ARTICLE DE LA BASE DE CONNAISSANCES

Indicateur de robustesse des mots de passe dans Password Vault : signification des niveaux

2026 © Vitextra SIA. Tous droits réservés.

Clause d'exclusion de responsabilité

Aux fins du présent Avis de non-responsabilité :

- La **Société** (désignée par « la Société », « Nous » ou « Notre » dans le présent Avis de non-responsabilité) désigne Vitextra SIA, Matīsa iela 61-25, Rīga, LV-1009, Latvia.
- Le **Document** désigne l'article de la base de connaissances.
- **Vous** désigne la personne physique qui accède au Document, ou la société ou autre entité juridique pour le compte de laquelle cette personne accède au Document ou l'utilise, selon le cas.
- Le **Site web** désigne Vitextra, accessible à l'adresse https://vitextra.com

Avis de non-responsabilité

Les informations contenues dans le Document sont fournies à titre purement informatif et général.

La Société décline toute responsabilité quant aux erreurs ou omissions dans le contenu du Document.

En aucun cas la Société ne pourra être tenue responsable de dommages spéciaux, directs, indirects, consécutifs ou accessoires, ni de quelque dommage que ce soit, que ce soit dans le cadre d'une action contractuelle, d'une action en négligence ou d'une autre action délictuelle, résultant de l'utilisation du contenu du Document ou en lien avec celle-ci. La Société se réserve le droit d'ajouter, de supprimer ou de modifier le contenu du Document à tout moment et sans préavis.

Avis de non-responsabilité relatif aux erreurs et omissions

Les informations fournies dans le Document sont destinées uniquement à une orientation générale sur des sujets d'intérêt. Par conséquent, des erreurs peuvent survenir, même si la Société prend toutes les précautions pour que le contenu du Document soit à jour et exact. En outre, compte tenu de l'évolution des lois, règles et réglementations, les informations contenues dans le Document peuvent comporter des retards, des omissions ou des inexactitudes.

La Société n'est responsable ni des erreurs ou omissions, ni des résultats obtenus par l'utilisation de ces informations.

Avis de non-responsabilité relatif à l'usage équitable

La Société peut utiliser des contenus protégés par le droit d'auteur que le titulaire des droits n'a pas expressément autorisés. La Société met ces contenus à disposition à des fins de critique, de commentaire, de reportage d'actualité, d'enseignement, d'étude ou de recherche.

La Société estime que cela constitue un « usage équitable » (« fair use ») de ces contenus protégés par le droit d'auteur, au sens de la Section 107 de la loi américaine sur le droit d'auteur (United States Copyright Act).

Si Vous souhaitez utiliser des contenus protégés par le droit d'auteur issus du Document pour Vos propres besoins, au-delà de l'usage équitable, Vous devez obtenir l'autorisation du titulaire des droits d'auteur.

Avis de non-responsabilité « Utilisation à Vos propres risques »

Toutes les informations du Document sont fournies « en l'état », sans garantie d'exhaustivité, d'exactitude, d'actualité ni des résultats obtenus par l'utilisation de ces informations, et sans garantie d'aucune sorte, expresse ou implicite, y compris, mais sans s'y limiter, les garanties de performance, de qualité marchande et d'adéquation à un usage particulier.

La Société ne sera responsable ni envers Vous ni envers quiconque de toute décision prise ou de toute action entreprise sur la base des informations fournies dans le Document, ni de tout dommage consécutif, spécial ou similaire, même si elle a été informée de la possibilité de tels dommages.

Nous contacter

Si Vous avez des questions concernant le présent Avis de non-responsabilité, Vous pouvez Nous contacter par e-mail : support@vitextra.com.

Table des matières

Où l'indicateur apparaît 4

Les cinq niveaux 4

Comment l'estimation est calculée 4

Exemples 5

L'indicateur n'empêche pas l'enregistrement 6

Conseils pour un mot de passe plus robuste 6

Où l'indicateur apparaît

Dans les boîtes de dialogue **Nouvel élément** et **Modifier les propriétés** de Password Vault, un indicateur de robustesse s'affiche directement sous le champ **Mot de passe** dès que celui-ci n'est pas vide. Il se compose d'une barre de cinq segments et du libellé **Robustesse**, par exemple *Robustesse : Moyen*. L'indicateur est mis à jour à chaque caractère saisi, ainsi que lorsque le générateur de mots de passe place un nouveau mot de passe dans le champ.

Les cinq niveaux

L'indicateur estime la difficulté à deviner le mot de passe et l'exprime en bits : chaque bit supplémentaire double le nombre de tentatives dont un attaquant aurait besoin. L'estimation est convertie en cinq niveaux :

Niveau	Segments remplis	Couleur	Robustesse estimée
Très faible	1 sur 5	Rouge foncé	moins de 28 bits
Faible	2 sur 5	Orange	de 28 à moins de 40 bits
Moyen	3 sur 5	Jaune	de 40 à moins de 60 bits
Fort	4 sur 5	Vert clair	de 60 à moins de 80 bits
Très fort	5 sur 5	Vert	80 bits ou plus

Comment l'estimation est calculée

Le calcul est effectué dans votre navigateur et tient compte de quatre facteurs.

1 **Ensemble de caractères.** L'indicateur vérifie quels types de caractères le mot de passe contient et additionne leur nombre : les lettres minuscules comptent pour 26, les lettres majuscules pour 26, les chiffres pour 10, et tout autre caractère (symboles, espaces, lettres accentuées, etc.) pour 32. Un mot de passe contenant les quatre types dispose donc d'un ensemble de 94 caractères, ce qui donne environ 6,55 bits par caractère ; un mot de passe composé uniquement de lettres minuscules donne environ 4,7 bits par caractère.
2 **Longueur effective.** La longueur est réduite en présence de motifs prévisibles. Tout

caractère qui répète le précédent (`aa`) ou qui prolonge une séquence croissante ou décroissante (`ab`, `21`) n'est pas compté. En outre, la longueur effective ne peut pas dépasser le double du nombre de caractères différents du mot de passe ; un long mot de passe construit à partir de quelques caractères y gagne donc peu.

3 **Bits.** L'estimation correspond à la longueur effective multipliée par le nombre de bits par caractère de l'ensemble.

4 **Mots courants.** Si le mot de passe contient l'un des mots faibles bien connus — `password`, `passw0rd`, `qwerty`, `admin`, `welcome`, `letmein`, `123456`, `abc123`, `iloveyou`, `11111` — quelle que soit la casse, l'estimation est plafonnée à 20 bits, ce qui correspond toujours à **Très faible**, quelle que soit la longueur du reste du mot de passe.

Exemples

Les exemples suivants montrent le niveau que l'indicateur affiche pour quelques mots de passe :

Mot de passe	Niveau	Pourquoi
`Password123!`	Très faible	Contient le mot courant *password*.
`qwerty2024!`	Très faible	Contient le mot courant *qwerty*.
`abcdefgh`	Très faible	Une seule longue séquence ; presque chaque caractère est prévisible.
`48271935`	Très faible	Chiffres uniquement : un petit ensemble de 10 caractères.
`contosocrm`	Moyen	Lettres minuscules uniquement.
`Contoso2026`	Moyen	Trois types de caractères, mais seulement 11 caractères.
`7Vq!x2Lp`	Moyen	Les quatre types, mais seulement 8 caractères.

Mot de passe	Niveau	Pourquoi
`7Vq!x2Lp#9`	Fort	Les quatre types, 10 caractères.
`7Vq!x2Lp#9Dk4`	Très fort	Les quatre types, 13 caractères sans motifs.

N'utilisez aucun de ces mots de passe d'exemple.

L'indicateur n'empêche pas l'enregistrement

L'indicateur est donné à titre indicatif uniquement. Vous pouvez enregistrer une entrée avec un mot de passe **Très faible** — par exemple lorsqu'un service impose le mot de passe ou que vous enregistrez un mot de passe existant. Password Vault ne le refuse pas et ne le modifie pas ; la décision vous appartient.

Remarque

L'estimation est un calcul rapide et local. En dehors de la courte liste de mots courants ci-dessus, elle ne compare pas le mot de passe à des dictionnaires ni à des listes de mots de passe divulgués, et elle ne sait pas si vous utilisez le même mot de passe ailleurs. Un mot de passe évalué **Très fort** peut néanmoins être dangereux s'il a été réutilisé sur un autre site victime d'une fuite de données.

Conseils pour un mot de passe plus robuste

- **Allongez-le.** La longueur est le facteur le plus efficace : chaque caractère aléatoire supplémentaire ajoute jusqu'à 6,55 bits.
- **Mélangez les quatre types de caractères** — lettres majuscules et minuscules, chiffres et symboles — lorsque le service le permet.
- **Évitez les motifs :** caractères répétés, séquences du clavier ou de l'alphabet, années et mots courants listés ci-dessus.
- **Gardez à l'esprit les limites d'un petit jeu de caractères.** Un mot de passe composé uniquement de chiffres n'atteint jamais **Très fort**, car il comporte au plus 10 caractères différents.
- **Laissez le générateur s'en charger.** Un mot de passe généré de 16 caractères avec les quatre classes est pratiquement toujours **Très fort** — voir KB10445. Comment générer un mot de passe robuste avec le générateur de Password Vault.

Conseil

Après avoir amélioré un mot de passe faible dans le coffre-fort, changez-le également sur le site ou le service. La modification des entrées est décrite dans KB10443. Comment ajouter, modifier et supprimer des entrées dans Password Vault.