KNOWLEDGE BASE ARTICLE

Password Strength Meter in Password Vault: What the Levels Mean

2026 © Vitextra SIA. All rights reserved.

Disclaimer

For the purposes of this Disclaimer:

- **Company** (referred to as either "the Company", "We", "Us" or "Our" in this Disclaimer) refers to Vitextra SIA, LV-1009 Riga, Matise iela 61 - 25.
- **Document** refers to the Knowledgebase Article.
- **You** means the individual accessing the Document, or the company, or other legal entity on behalf of which such individual is accessing or using the Document, as applicable.
- **Website** refers to Vitextra, accessible from https://vitextra.com

Disclaimer

The information contained in the Document is for general information purposes only.

The Company assumes no responsibility for errors or omissions in the contents of the Document.

In no event shall the Company be liable for any special, direct, indirect, consequential, or incidental damages or any damages whatsoever, whether in an action of contract, negligence, or other torts, arising out of or in connection with the use of the contents of the Document. The Company reserves the right to make additions, deletions, or modifications to the contents in the Document at any time without prior notice.

Errors and Omissions Disclaimer

The information given by the Document is for general guidance on matters of interest only. Therefore, errors can occur even if the Company takes every precaution to ensure that the Document's content is current and accurate. Plus, given the changing nature of laws, rules, and regulations, there may be delays, omissions, or inaccuracies in the information contained in the Document.

The Company is not responsible for any errors or omissions, or for the results obtained from the use of this information.

Fair Use Disclaimer

The Company may use copyrighted material that the copyright owner has not explicitly authorized. The Company is making such material available for criticism, comment, news reporting, teaching, scholarship, or research.

The Company believes this constitutes a "fair use" of any such copyrighted material as provided for in section 107 of the United States Copyright law.

If You wish to use copyrighted material from the Document for your own purposes that go beyond fair use, You must obtain permission from the copyright owner.

"Use at Your Own Risk" Disclaimer

All information in the Document is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

The Company will not be liable to You or anyone else for any decision made or action taken in reliance on the information given by the Service or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Contact Us

If you have any questions about this Disclaimer, You can contact Us by email: support@vitextra.com.

Table Of Contents

Where the meter appears 4

The five levels 4

How the estimate is calculated 4

Examples 5

The meter does not block saving 6

Tips for a stronger password 6

Where the meter appears

In the **New Item** and **Edit Properties** dialogs of Password Vault, a strength meter is shown directly under the **Password** field as soon as the field is not empty. It consists of a bar of five segments and the label **Strength**, for example *Strength: Fair*. The meter is updated with every character you type, and also when the password generator puts a new password into the field.

The five levels

The meter estimates how hard the password would be to guess and expresses it in bits: each additional bit doubles the number of guesses an attacker would need. The estimate is mapped to five levels:

Level	Filled segments	Colour	Estimated strength
Very weak	1 of 5	Dark red	less than 28 bits
Weak	2 of 5	Orange	28 to less than 40 bits
Fair	3 of 5	Yellow	40 to less than 60 bits
Strong	4 of 5	Light green	60 to less than 80 bits
Very strong	5 of 5	Green	80 bits or more

How the estimate is calculated

The calculation is done in your browser and takes four factors into account.

1 **Character pool.** The meter checks which kinds of characters the password contains and adds up their number: lowercase letters count as 26, uppercase letters as 26, digits as 10, and any other character (symbols, spaces, letters with diacritics and so on) as 32. A password with all four kinds therefore has a pool of 94 characters, which gives about 6.55 bits per character; a password of lowercase letters only gives about 4.7 bits per character.

2 **Effective length.** The length is reduced for predictable patterns. Every character that repeats the previous one (`aa`) or continues an ascending or descending sequence (`ab`, `21`) is not counted. In addition, the effective length cannot exceed twice the number of different characters in the password, so a long password built from a few

characters gains little.

3 **Bits.** The estimate is the effective length multiplied by the bits per character of the pool.

4 **Common words.** If the password contains one of the well-known weak words — `password`, `passw0rd`, `qwerty`, `admin`, `welcome`, `letmein`, `123456`, `abc123`, `iloveyou`, `11111` — in any letter case, the estimate is capped at 20 bits, which is always **Very weak**, however long the rest of the password is.

Examples

The following examples show the level the meter displays for some passwords:

Password	Level	Why
`Password123!`	Very weak	Contains the common word *password*.
`qwerty2024!`	Very weak	Contains the common word *qwerty*.
`abcdefgh`	Very weak	One long sequence; almost every character is predictable.
`48271935`	Very weak	Digits only: a small pool of 10 characters.
`contosocrm`	Fair	Lowercase letters only.
`Contoso2026`	Fair	Three kinds of characters, but only 11 characters long.
`7Vq!x2Lp`	Fair	All four kinds, but only 8 characters long.
`7Vq!x2Lp#9`	Strong	All four kinds, 10 characters.
`7Vq!x2Lp#9Dk4`	Very strong	All four kinds, 13 characters without patterns.

Do not use any of these example passwords.

The meter does not block saving

The meter is indicative only. You can save an entry with a **Very weak** password — for example when a service dictates the password or you are recording an existing one. Password Vault does not reject or change it; the decision is yours.

Note

The estimate is a quick, local calculation. Apart from the short list of common words above, it does not compare the password with dictionaries or with lists of leaked passwords, and it does not know whether you use the same password elsewhere. A password rated **Very strong** can still be unsafe if it has been reused on another site that was breached.

Tips for a stronger password

- **Make it longer.** Length is the most effective factor: every additional random character adds up to 6.55 bits.
- **Mix all four kinds of characters** — uppercase and lowercase letters, digits and symbols — where the service allows it.
- **Avoid patterns:** repeated characters, keyboard or alphabet sequences, years and the common words listed above.
- **Remember the limits of a small character set.** A password made only of digits never reaches **Very strong**, because it has at most 10 different characters.
- **Let the generator do it.** A generated password of 16 characters with all four classes is practically always **Very strong** — see KB10445. How to Generate a Strong Password with the Password Vault Generator.

Tip

After you have improved a weak password in the vault, change it on the site or service as well. Editing entries is described in KB10443. How to Add, Edit and Delete Entries in Password Vault.