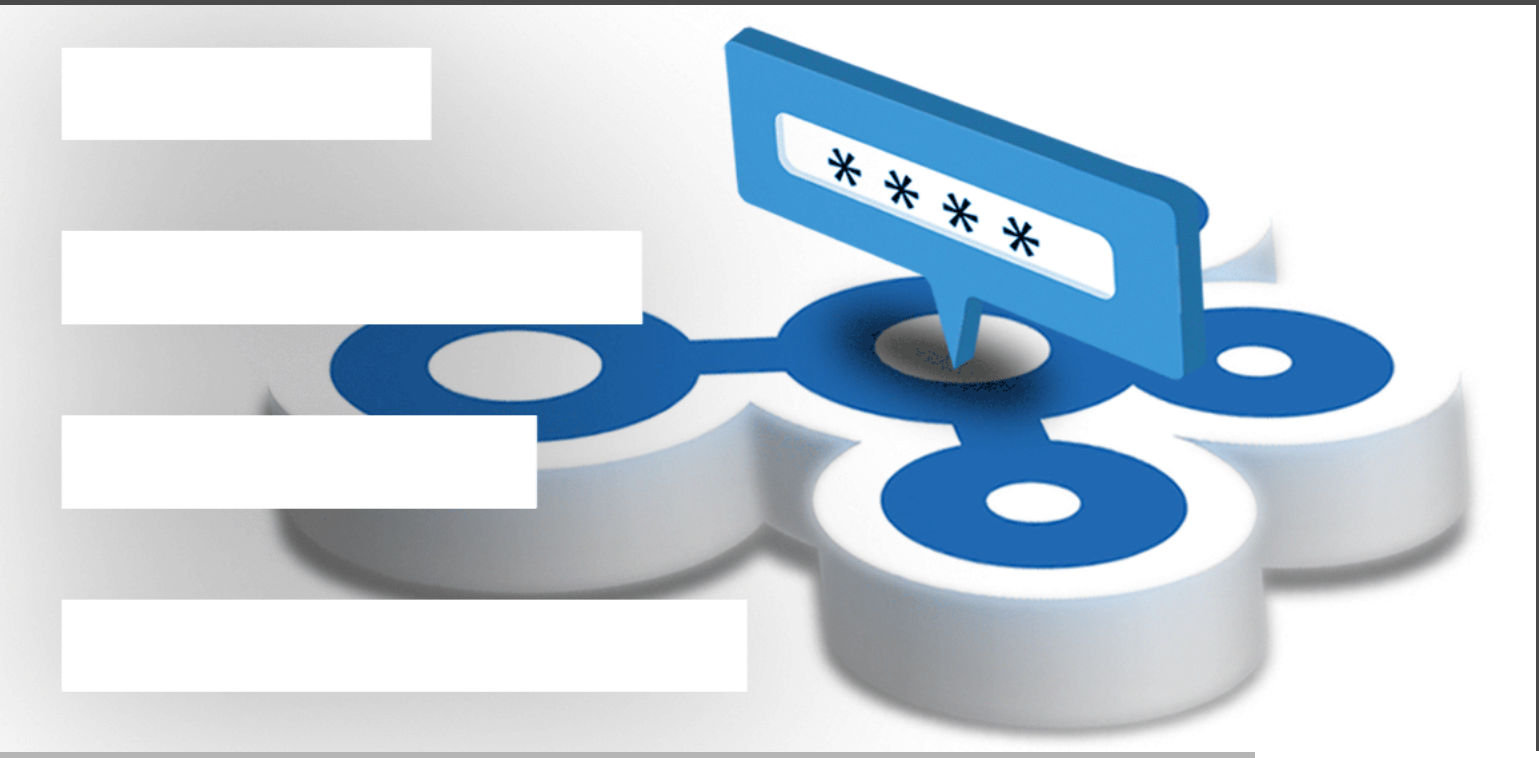
Devolutions

[New Feature Spotlight] Password Analyzer Report in Password Hub Business 2021.1.



INCLUDES SEVERAL ADDITIONS AND ENHANCEMENTS

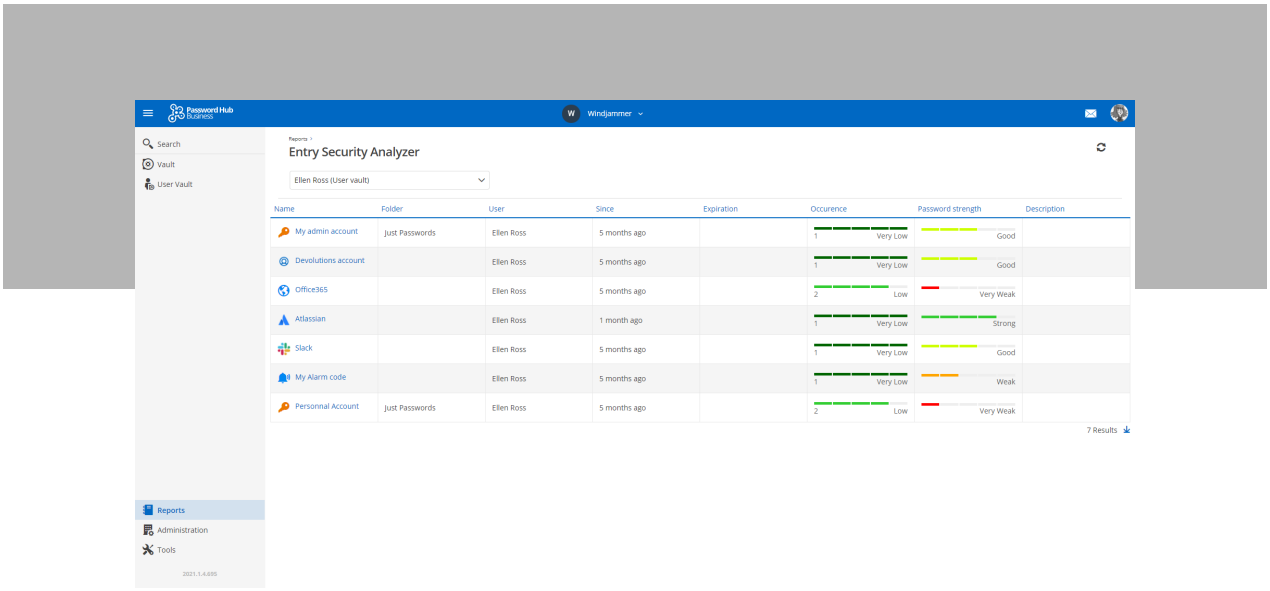
Recently, we launched the much anticipated version 2021.1 of Password Hub Business, which includes several additions and enhancements. Today, I'm taking a deeper look at one of the most important and exciting new features: **Password Analyzer Report**. As you will see in a moment, this report is designed to help you improve security hygiene across your organization — which is essential for preventing data breaches and leaks.

The Entry Security Analyzer

Before we explore the Password Analyzer Report, let's take a quick look at another feature in Password Hub Business that used to be called Password Analyzer (and is still called this in Remote Desktop Manager and Devolutions Server), but is now called Entry Security Analyzer.

This feature highlights key security information about entries, such as:

- The last time the password of the entry was modified.
- How many times a password has been re-used for the same vault.
- If a password used in an entry is very strong, strong, good, weak, or very weak.



While the Entry Security Analyzer is useful for improving security hygiene, it focuses on entries. **But what if you want to focus on passwords instead?** This is where the new Password Analyzer Report comes in!

About the Password Analyzer Report

The Password Analyzer Report is only available in Password Hub Business (i.e. you will not find it yet in Remote Desktop Manager or Devolutions Server), and it adds another critical layer of password hygiene.

As mentioned above, the Password Analyzer Report focuses on passwords — not entries. **Specifically, it reveals:**

- How many passwords are associated with a vault.
- How many of those passwords are very strong, strong, good, weak, or very weak.
- How many times a password is used across all of the entries in a vault.

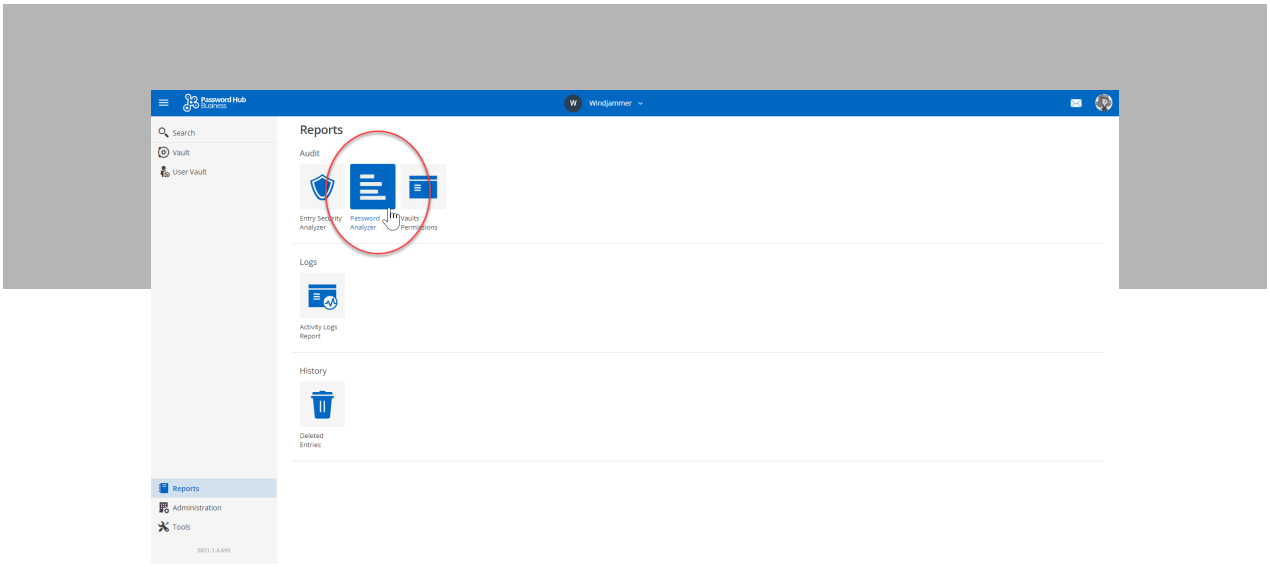
One of the most important advantages of the Password Analyzer Report vs. the Entry Security Analyzer is that the **Password Analyzer Report highlights where vulnerabilities exist** — so they can be targeted and fixed right away. For example, if you have 30 re-used passwords, with the Entry Security Analyzer you need to hunt down each one, which can be an administrative burden. But **with the Password Analyzer Report, you know exactly where each one is**. You can even jump to them directly, as we will discuss later on in this article. **First, let's look at generating a report.**

How to Generate a Password Analyzer Report

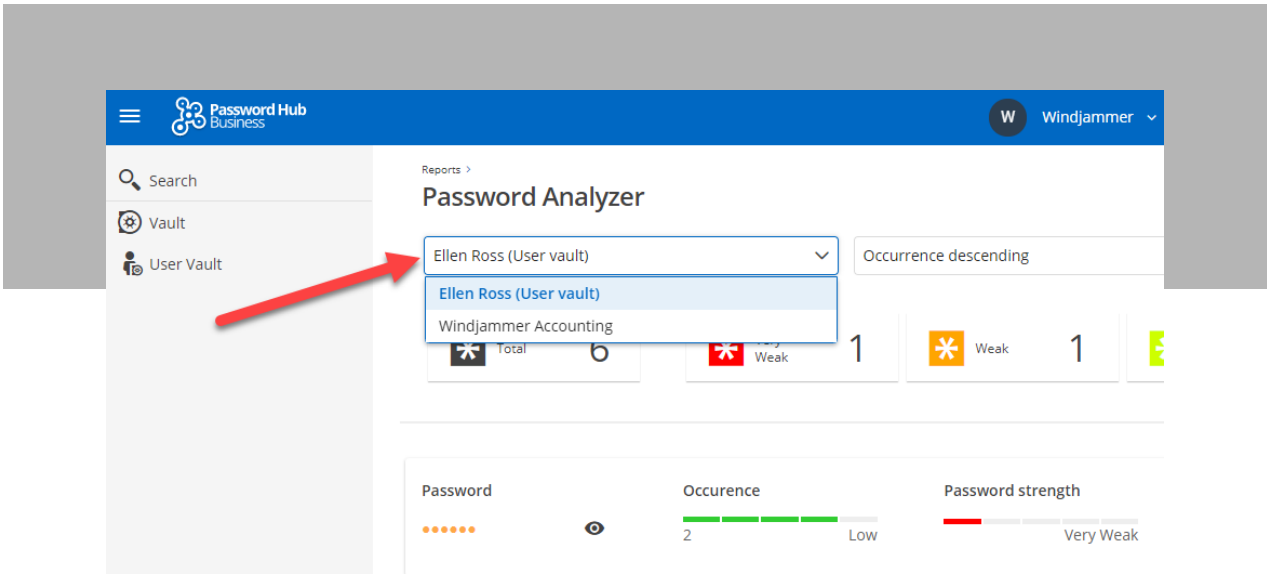
The Password Analyzer Report is available to all users. Admins can generate reports for all vaults, while other users can generate reports for vaults they have access to. In this way, everyone plays a role in improving security hygiene — not just Admins.

Generating a Password Analyzer Report is fast and easy. **Here are the steps:**

Step 1: Click on ***Reports*** and select ***Password Analyzer***.

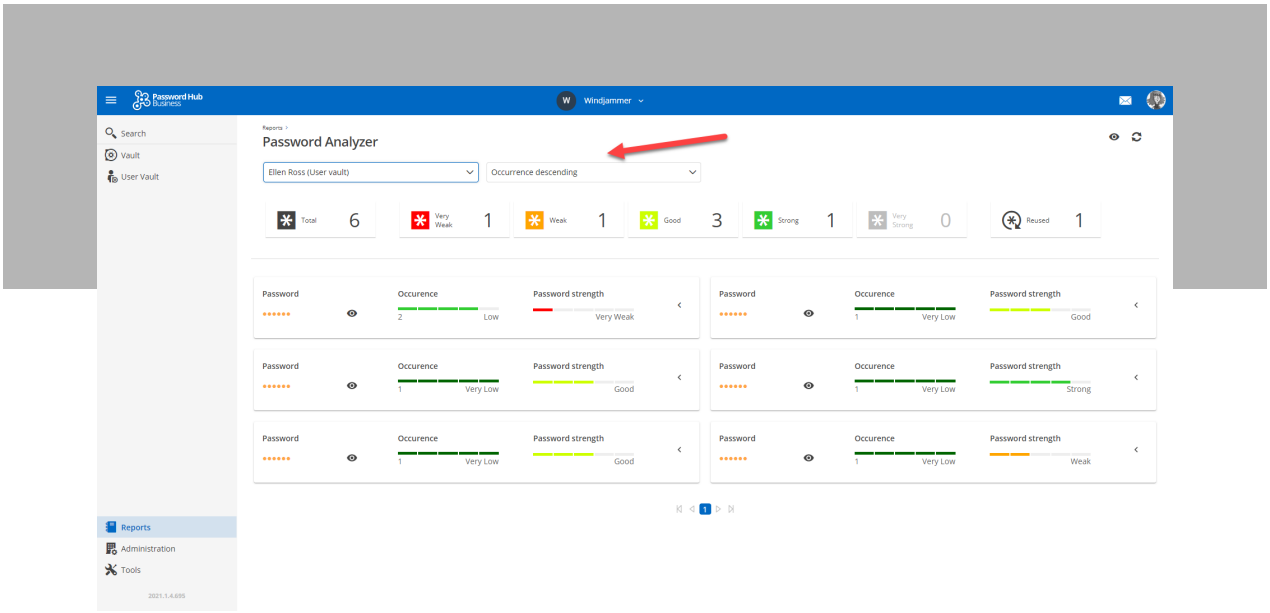


Step 2: From the dropdown menu, choose the vault you want to analyze.



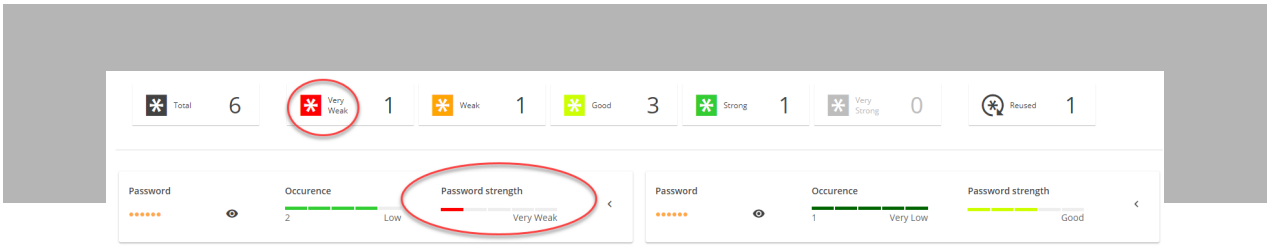
Step 3: Review the results.

Note that you can also toggle whether you want the **occurrence** (i.e., the number of times the same password is used across multiple entries) to be displayed in descending order or the **password strength** to be displayed in ascending order. In the example below, it is set to occurrence descending order, which is why the first result in the report has an occurrence of 2, while the last result has an occurrence of 1.

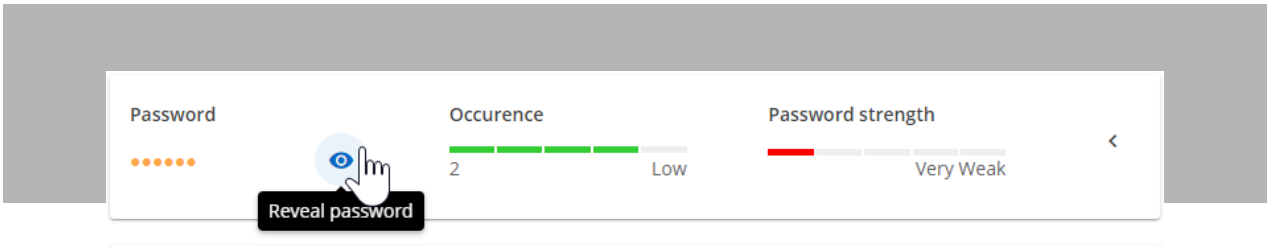


You will also notice that the report is **color-coded** (for both occurrence and password strength), which makes it even faster and easier to assess password hygiene:

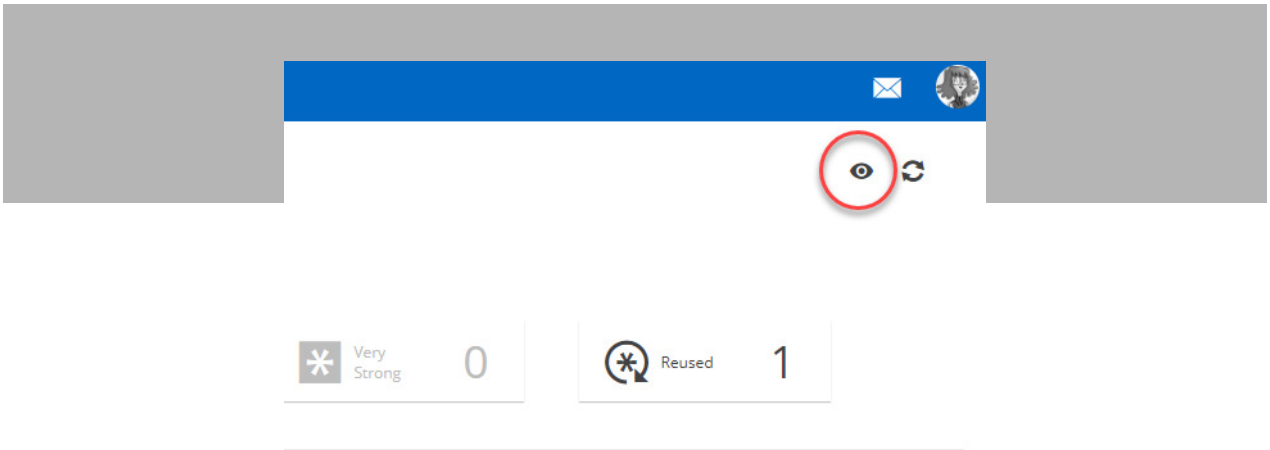
- Dark green indicates a very strong password.
- Green indicates a strong password.
- Yellow indicates a good password .
- Orange indicates a weak password.
- Red indicates a very weak password.



If you wish, you can also click the "eye" icon to see a specific password.

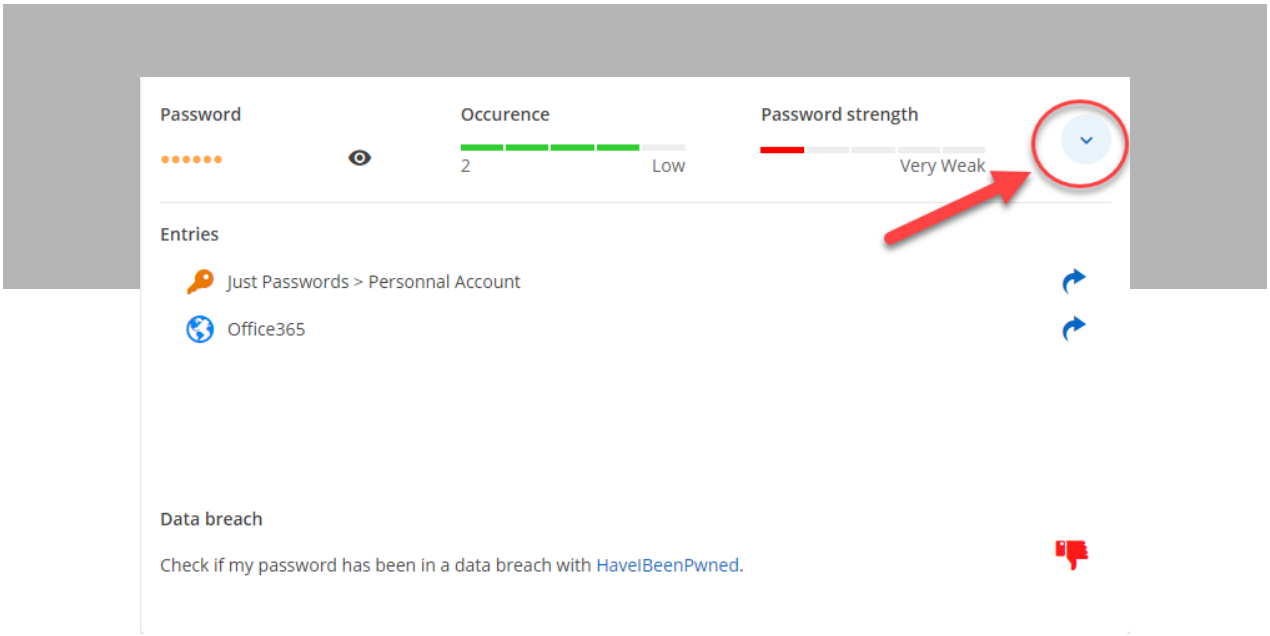


And if you want to see all of the passwords in a selected vault, simply click on the "eye" icon at the top-right corner of the Password Analyzer Report, which will toggle a global reveal.

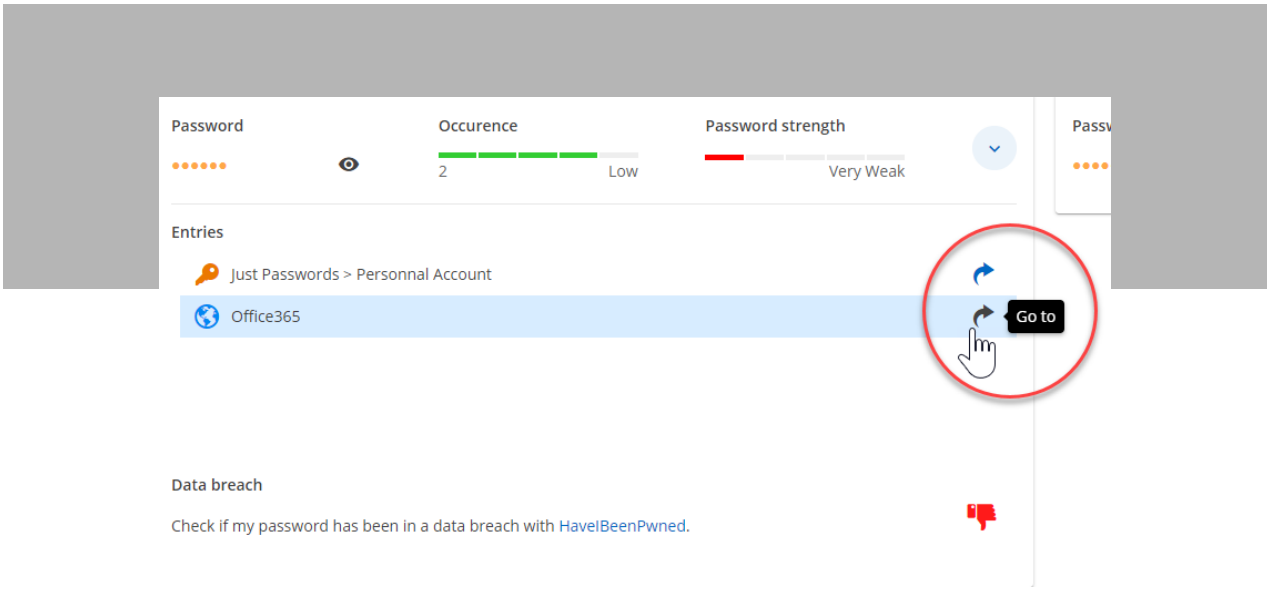


Expanded View

If you want more detail, then click on the small arrow to the right of the Password strength indicator. This will reveal all of the entries where a password is reused.

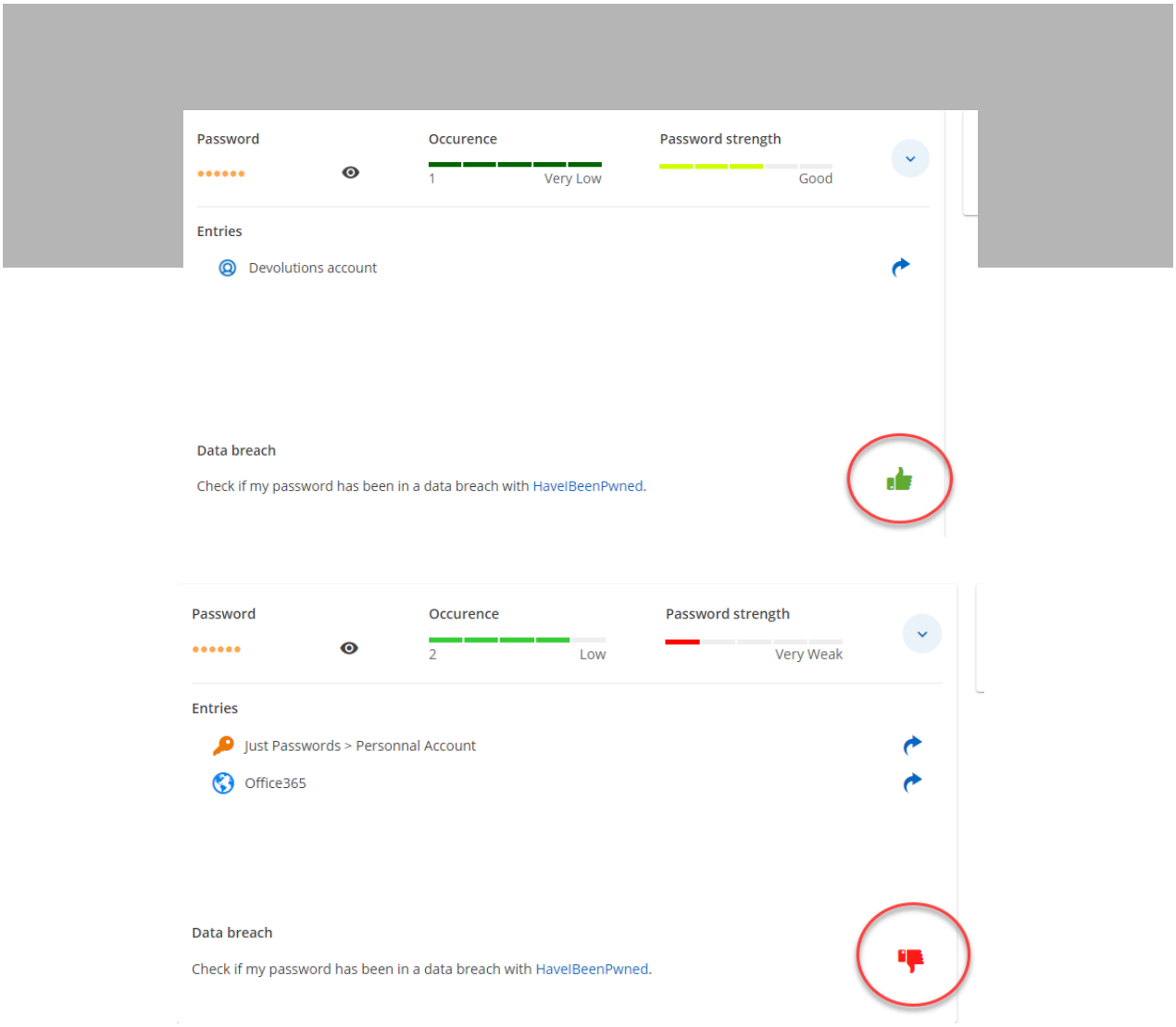


By clicking the blue ***"Go to"*** arrow on each entry, you can go directly to that entry to change the password, and then jump back to the report.



HaveIBeenPwned?

Lastly, we have integrated the Password Analyzer Report with the HaveIBeenPwned? database. In the expanded view, you will see an icon that will tell you whether your password has been used in a breach. A green thumbs up means that the password is OK, while a red thumbs down means that the password has been breached. In that case, the password is not safe and should be changed.



Send Us Your Feedback

We hope that you find the Password Analyzer Report useful, and that it helps you improve security hygiene across your organization. Please share your feedback by commenting below or by posting in our forum.