KNOWLEDGE BASE ARTICLE

How to Generate a Strong Password with the Password Vault Generator

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

Introduction 4

Opening the generator 4

Generator options 5

How the password is generated 6

Recommendations 7

Introduction

Passwords that people invent themselves tend to be short and predictable: a word, a year, an exclamation mark. Since Password Vault remembers the password for you, there is no reason to keep it memorable. The built-in generator creates a random password of the length and character set you choose and puts it straight into the entry.

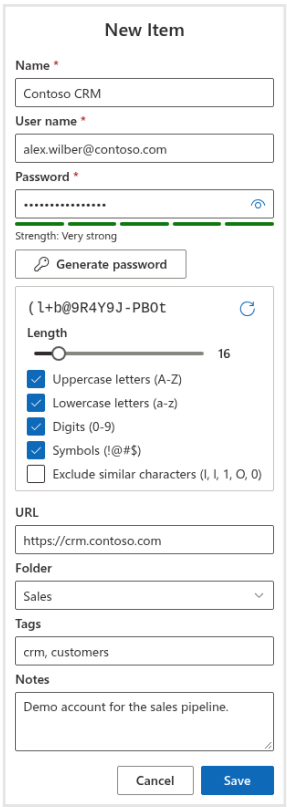
The generator is part of the **New Item** and **Edit Properties** dialogs, so you use it while creating or editing an entry (see KB10443. How to Add, Edit and Delete Entries in Password Vault). These dialogs are available only while the vault is unlocked.

Opening the generator

1 Click **New Item**, or expand an existing entry and click **Edit**.
2 Under the **Password** field, click **Generate password**.

The generator panel opens below the button and a new password is generated immediately: it appears in the panel and is put into the **Password** field at the same time. The strength meter under the field shows its estimated strength.

Click **Generate password** again to close the panel. The last generated password stays in the **Password** field.



The password generator panel

Warning

In the **Edit Properties** dialog, opening the generator replaces the current password in the **Password** field right away, and every change in the panel replaces it again. If you only wanted to look at the generator, click **Cancel**: the entry keeps its old password. If you click **Save**, the new password is stored — change it on the site or service as well.

Generator options

Option	Default	Description
Preview and **Generate again**	—	The generated password in plain text. The **Generate again** button (circular arrow) creates a new password with the same settings.
Length	16	A slider from 8 to 64 characters.

Option	Default	Description
Uppercase letters (A-Z)	On	Include capital letters.
Lowercase letters (a-z)	On	Include small letters.
Digits (0-9)	On	Include digits.
Symbols (!@#$)	On	Include the symbols `! @ # $ % ^ & * ( ) - _ = + [ ] { } ; : , . ?`
Exclude similar characters (I, l, 1, O, 0)	Off	Leave out characters that are easy to confuse when a password is read or typed by hand: `I`, `l`, `1`, `O`, `0` and also the lowercase `o`.

Every change — moving the slider, selecting or clearing a check box — generates a new password at once and puts it into the **Password** field. You do not need a separate confirmation; the field always contains the password shown in the preview.

Note

The preview shows the generated password as plain text, while the **Password** field keeps it masked. Make sure nobody is looking at your screen while the panel is open.

How the password is generated

- **Every selected character class is guaranteed.** The password always contains at least one character from each class you have selected — for example at least one digit when **Digits (0-9)** is on. The remaining characters are picked from all selected classes together.
- **The characters are shuffled.** After the password is assembled, its characters are shuffled randomly, so the guaranteed characters do not always sit at the beginning.
- **If you clear all four classes,** the generator does not stop: it uses lowercase letters.
- **The random source is cryptographic.** Characters are chosen with the browser's cryptographic random number generator (`crypto.getRandomValues`), not with an ordinary pseudo-random function, and in a way that gives every character of the set the same probability (no modulo bias).

- **Everything happens in your browser.** The password is generated on your device and travels only as part of your encrypted vault file, between your browser and your OneDrive, when you save the entry. Vitextra receives no vault data (see KB10363. Where Vitextra Products Store Your Data: Privacy, Data Residency and GDPR).

Recommendations

- **Keep the default length of 16 or more.** With all four classes on, a generated 16-character password is practically always rated **Very strong** by the strength meter. A password of the minimum length of 8 characters is rated **Fair** at best, even with all four classes.
- **Use all four classes when the service allows it.** If a site does not accept some symbols, clear **Symbols (!@#$)** and increase the length instead — length adds more strength than a larger character set.
- **Exclude similar characters only when needed** — for a password that someone will read aloud or type from a printout. It slightly reduces the number of possible characters.
- **Use a different password for every account.** With the generator and the vault, there is no extra effort in doing so.
- **Save the entry first, then set the password on the service.** After saving, expand the entry and use **Copy to Clipboard** to paste the password into the service's "change password" form (see KB10444. How to View and Copy a Password or User Name in Password Vault). This way the new password is never lost between the two steps.

Tip

What the strength levels mean and how they are calculated is described in KB10446. Password Strength Meter in Password Vault: What the Levels Mean. For a short introduction to all everyday tasks, see KB10441. Password Vault: A Quick Guide for End Users.