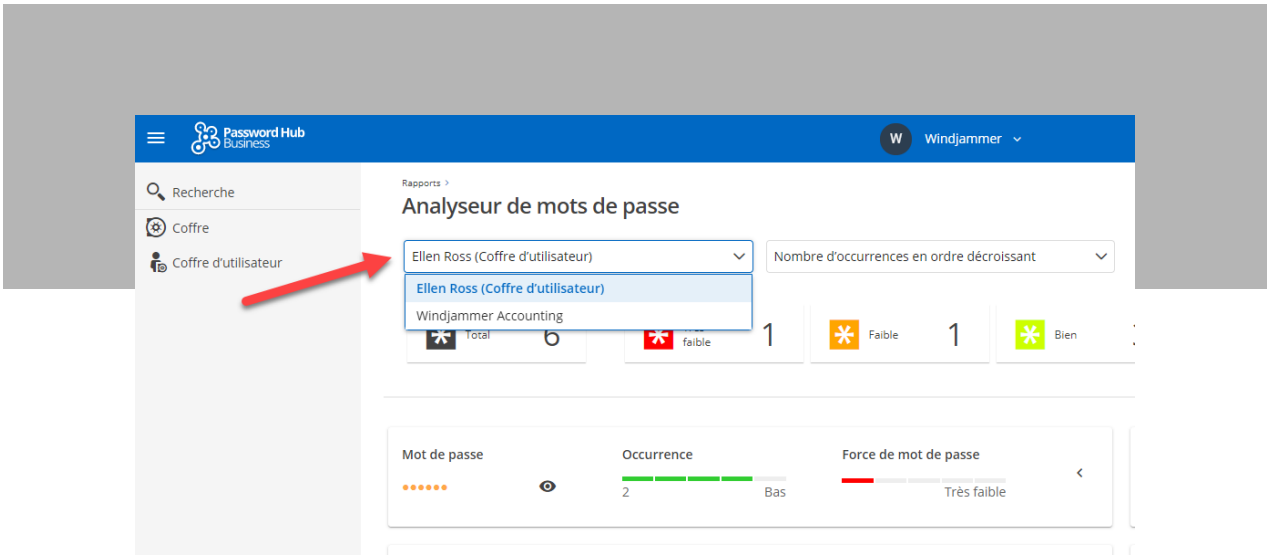
Le rapport d'analyse des mots de passe est accessible à tous les utilisateurs. Les administrateurs peuvent générer des rapports pour tous les coffres, tandis que les autres utilisateurs peuvent générer des rapports pour les coffres auxquels ils ont accès. De cette façon, tout le monde joue un rôle dans l'application des bonnes pratiques de sécurité et pas seulement les administrateurs.

Générer un rapport d'analyse des mots de passe, c'est simple et rapide :

Étape 1 : Cliquez sur **Rapports** et sélectionnez **Analyseur de mots de passe**.

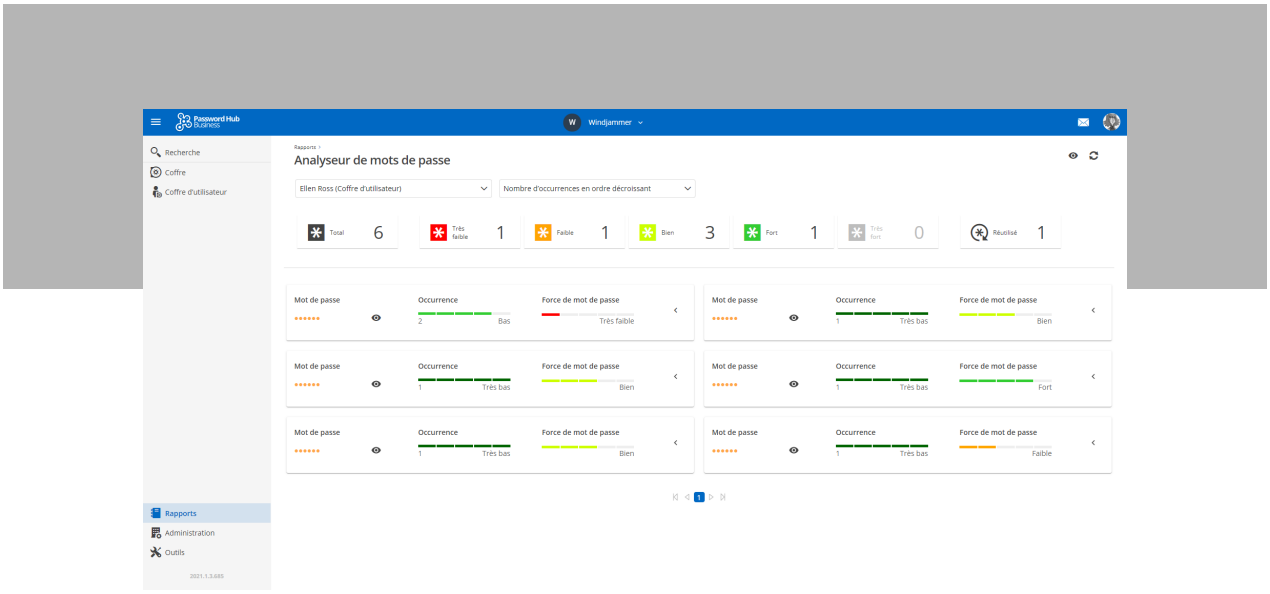


Étape 2 : Dans le menu déroulant, sélectionnez le coffre que vous souhaitez analyser.



Étape 3 : Passez en revue les résultats.

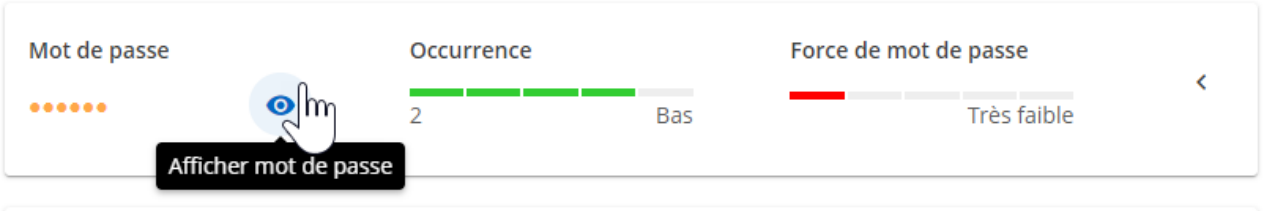
Vous pouvez aussi personnaliser **l'occurrence** (le nombre de fois où le même mot de passe est utilisé sur plusieurs entrées) de manière à ce qu'elle soit affichée par ordre décroissant, ou que la force du mot de passe soit affichée en ordre croissant. L'exemple ci-dessous montre qu'elle est définie par ordre décroissant. C'est pourquoi le premier résultat du rapport a une occurrence de 2, tandis que le dernier résultat a une occurrence de 1.



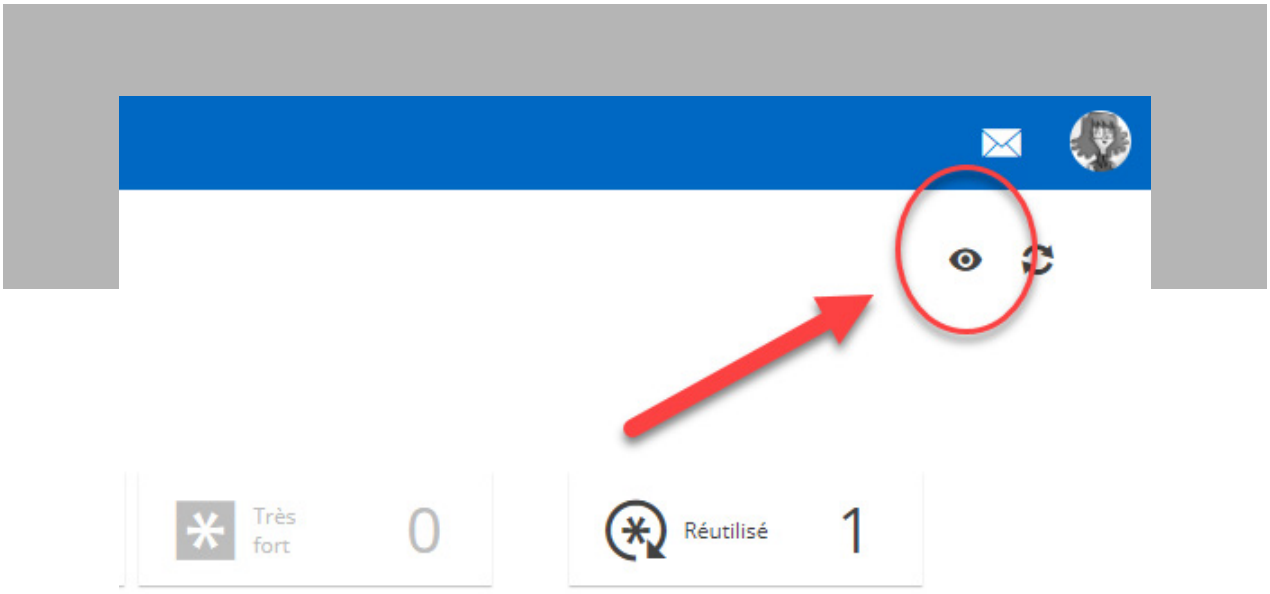
Vous observerez aussi que le rapport est classifié par couleur (pour l'occurrence et la force du mot de passe), ce qui rend encore plus rapide et facile l'évaluation des bonnes pratiques :

- Vert foncé signifie un mot de passe très fort.
- Vert signifie un mot de passe fort.
- Jaune signifie un mot de passe bon.
- Orange signifie un mot de passe faible.
- Rouge signifie un mot de passe très faible.

Si vous le souhaitez, vous pouvez également cliquer sur l'icône « œil » pour afficher un mot de passe en particulier.

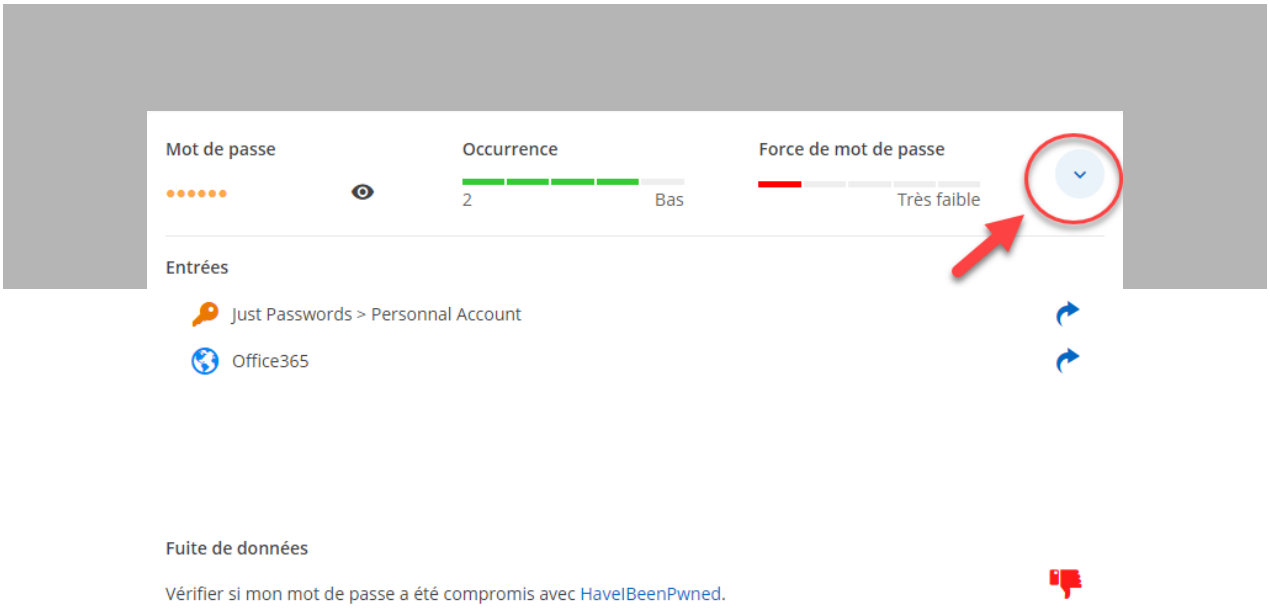


Si vous souhaitez voir tous les mots de passe d'un coffre, cliquez sur l'icône « œil » en haut à droite du rapport, ce qui révélera la liste complète.

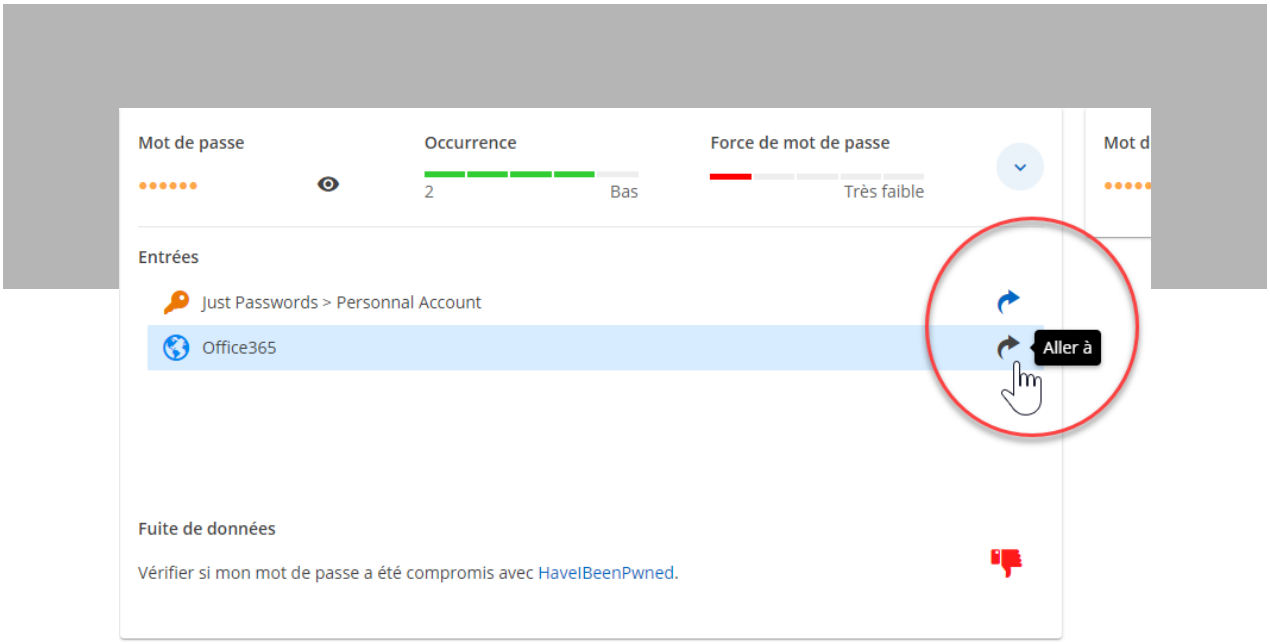


Affichage élargi

Vous avez besoin de plus de détails? Cliquez sur la petite flèche à droite de l'indicateur de force du mot de passe, ce qui indiquera toutes les entrées où un mot de passe est réutilisé.

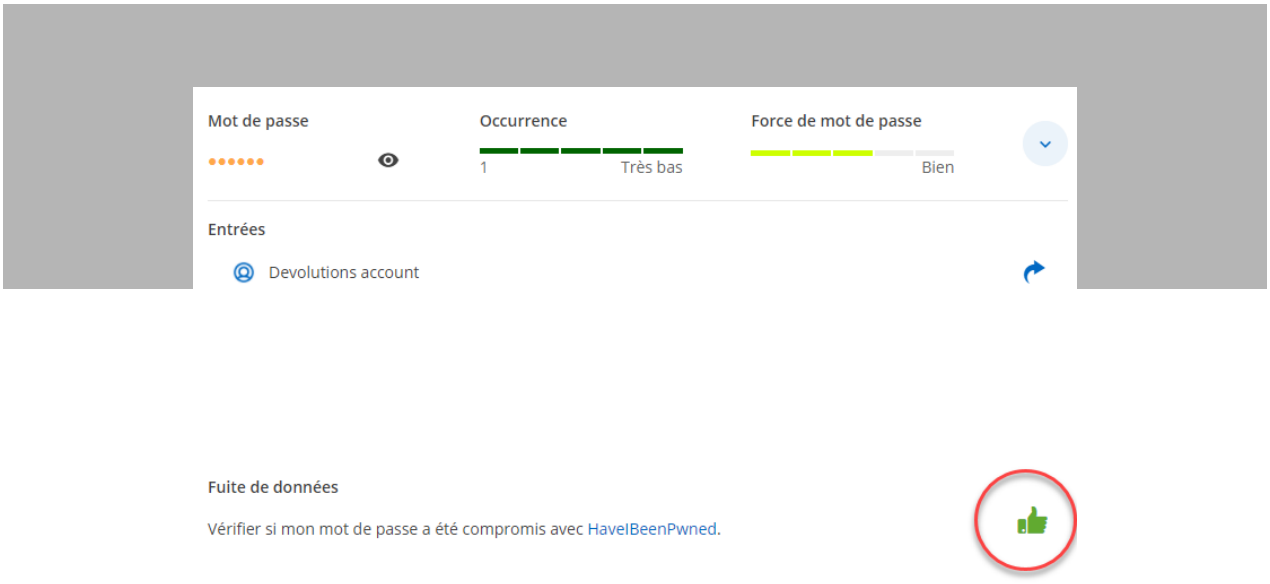


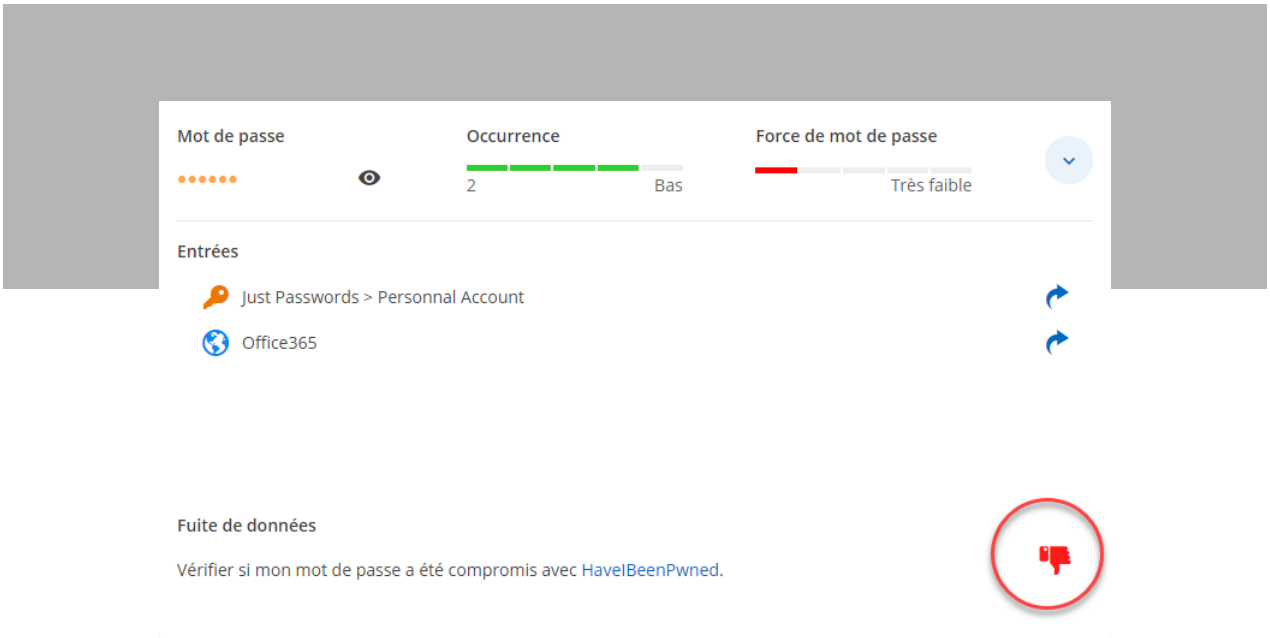
En cliquant sur la flèche bleue « **Aller à** » propre à chaque entrée, vous pourrez modifier le mot de passe associé et revenir au rapport par la suite.



HaveIBeenPwned?

Le rapport d'analyseur de mots de passe vérifie également dans la base de données HaveIBeenPwned si le mot de passe a été piraté. Lorsque vous vous trouvez en mode d'affichage élargi, un pouce vert vers le haut signifie que le mot de passe n'a pas été piraté, tandis qu'un pouce rouge vers le bas signifie que le mot de passe a été piraté. Dans ce cas, le mot de passe n'est pas sûr et doit être changé immédiatement.





Laissez-nous un commentaire

On espère que le nouveau rapport vous sera utile et qu'il vous aidera à adopter les bonnes pratiques de sécurité au sein de votre entreprise. **Dites-nous ce que vous en pensez en laissant un commentaire ci-dessous ou en publiant sur notre forum.**