vitextra

WISSENSDATENBANKARTIKEL

Kennwort-Stärkeanzeige in Password Vault: Was die Stufen bedeuten

2026 © Vitextra SIA. Alle Rechte vorbehalten.

Haftungsausschluss

Für die Zwecke dieses Haftungsausschlusses:

- **Das Unternehmen** (in diesem Haftungsausschluss entweder als „das Unternehmen“, „wir“, „uns“ oder „unser“ bezeichnet) bezieht sich auf Vitextra SIA, LV-1009 Riga, Matīsa iela 61 – 25.
- **Dokument** verweist auf den Wissensdatenbank-Artikel.
- **Sie** sind die Person, die auf das Dokument zugreift, bzw. das Unternehmen oder eine andere juristische Person, in deren Namen eine solche Person auf das Dokument zugreift oder es nutzt.
- **Die Website** verweist auf Vitextra, zugänglich über https://vitextra.com

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen dienen nur der allgemeinen Information.

Das Unternehmen übernimmt keine Verantwortung für Fehler oder Auslassungen im Inhalt des Dokuments.

In keinem Fall haftet das Unternehmen für besondere, direkte, indirekte oder zufällige Schäden oder für Schäden jeglicher Art, die sich aus der Nutzung des Inhalts des Dokuments ergeben, unabhängig davon, ob es sich um eine Klage aufgrund von Vertrag, Fahrlässigkeit oder anderen Delikten handelt. Das Unternehmen behält sich das Recht vor, den Inhalt des Dokuments jederzeit und ohne vorherige Ankündigung zu ergänzen, zu streichen oder zu ändern.

Haftungsausschluss für Fehler und Auslassungen

Die in dem Dokument enthaltenen Informationen dienen lediglich als allgemeine Orientierungshilfe zu Fragen von Interesse. Daher können Fehler auftreten, auch wenn das Unternehmen alle Vorsichtsmaßnahmen ergreift, um sicherzustellen, dass der Inhalt des Dokuments aktuell und korrekt ist. Außerdem kann es angesichts der sich ändernden Gesetze, Regeln und Vorschriften zu Verzögerungen, Auslassungen oder Ungenauigkeiten bei den in diesem Dokument enthaltenen Informationen kommen.

Das Unternehmen haftet nicht für etwaige Fehler oder Auslassungen oder für die Ergebnisse, die sich aus der Verwendung dieser Informationen ergeben.

Haftungsausschluss für faire Nutzung

Das Unternehmen darf urheberrechtlich geschütztes Material verwenden, das der Urheberrechtsinhaber nicht ausdrücklich genehmigt hat. Das Unternehmen stellt dieses Material für Kritik, Kommentare, Berichterstattung, Schulung, Wissenschaft oder Forschung zur Verfügung.

Das Unternehmen ist der Ansicht, dass dies eine „faire Nutzung“ von urheberrechtlich geschütztem Material im Sinne von Abschnitt 107 des US-Urheberrechtsgesetzes darstellt.

Wenn Sie urheberrechtlich geschütztes Material aus dem Dokument für Ihre eigenen Zwecke verwenden möchten, die über eine angemessene Nutzung hinausgehen, müssen Sie die Erlaubnis des Urheberrechtsinhabers einholen.

„Benutzung auf eigene Gefahr“ Haftungsausschluss

Alle Informationen in diesem Dokument werden im Ist-Zustand zur Verfügung gestellt, ohne Garantie auf Vollständigkeit, Genauigkeit, Aktualität oder auf die Ergebnisse, die sich aus der Verwendung dieser Informationen ergeben, und ohne jegliche ausdrückliche oder stillschweigende Garantie, einschließlich, aber nicht beschränkt auf Garantien für Leistung, Marktgängigkeit und Eignung für einen bestimmten Zweck.

Das Unternehmen haftet weder Ihnen noch anderen gegenüber für Entscheidungen oder Handlungen, die im Vertrauen auf die Informationen des Dienstes getroffen wurden, noch für Folgeschäden, besondere oder ähnliche Schäden, selbst wenn auf die Möglichkeit solcher Schäden hingewiesen wurde.

Kontaktieren Sie uns

Wenn Sie Fragen zu diesem Haftungsausschluss haben, können Sie uns per E-Mail kontaktieren: support@vitextra.com.

Inhaltsverzeichnis

Wo die Anzeige erscheint 4

Die fünf Stufen 4

Wie die Schätzung berechnet wird 4

Beispiele 5

Die Anzeige verhindert das Speichern nicht 5

Tipps für ein stärkeres Kennwort 6

Wo die Anzeige erscheint

In den Dialogfeldern **Neues Element** und **Eigenschaften bearbeiten** von Password Vault wird direkt unter dem Feld **Kennwort** eine Stärkeanzeige eingeblendet, sobald das Feld nicht leer ist. Sie besteht aus einem Balken mit fünf Segmenten und der Beschriftung **Stärke**, zum Beispiel *Stärke: Mittel*. Die Anzeige wird bei jedem eingegebenen Zeichen aktualisiert und auch dann, wenn der Kennwortgenerator ein neues Kennwort in das Feld einfügt.

Die fünf Stufen

Die Anzeige schätzt, wie schwer das Kennwort zu erraten wäre, und drückt dies in Bit aus: Jedes zusätzliche Bit verdoppelt die Anzahl der Versuche, die ein Angreifer bräuchte. Die Schätzung wird fünf Stufen zugeordnet:

Stufe	Gefüllte Segmente	Farbe	Geschätzte Stärke
Sehr schwach	1 von 5	Dunkelrot	weniger als 28 Bit
Schwach	2 von 5	Orange	28 bis unter 40 Bit
Mittel	3 von 5	Gelb	40 bis unter 60 Bit
Stark	4 von 5	Hellgrün	60 bis unter 80 Bit
Sehr stark	5 von 5	Grün	80 Bit oder mehr

Wie die Schätzung berechnet wird

Die Berechnung erfolgt in Ihrem Browser und berücksichtigt vier Faktoren.

1 **Zeichenvorrat.** Die Anzeige prüft, welche Zeichenarten das Kennwort enthält, und addiert deren Anzahl: Kleinbuchstaben zählen als 26, Großbuchstaben als 26, Ziffern als 10 und jedes andere Zeichen (Sonderzeichen, Leerzeichen, Buchstaben mit diakritischen Zeichen usw.) als 32. Ein Kennwort mit allen vier Arten hat daher einen Vorrat von 94 Zeichen, was etwa 6,55 Bit pro Zeichen ergibt; ein Kennwort nur aus Kleinbuchstaben ergibt etwa 4,7 Bit pro Zeichen.

2 **Effektive Länge.** Die Länge wird bei vorhersehbaren Mustern verringert. Jedes Zeichen, das das vorherige wiederholt (aa) oder eine aufsteigende oder absteigende Folge fortsetzt (ab, 21), wird nicht gezählt. Außerdem kann die effektive Länge das Doppelte der Anzahl unterschiedlicher Zeichen im Kennwort nicht überschreiten, sodass ein langes Kennwort aus wenigen Zeichen kaum etwas gewinnt.

3 **Bit.** Die Schätzung ist die effektive Länge multipliziert mit den Bit pro Zeichen des

Vorrats.

4 **Häufige Wörter.** Enthält das Kennwort eines der bekannten schwachen Wörter – `password`, `passw0rd`, `qwerty`, `admin`, `welcome`, `letmein`, `123456`, `abc123`, `iloveyou`, `11111` – in beliebiger Groß-/Kleinschreibung, wird die Schätzung auf 20 Bit begrenzt, was immer **Sehr schwach** ist, egal wie lang der Rest des Kennworts ist.

Beispiele

Die folgenden Beispiele zeigen die Stufe, die die Anzeige für einige Kennwörter darstellt:

Kennwort	Stufe	Grund
`Password123!`	Sehr schwach	Enthält das häufige Wort *password*.
`qwerty2024!`	Sehr schwach	Enthält das häufige Wort *qwerty*.
`abcdefgh`	Sehr schwach	Eine lange Folge; fast jedes Zeichen ist vorhersehbar.
`48271935`	Sehr schwach	Nur Ziffern: ein kleiner Vorrat von 10 Zeichen.
`contosocrm`	Mittel	Nur Kleinbuchstaben.
`Contoso2026`	Mittel	Drei Zeichenarten, aber nur 11 Zeichen lang.
`7Vq!x2Lp`	Mittel	Alle vier Arten, aber nur 8 Zeichen lang.
`7Vq!x2Lp#9`	Stark	Alle vier Arten, 10 Zeichen.
`7Vq!x2Lp#9Dk4`	Sehr stark	Alle vier Arten, 13 Zeichen ohne Muster.

Verwenden Sie keines dieser Beispielkennwörter.

Die Anzeige verhindert das Speichern nicht

Die Anzeige dient nur zur Orientierung. Sie können einen Eintrag auch mit einem Kennwort der Stufe **Sehr schwach** speichern – zum Beispiel, wenn ein Dienst das Kennwort vorgibt oder Sie ein bestehendes Kennwort erfassen. Password Vault lehnt es weder ab noch ändert es; die Entscheidung liegt bei Ihnen.

Hinweis

Die Schätzung ist eine schnelle, lokale Berechnung. Abgesehen von der kurzen Liste häufiger Wörter oben vergleicht sie das Kennwort weder mit Wörterbüchern noch mit Listen geleakter Kennwörter, und sie weiß nicht, ob Sie dasselbe Kennwort anderswo verwenden. Ein als **Sehr stark** bewertetes Kennwort kann dennoch unsicher sein, wenn es auch auf einer anderen Website verwendet wurde, deren Daten kompromittiert wurden.

Tipps für ein stärkeres Kennwort

- **Machen Sie es länger.** Die Länge ist der wirksamste Faktor: Jedes zusätzliche zufällige Zeichen bringt bis zu 6,55 Bit.
- **Kombinieren Sie alle vier Zeichenarten** – Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen –, sofern der Dienst es zulässt.
- **Vermeiden Sie Muster:** wiederholte Zeichen, Tastatur- oder Alphabetfolgen, Jahreszahlen und die oben aufgeführten häufigen Wörter.
- **Bedenken Sie die Grenzen eines kleinen Zeichenvorrats.** Ein Kennwort nur aus Ziffern erreicht nie die Stufe **Sehr stark**, da es höchstens 10 unterschiedliche Zeichen enthält.
- **Überlassen Sie es dem Generator.** Ein generiertes Kennwort aus 16 Zeichen mit allen vier Klassen ist praktisch immer **Sehr stark** – siehe KB10445. So generieren Sie ein starkes Kennwort mit dem Kennwortgenerator von Password Vault.

Tipp

Wenn Sie ein schwaches Kennwort im Tresor verbessert haben, ändern Sie es auch auf der Website oder im Dienst. Das Bearbeiten von Einträgen ist in KB10443. So fügen Sie Einträge in Password Vault hinzu, bearbeiten und löschen sie beschrieben.