



Most Popular Password Managers Compared

Devolutions

LASTPASS vs KEEPASS vs 1PASSWORD vs PASSWORD VAULT MANAGER vs DASHLANE vs PASSWORDSTATE vs KEEPER vs STICKY PASSWORD

There are a lot of options out there for password manager software, but finding the one that will fulfill your needs can sometimes feel overwhelming and a tad like trying to find a needle in a haystack. To help you find the one that will fit you like a glove, we've gathered some of the most popular ones and broken down their features.

A great password manager software should be of great help in your everyday routine by generating, managing and storing all of your passwords for you. It should be able to generate secure passwords rapidly, and save them automatically in an encrypted database.

Some of the features that we look for in a great password manager are security assessments, random-character generation, and automatic login on your favourite websites.

Now let's start doing some digging and take a closer look at some of the most popular password manager applications. As you all know there are password management software that are more enterprise driven and made for larger teams like [Secret Server](#), [AuthAnvil](#), [Lieberman](#), [CyberArk](#) and [ManageEngine](#). However, we have opted for the utmost popular ones according to our RDMers: [LastPass](#), [KeePass](#), [1Password](#), [Password Vault Manager](#), [Dashlane](#) and [Passwordstate](#).

LastPass... |

LASTPASS IS ONE OF THE MOST WIDELY KNOWN AND WIDELY USED PASSWORD MANAGERS.

WHAT WE LOVE

CONVENIENT ACCESS: With the browser extensions, you can use LastPass with almost any browser available to you. Your login and password information are automatically saved on LastPass's servers, and are available to you from any computer with the extension installed.

PASSWORDS ON THE GO: If browsing on your phone or tablet is part of your daily routine, then LastPass might be the perfect fit for you. It is available on Android and iOS, but you also have the options of having it on your Windows Phone or Blackberry.

PASSWORD CHANGES: LastPass keeps a database of hacks on the web and will alert you if your accounts have been affected by a breach of another website. Once you have been notified, you can easily and quickly change your password with just a mouse click.

PASSWORD AUDITS: LastPass performs an "audit" of your passwords, highlighting weak or duplicate passwords, and then helps you create more secure ones. It is a top-tier feature that really makes it easy to test both the quality of your passwords as well as making changes to enhance them.

WHERE IT NEEDS IMPROVEMENT

INTERFACE: You might find LastPass's interface a little hefty, while they are improving it with the new LastPass 4.0, some users could still take a while to get the hang of it.

PASSWORD STORAGE: The software keeps your encrypted passwords in the cloud, which might make some of you uncomfortable, but it will still keep your passwords safe from hackers. LastPass quickly and efficiently notify users if a breach occurs. By enabling the two-factor authentication you will be even more protected from any intrusion.

WHO IT'S FOR

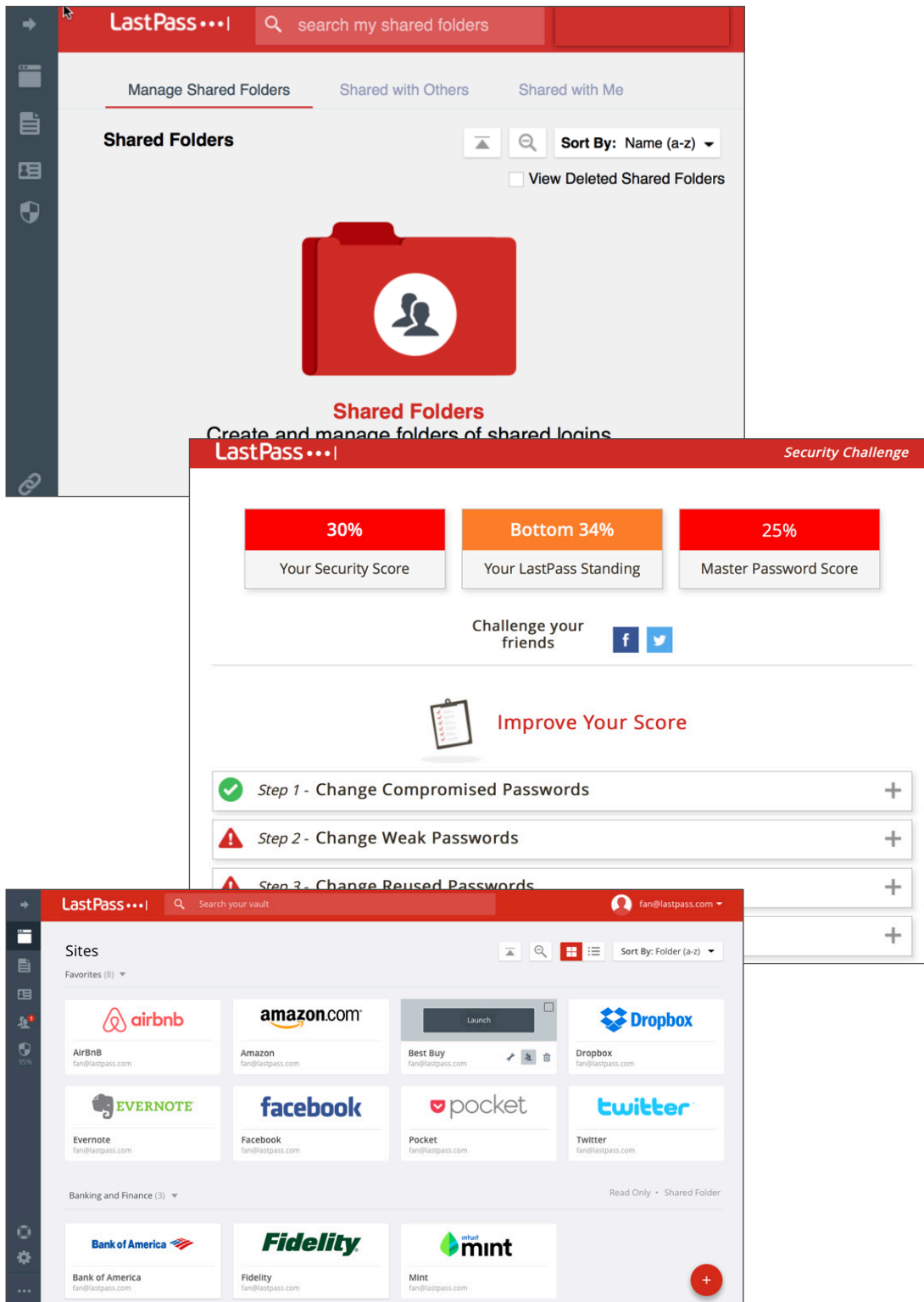
LastPass is a perfect fit for **people who just wish to keep their passwords safe** without any headache. It has multiple advanced features that will please most power users, even if you're only working with the free version.

LastPass also has the largest mobile support of all password managers, with apps on Android, iOS, Windows Phone and Blackberry. Between the outstanding browser integration and the great mobile apps, **LastPass helps to bring harmony between the user and an easy to manage password management.**



LastPass is free if you're only using it on your computer, but the extra features and mobile apps do cost **\$12/year**.

If you wish to use it for your company the price ranges from **\$18 to \$24/user/year**, they also do offer site licencing.



GET MORE INFORMATION ON LASTPASS AT
<https://www.lastpass.com/>



KeePass

KEEPASS IS INCREDIBLY POWERFUL AND WELL SUPPORTED. IT IS A FREE OPEN SOURCE PASSWORD MANAGER, WHICH HELPS YOU TO MANAGE YOUR PASSWORDS IN A SECURE WAY.

WHAT WE LOVE

OPEN SOURCE: KeePass gives you full access to its source code. You can easily have a look at its source code and compile it yourself, thus making it easy to verify if the security is properly implemented and, if you wish, use any other encryption algorithm.

PORTABILITY: You can carry your KeePass on a USB stick since it doesn't require any installation on your system. It will even run on Windows systems without being installed.

MOBILE APPS: The KeePass team doesn't officially support any mobile apps, but developers have taken the open source code and adapted it for various platforms like iOS, Android and Blackberry, only to mention a few of them.

PLUG-IN ARCHITECTURE: One of the strengths of KeePass is the support for multiple plugins since other people can write plugins for KeePass. If you are a DIY'er you can easily extend the functionality of KeePass, providing additional import/export methods for other file format.

WHERE IT NEEDS IMPROVEMENT

HANDS-ON MANAGING: Since there is no official mobile apps there will be some work to do, there is no one easy click setup or installation wizard with the KeePass system.

MISSING FEATURES: KeePass doesn't support the security alerts and automatic password changing features of some of the other Password Managers.

WHO IT'S FOR

KeePass is the best password manager for the **DIYer willing to put in the time to set it up** and trade the convenience of cloud-based systems like LastPass for total control and customization of their password system. It is perfect for anyone who doesn't want to keep their data stored on a third-party server.



KeePass is **completely free**, although donations are much appreciated to help support the development of the project.

KeePass Password Safe

This is the official website of KeePass, the free, open source, light-weight and easy-to-use password manager.

Latest News

- KeePass 2.32 released** (2016-03-09 15:17, [Read More >](#))
- KeePass 1.31 released** (2016-03-02 13:46, [Read More >](#))
- KeePass 2.31 released** (2016-01-09 16:43, [Read More >](#))
- KeePass 1.30 released** (2016-01-02 16:41, [Read More >](#))

What is KeePass?
 Today you need to remember many passwords. You need a password for the Windows network logon, your e-mail account, your website's FTP password, online passwords (like website member account), etc. etc. etc. The list is endless. Also, you should use different passwords for each account. Because if you use only one password everywhere and someone gets this password you have a problem... A serious problem. The thief would have access to your e-mail account, website, etc. Unimaginable.

Edit Entry
 You're editing an existing entry.

Entry | Advanced | Properties | Auto-Type | History

Title: Icon:

User name:

Password:

Repeat:

Quality: 6 ch.

URL:

Notes:

Expires: 2016-04-14 00:00:00

Tools

KeePassDatabase.kdbx - KeePass

File Edit View Tools Help

Search...

Title	User Name	Password	URL	Notes
dev\admin_nc_aan	dev\admin_nc_aan	*****		
dev\admin_nc_bbm	dev\admin_nc_bbm	*****		
dev\admin_nc_ccv	dev\admin_nc_ccv	*****		
dev\admin_nc_vvb	dev\admin_nc_v...	*****		
Devolutions-HV	test	*****		
Devolutions-HV2	test	*****		
prod\admin_nc_hht	prod\admin_nc_hht	*****		
TST-SBS-Win7-1	test	*****		
TST-SBS-Win7-2	patatte	*****		
windjammer\david	windjammer\david	*****		

Group: [folder1](#), Title: dev\admin_nc_aan, User Name: dev\admin_nc_aan, Password: *****, Creation Time: 2015-09-21 10:55:55, Last Modification Time: 2015-09-21 10:56:28

1 of 10 selected | Ready.

GET MORE INFORMATION ON KEEPASS AT
<http://keepass.info/>



**1PASSWORD IS THE BEST-LOOKING SOFTWARE OF THEM ALL.
IT HAS A WINDOWS APP AS WELL AS IOS AND ANDROID.**

WHAT WE LOVE

INTEGRATED BROWSER EXTENSIONS: You will need the 1Password desktop app installed, but you can easily integrate it into your browser with different extensions. You can smoothly sync your account across multiple devices.

ADVANCED ENCRYPTION: 1Password will keep your data safe with a strong AES-256 encryption, which protects your sensitive information at all times.

PASSWORD AUDITS: 1Password performs an audit of your existing passwords highlighting weak or duplicate passwords, and then helps you create more secure ones.

1PASSWORD WATCHTOWER: 1Password will send you around-the-clock security alerts for the services and sites that you use.

WHERE IT NEEDS IMPROVEMENT

OPERATING SYSTEMS: If you are not using Windows, Mac, iOS or Android, you will be disappointed by their lack of support for the other operating systems.

TWO-FACTOR AUTHENTICATION: 1Password does not support the two-factor authentication method, which might be seen as a drawback for some users, however 1Password does offer another option - the [Account Key](#).

WHO IT'S FOR

1Password is surely the **best-looking password manager** out there with a polished browser integration. They are constantly releasing updates and new features, which is always a plus.

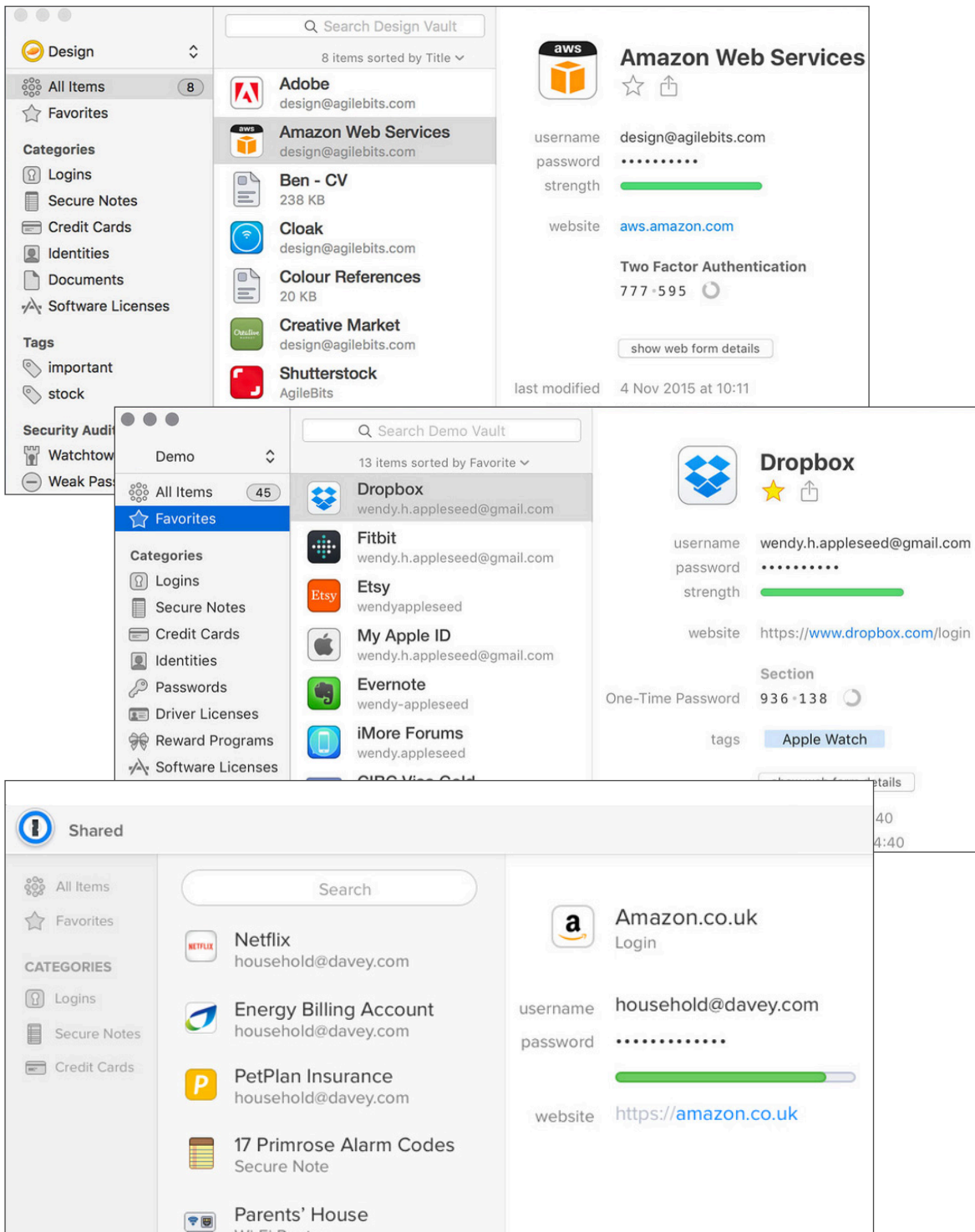


1Password offers the 1Password Family package which is a subscription that includes all the apps, free upgrades, web access and sharing for up to 5 people in the same household for **\$5 per month**.

The desktop app single license, meaning having the Mac and Windows licenses,

will set you back **\$69.99 one-time purchased**. The **iOS app is a \$9.99** premium upgrade and the **Android app is a \$7.99** premium upgrade.

All that said, there is no subscription model for 1Password. So while a desktop and mobile license will set you back around \$80, it would still be cheaper than a LastPass or Dashlane license over time.



GET MORE INFORMATION ON 1PASSWORD AT
<https://1password.com/>



PASSWORD VAULT MANAGER LETS YOU AND YOUR TEAM CENTRALIZE YOUR ORGANIZATION'S PASSWORDS AND CREDENTIALS INTO ONE SECURE REPOSITORY. THE APPLICATION IS ACTUALLY INTEGRATED IN THE REMOTE DESKTOP MANAGER SOFTWARE.

WHAT WE LOVE

WINDOWS AND MAC APPS, WITH INTEGRATED BROWSER EXTENSIONS: You will need the Password Vault Manager installed. However, you can easily integrate it into your browser with different extensions. You can use Password Vault Manager locally only, or sync to the web if you wish to use it across multiple devices.

MOBILE APPS: Password Vault Manager has free apps available on iOS and Android. You can download and use these apps for free, but you will still need the desktop version to have full access to all features.

PASSWORD ANALYZER: Password Vault Manager will take a look at all your existing passwords, then audit them for duplicates, weak passwords and expired passwords, allowing you to improve security on a company-wide level. Automatic generated secure passwords allow you to create stronger passwords that you can then access using a master password.

EASY SHARING OF DATA ENTRIES BETWEEN MULTIPLE USERS: By using SQL Server, Devolutions Online Database or Devolutions Server data source, the application operates efficiently and securely in a multi-user environment. Plus, with the user-specific settings, each user can (if desired) apply his credentials to override the default configuration.

WHERE IT NEEDS IMPROVEMENT

USER INTERFACE: Password Vault Manager's user interface might be confusing or heavy for some users, and it could take some time getting used to.

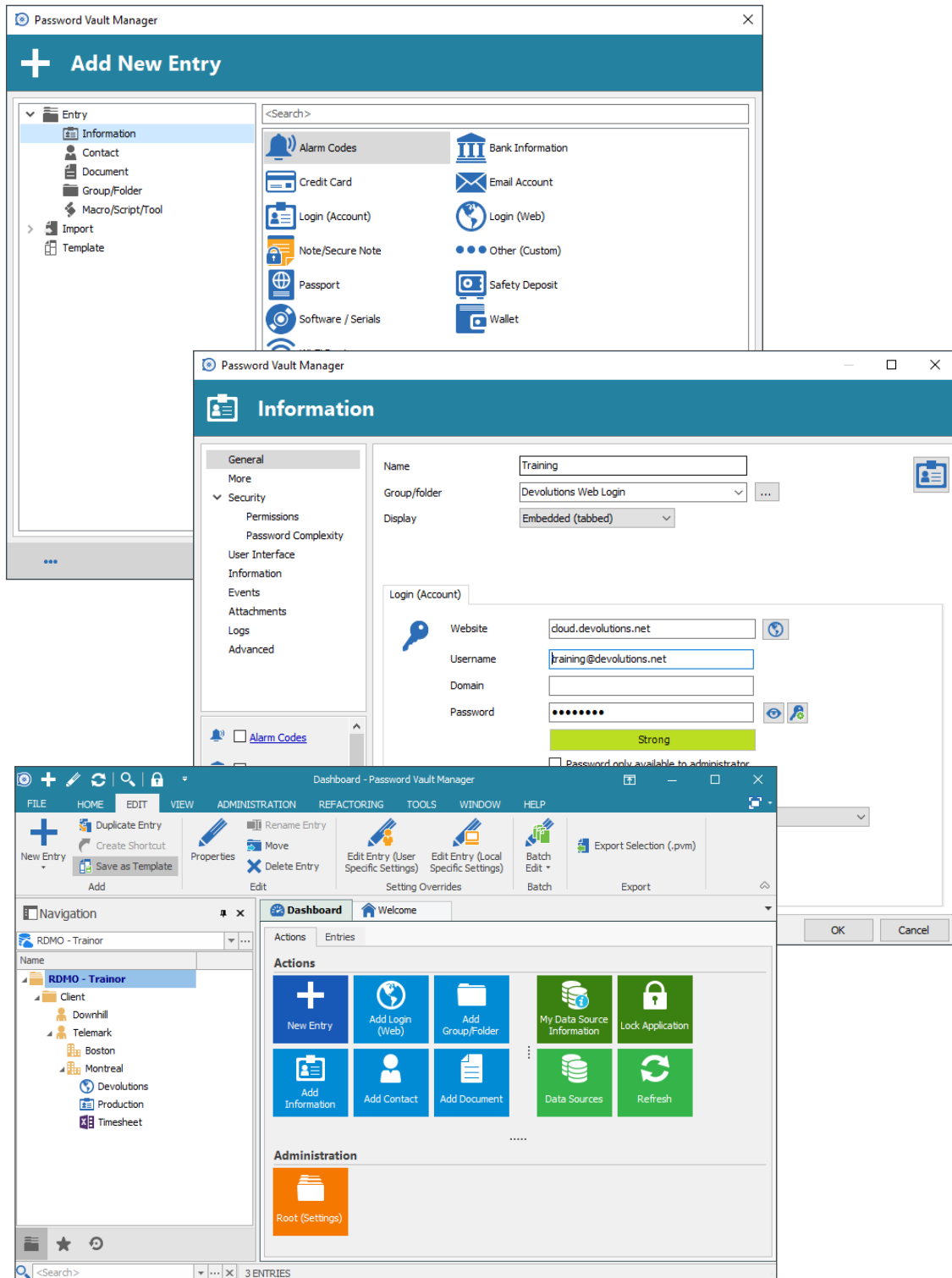
TOO MANY OPTIONS: Password Vault Manager seems to be trying to do too many things at once; so finding ways to share password could be time consuming.

WHO IT'S FOR

Password Vault Manager might be more suitable for **power users or companies** than for personal use as it has exhaustive advanced options, and it may take some time to get comfortable navigating through this application.



Password Vault Manager has a Free Edition with limited access. If you wish to have an Enterprise single license, it will set you back **\$59.99**, but you will be able to use your license on Windows and Mac. The PVM license is perpetual, although if you wish to use the maintenance plan, it will set you back another **\$29.99 per year**. If you are using Remote Desktop Manager, then you will never have to actually buy a Password Vault Manager license, as it is included in the Remote Desktop Manager application.



GET MORE INFORMATION ON PASSWORD VAULT MANAGER AT

<https://password.devolutions.net/>



DASHLANE IS A BEAUTIFULLY DESIGNED AND VERY HELPFUL PASSWORD MANAGER THAT IS AVAILABLE ON MULTIPLE DEVICES.

WHAT WE LOVE

AUTOMATIC LOGIN: Dashlane will proceed with the automatic login of all your accounts. Even on complex logins with two steps or three fields, like bank accounts. No clicks or keystrokes are required.

SECURITY DASHBOARD: Dashlane easily identify dangerously weak or reused passwords that are stored in your password vault, and quickly see what accounts hackers may have compromised with a handy security score screen. Dashlane will alert you if a security breach is recorded.

EMERGENCY CONTACT: Dashlane allows you to set an emergency contact for your important accounts in case of an urgent and critical matter. This can be utilized at work or for a personal account. Set your emergency contact to one of your coworkers or loved ones so they can temporarily access your account.

GREAT INTERFACE: Dashlane has a very sleek and nice interface that is far more polished than some of its competitors.

WHERE IT NEEDS IMPROVEMENT

COSTLY: Dashlane can be expensive if you wish to use features like syncing and web access to passwords..

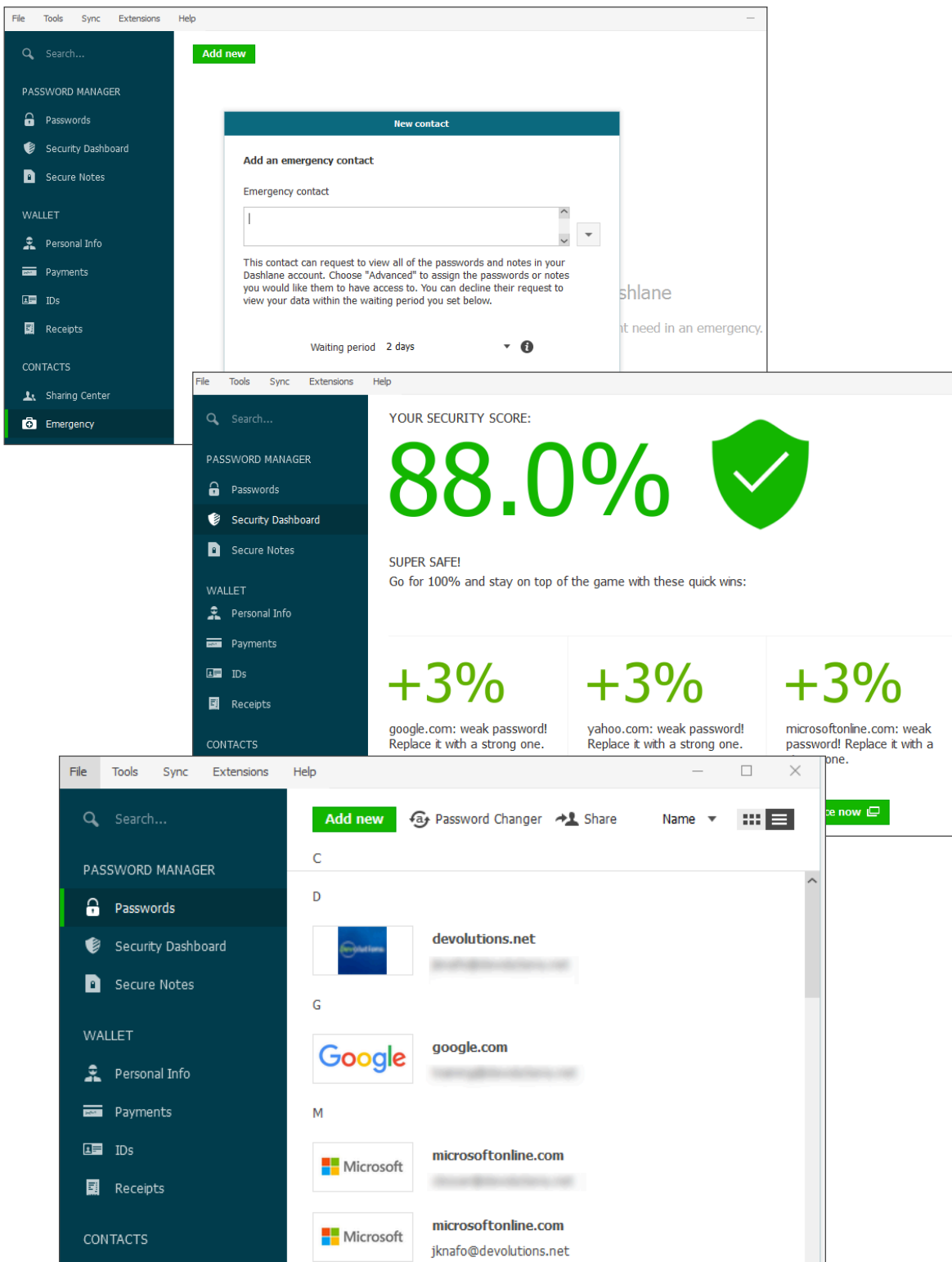
EMAIL SUPPORT: Dashlane could improve their email support, as it is not the fastest or most efficient support at the moment.

WHO IT'S FOR

Dashlane is packed with multiple features and is **incredibly easy to use**. It's beautiful and simple interface is perfect for anyone who isn't too computer-friendly.



Dashlane Free works on one device, Mac or PC. You can share up to 5 logins with other users, although you have no access to your Dashlane passwords online. Dashlane Premium costs **\$39.99/year** and allows unlimited login shares with other users. It works on multiple devices so they will continuously be syncing.



GET MORE INFORMATION ON DASHLANE AT
<https://www.dashlane.com/en/lp/neverforget-teal>



PASSWORDSTATE IS A WEB-BASED SOLUTION FOR SECURE PASSWORDS MANAGEMENT, FOR BOTH INDIVIDUALS AND TEAMS.

WHAT WE LOVE

APPLICATION PROGRAMMING INTERFACE (API):

Passwordstate combines the API into your own applications, putting an end to hard-coded passwords. You may write your own scripts or code to retrieve, update and add passwords to the system, and maintain standard auditing and real-time notifications through-out the process.

MOBILE CLIENT SUPPORT: Passwordstate mobile client supports iOS, Android, Windows 8 Phone and Blackberry mobile platforms.

ROLE-BASED ACCESS CONTROL: Passwordstate is built on the concept of role-based access. This incorporates access to password information, administering the Passwordstate application.

REAL-TIME NOTIFICATIONS: Passwordstate has 54 different built-in email notifications. These can be customized or disabled by the Security Administrators of Passwordstate, and each user can specify which email notifications they would like to receive.

WHERE IT NEEDS IMPROVEMENT

NO CLOUD BASED SOLUTION: Some companies would rather work with a Cloud based solution and at the moment it is not an option that Passwordstate offers.

BETTER SUPPORT FOR MANAGED SERVICE PROVIDERS (MSP'S): Passwordstate could offer a better support of MSP, allowing users to perform account discoveries and password resets on disconnected networks.

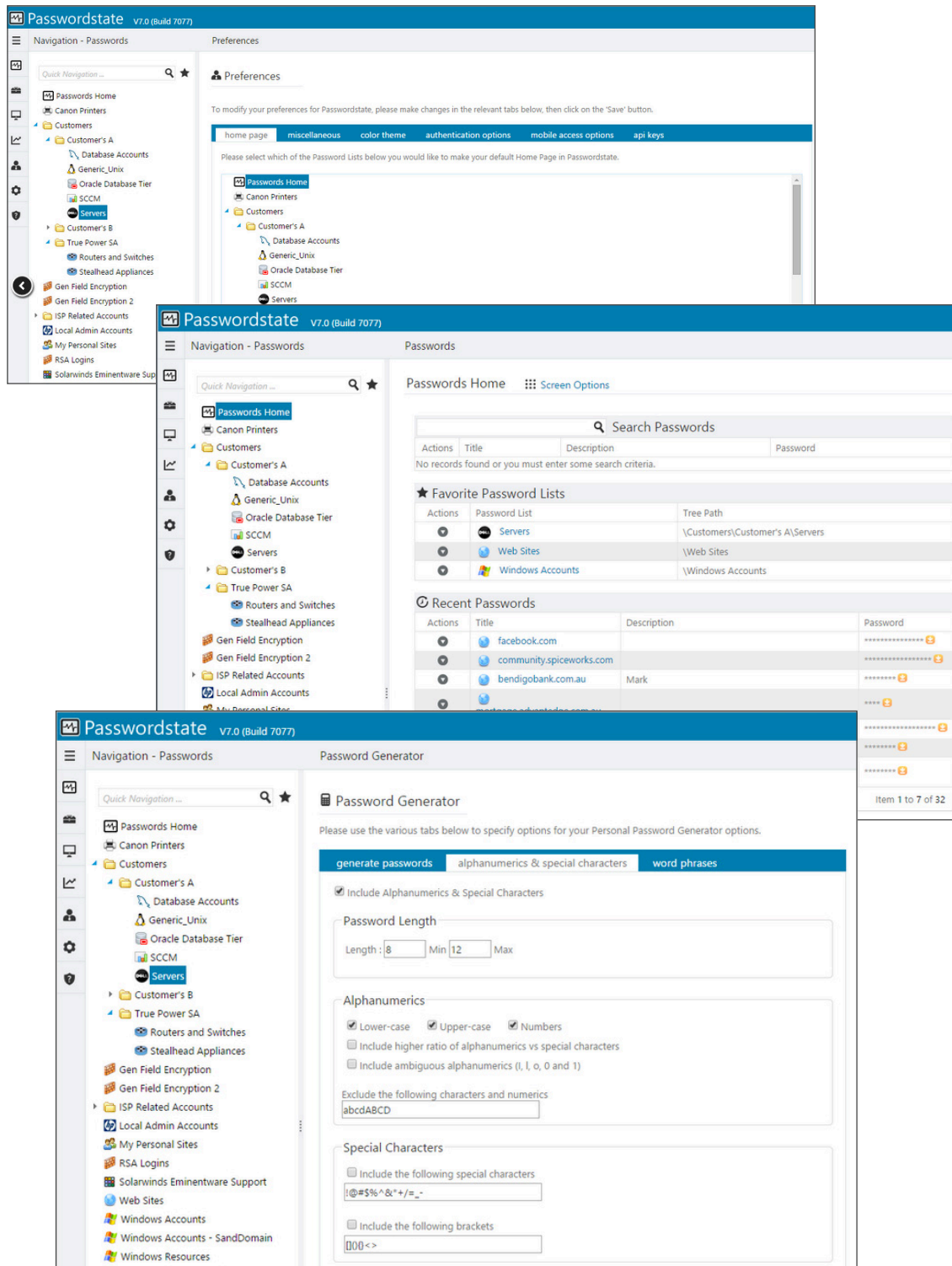
WHO IT'S FOR

Password state makes everything pretty easy to get to, and with their free license for up to 5 users, it could be a **good choice for small companies**. Their Enterprise and Global licenses would also please larger companies with all the advantages they offer.



Passwordstate is free for up to 5 users. To have full access including the additional support and upgrades, it will come up to **\$49/license/user** (the price lowers as you add more users).

The Enterprise license is **\$5,640**, and if you wish to have a Global license with all the perks, it will come up to **\$14,940**. They also offer a High Availability Module, which runs as read-only on a failsafe server for **\$1,707**.



GET MORE INFORMATION ON PASSWORDSTATE AT

<https://www.clickstudios.com.au/>



KEEPER IS ONE OF THE MOST DOWNLOADED PASSWORD MANAGER AND SECURE DIGITAL VAULT. PROTECTING AND MANAGING YOUR PASSWORDS ON SMARTPHONES, TABLETS AND COMPUTERS.

WHAT WE LOVE

KEEPER DNA: Most Password Management application supports the two-factor authentication as their security measure but Keeper exceeded our expectations. Instead of using a code sent to a device, Keeper DNA uses a person's connected object device to create a unique "**Keeper DNA Profile**". Apple Watch will be the first to support Keeper DNA but it will soon spread to other devices.

TECHNICAL SUPPORT: Keeper provides its clients with a 24/7 live chat support. Generally, password manager software supports users by email only and more between 9 to 5 then 24/7.

DIGITAL VAULT: Keeper allows users to attach photos and videos in addition to passwords. Users can take pictures of their passports or credit card and store them in their vault without having to save those pictures in their phone or camera, keeping them safe from others.

PRELOADED APPLICATION: Keeper is the only product that has been evaluated, approved and preloaded by main mobile carriers. AT&T selected Keeper as the only password manager to be preloaded on all of their Android and Windows devices.

WHERE IT NEEDS IMPROVEMENT

DESKTOP INTERFACE: Keeper is presently not up to par with their desktop interface compare to other password managers. A sleeker and friendlier user interface would definitely benefit them.

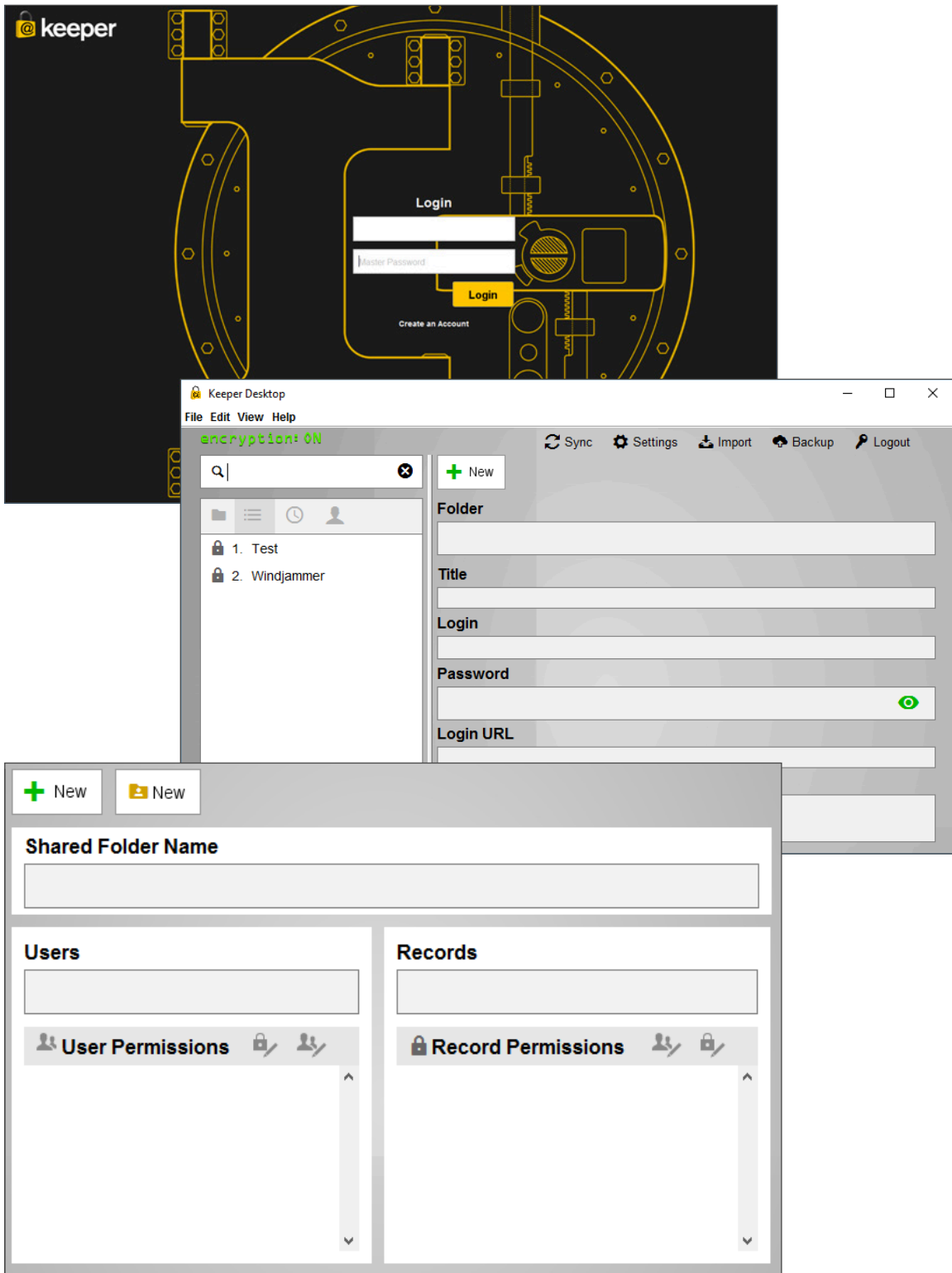
SECURITY DASHBOARD: Keeper doesn't have a Security Dashboard feature that most other password software supports. Thus, making it more complicated to evaluate the strengths and weaknesses of your passwords.

WHO IT'S FOR

Keeper is best suited for **small businesses** and for **personal use**. It's also an application that offers a better experience on the mobile app than on the desktop application.



Keeper can be downloaded for free, giving you access to their basic functionalities on one device with no backup protection. It will cost you **\$29,99** per year for unlimited devices, password storage, cloud backups, sharing and 24/7 support. Keeper also has an Enterprise Edition with multiple features.



GET MORE INFORMATION ON KEEPER AT
<https://keepersecurity.com/>



STICKY PASSWORD IS A GREAT AND EASY WAY TO SECURELY MANAGE ALL YOUR PASSWORDS, MAKING IT EASY TO STORE THEM FOR MULTIPLE SITES.

WHAT WE LOVE

NO-CLOUD WI-FI SYNC AVAILABLE: Sticky Password allows the user to select their sync method between: synchronization through their cloud servers, local Wi-Fi or sync manually. The Wi-Fi sync mode allows you to sync your devices directly with each other when they're on the same Wi-Fi network. The big advantage is that your data will never be on the cloud, thus making it even more secure as it never actually has to leave your device.

PORTABILITY: The portable feature allows you to carry all of your passwords on a USB stick everywhere you go. The USB-based tool can be used to log in to all your saved web sites.

BIOMETRIC AUTHENTICATION: Biometric authentication via fingerprint allows you to use fingerprint authentication on iOS and Android devices. The identity authentication for the account owner is made as easy as just a swipe of a finger!

SAVE THE MANATEES: Sticky Password is one of the only password managers with a good cause at heart! Not many software out there donates toward saving an endangered species and this kind-hearted gesture doesn't go unnoticed. A portion of the profits from the sale of each Sticky Password Premium license goes to a fund devoted to protecting endangered manatees.

WHERE IT NEEDS IMPROVEMENT

TWO-FACTOR AUTHENTICATION: Sticky Password doesn't support the standard two-factor authentication like Google Authenticator, Yubikey or Duo. At the moment the USB/Bluetooth authentication substitutes the master password, thus it is not really a two-factor authentication.

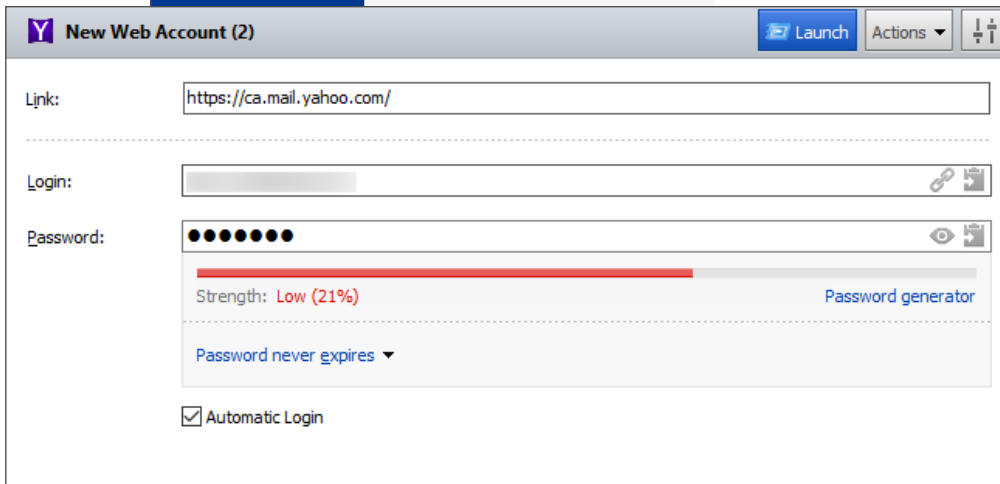
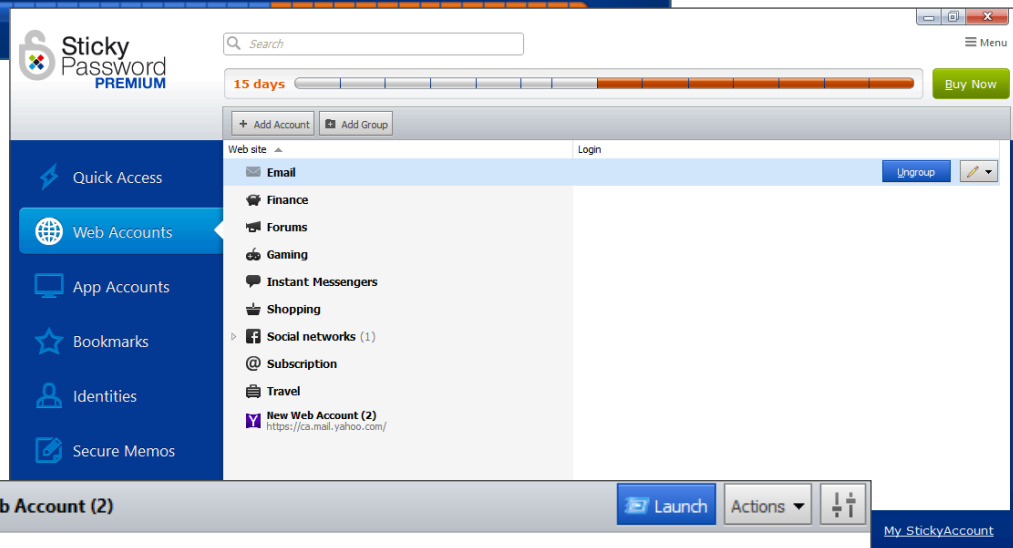
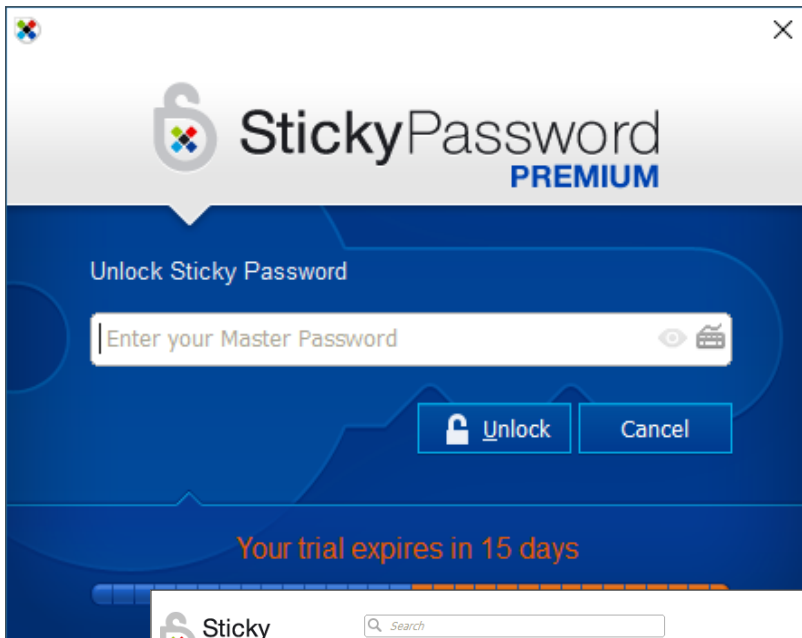
REPORT LISTS: The password strength report only indicates your weakest password. Sticky Password could benefit from a security audit feature including weak and duplicates password plus the help to automatically create new, more secure one.

WHO IT'S FOR

With its biometric authentication and easy portability, Sticky Password is perfect for **personal use** and for **smaller companies**. The lack of a two-factor authentication feature makes it hard to recommend it for larger enterprise.











Sticky Password can be downloaded for free to use their basic functionality, it will not include the cross-device syncing. The Premium edition can be installed for **\$29,99** per year or for a one-time payment of **\$149,99** for a lifetime license.



GET MORE INFORMATION ON STICKY PASSWORD AT
<https://www.stickypassword.com/>

HERE IS A TABLE FOR A QUICK OVERVIEW OF SOME ADVANCED OPTIONS SUPPORTED BY THE DIFFERENT PASSWORD MANAGER APPLICATIONS.

	 Lastpass	 KeePass	 1Password	 PVM	 Dashlane	 Passwordstate	 Keeper	 Sticky Password
Offline Mode	X	X	X	X	X	X	X	X
Two-Factor Authentication	X	X	-	X	X	X	X	-
Browser Integration	X	X	X	X	X	X	X	X
Password Capture	X	-	X	X	X	X	X	X
Password Changes	X	-	-	-	X	X	-	-
Security Alert	X	-	X	-	X	-	-	-
Portable Application	X	X	-	-	X	-	-	X
Mobile Application	X	-	X	X	X	X	X	X
Security Audits	X	-	X	X	X	X	X	-
Import	X	X	X	X	X	X	X	X
Export	X	X	X	X	X	X	X	X
Throwaway Passwords	X	-	X	-	X	X	-	-
Password Sharing	X	X	X	X	X	X	X	-
Integrated Database	X	-	X	X	X	X	X	X

A little side note, [Remote Desktop Manager](#) actually integrates all of the above-mentioned password manager solutions for the exception of Keeper and Sticky Password.

After taking your time in choosing and doing some careful comparison-shopping, all there is left to do, is to pick out the right password manager for you! In the end, what is important once you have chosen one is to stick with that one only as it is the best way to ensure that you are always selecting long, strong, and unique passwords to keep all your data safe.

Have fun shopping!