



[UPDATED] 2019 Most Popular Password Managers Compared

Updated January 10, 2019: We have added Devolutions Password Server!

Please look below for the added Password Managers review and also take a look at our updated comparison table.

Devolutions

LAST PAST vs KEEPASS vs 1PASSWORD VS DASHLANE vs PASSWORDSTATE vs KEEPER vs STICKY PASSWORD vs DEVOLUTIONS PASSWORD SERVER vs ROBOFORM

LastPass vs KeePass vs 1Password vs Dashlane vs Passwordstate vs Keeper vs Sticky Password vs Devolutions Password Manager

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 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 we look for in a great password manager are security assessments, random-character generation, and automatic login on your favorite websites.

Now let's start doing some digging and take a closer look at 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 most popular ones according to our RDMers: LastPass, KeePass, 1Password, Dashlane, Passwordstate, Keeper, Sticky Password and Devolutions Password Manager.

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, LastPass might be the perfect fit for you. It is available on Android and iOS, but you can also use 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 click of the mouse.

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, and then enabling you to make changes to enhance them.



LastPass offers a free version that includes all basic features. To have full access, including advanced features such as Emergency Access and One-to-Many sharing, it will cost \$2.61/month for 1 user and \$5.22/month for 6 users.

The Team license is \$3.16/user/month, while an Enterprise license starts at \$5.22/user/month.

WHERE IT NEEDS IMPROVEMENT

CUSTOMER SUPPORT: LastPass could easily improve their customer support by offering live chat or phone support.

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 notifies users if a breach occurs. By enabling two-factor authentication, you will be even more protected from any intrusions.

WHO IT'S FOR


LastPass is a perfect fit for **people who simply wish to keep their passwords safe** without any headaches. 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 create harmony between the user and an easy-to-manage password management.**

LastPass... | search my shared folders

Manage Shared Folders | Shared with Others | Shared with Me

Shared Folders Sort By: Name (a-z) View Deleted Shared Folders





Shared Folders
Create and manage folders of shared logins and notes.


LastPass... | Security Challenge

30% Your Security Score

Bottom 34% Your LastPass Standing

25% Master Password Score

Challenge your friends  









 **Improve Your Score**

- Step 1 - Change Compromised Passwords +
- Step 2 - Change Weak Passwords +
- Step 3 - Change Reused Passwords +
- Step 4 - Change Old Passwords +




LastPass... | Search your vault | fan@lastpass.com

Sites Sort By: Folder (a-z)

Favorites (8)

 AirBnB fan@lastpass.com	 Amazon fan@lastpass.com	 Best Buy fan@lastpass.com	 Dropbox fan@lastpass.com
 Evernote fan@lastpass.com	 Facebook fan@lastpass.com	 Pocket fan@lastpass.com	 Twitter fan@lastpass.com

Banking and Finance (3) Read Only · Shared Folder

 Bank of America fan@lastpass.com	 Fidelity fan@lastpass.com	 Mint fan@lastpass.com
--	---	--



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 look at its source code and compile it yourself, which makes it easy to ensure the security is properly implemented. You could also use any other encryption algorithm if you wish.

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, to name a few.

PLUG-IN ARCHITECTURE: One of the strengths of KeePass is how it supports multiple plugins, since other people can write plugins for KeePass. If you are a DIYer, you can easily extend the functionality of KeePass, providing additional import/export methods for other file formats.

WHERE IT NEEDS IMPROVEMENT

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

OUTDATED INTERFACE: KeePass's interface looks like it hasn't been updated since the last century; it's not appealing and has an old-fashioned feel to it.

WHO IT'S FOR

KeePass is the best password manager for the **DIYer willing to put in the time to set it up**, trading 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 and who is tech-savvy, but perhaps **not a great choice for the average user**.



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.

Home

- Home & News
- Forums
- Feature List
- Screenshots

Getting KeePass

- Downloads
- Translations
- Plugins / Ext.

Information / WWW

- Help
- FAQ
- Security
- Awards
- Links

Support KeePass

- Donate

Latest News

KeePass 2.40 released
2018-09-10 16:37. [Read More >](#)

KeePass 1.36 released
2018-09-03 14:05. [Read More >](#)

KeePass 2.39 (2.39.1) released
2018-05-06 11:43. [Read More >](#)

KeePass 2.38 released
2018-01-09 17:54. [Read More >](#)

[\[News Archive\]](#)

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. 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.

KeePass is a free open source password manager, which helps you to manage your passwords in a secure way. You can put all your passwords in one database, which is locked with one master key or a key file. So you only have to remember one single master password or select the key file to unlock the whole database. The databases are encrypted using the best and most secure encryption algorithms currently known (AES and Twofish). For more information, see the [features page](#).

Is it really free?
Yes, KeePass is really free, and more than that: it is open source (OSI certified). You can have a look at its full source and check whether the encryption algorithms are implemented correctly.

As a cryptography and computer security expert, I have never understood the current fuss about the open source software movement. In the cryptography world, we consider open source necessary for good security; we have for decades. Public security is always more secure than proprietary security. It's true for cryptographic algorithms, security protocols, and security source code. For us, open source isn't just a business model; it's smart engineering practice.
Bruce Schneier, Crypto-Gram 1999-09-15

Edit Entry

You're editing an existing entry.

Entry **Advanced** Properties Auto-Type History

Title: Icon:

User name:

Password:

Repeat:

Quality: 6 bits 6 ch.

URL:

Notes:

Expires:

KeePassDatabase.kdbx - KeePass

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



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

WHAT WE LOVE

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.

TRAVEL MODE: The travel mode allows you to temporarily remove data on your mobile device while traveling. This means that if your device is lost, stolen, or if someone at the border demands to check your mobile devices, they'll never be able to access the data – since it won't be there! Once you're back from your trip, simply restore your data with a single tap. We know this isn't a feature most people actually need, but it's a truly unique feature that only 1Password offers.

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

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

WHO IT'S FOR

1Password offers high security, a great support forum, easy day-to-day usage and a polished browser integration that makes it a great option for personal use as well as large enterprises.

WHERE IT NEEDS IMPROVEMENT

IMPORT PASSWORDS: 1Password lets you import passwords from competing password managers, but the issue is that they support the import from only a handful of password managers, whereas LastPass gives you the ability to import from more than 30 competing products.

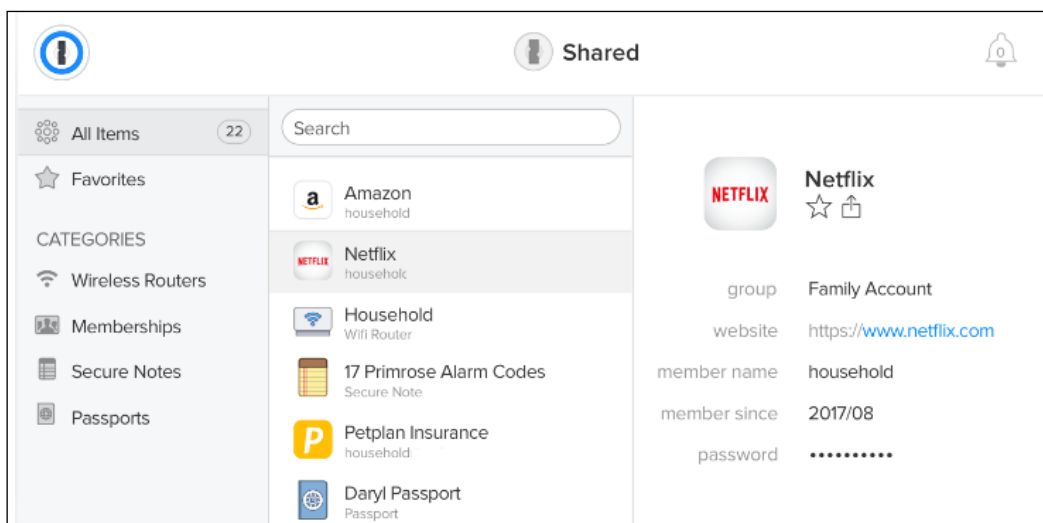
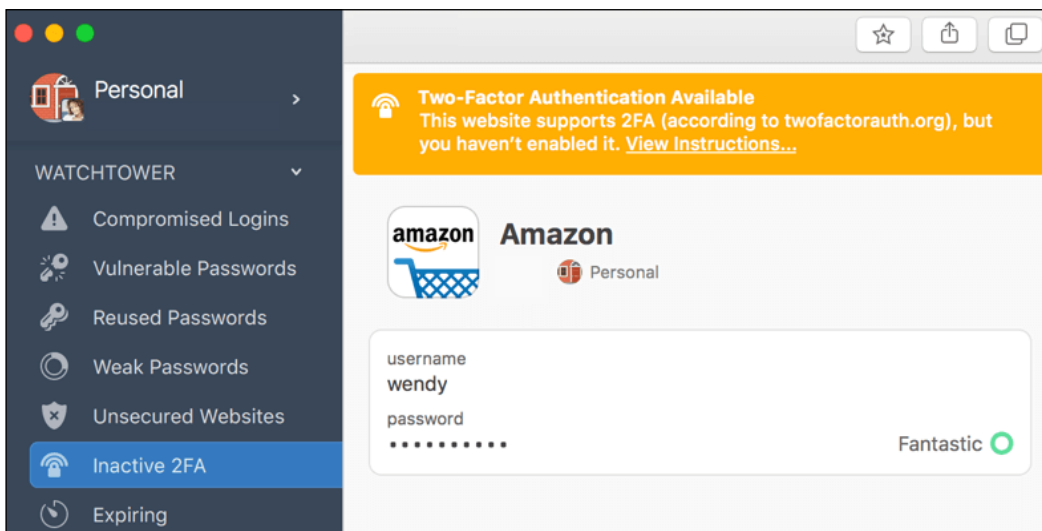
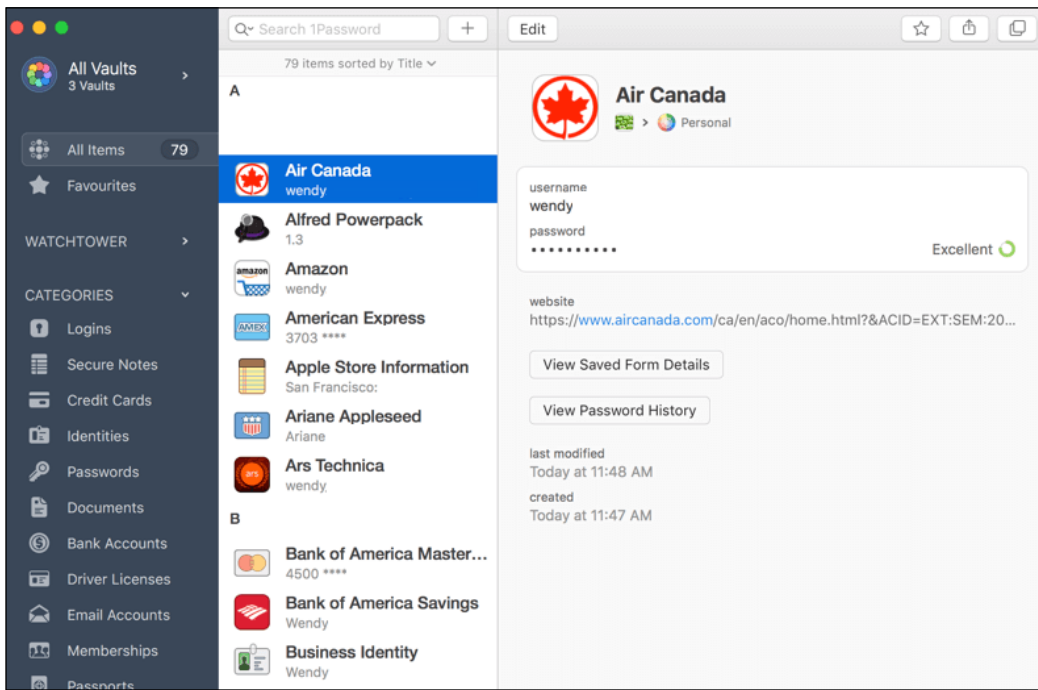
NO FREE VERSION: Most of the popular password managers include some sort of free plan for single users, even if it's restricted. The lack of a free version with 1Password is quite disappointing.



The single license will set you back **\$2.99/month**, and it includes unlimited passwords and 1GB of document storage.

1Password also 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. The Family package runs **\$4.99/month**.

For teams and businesses, 1Password offers 3 different plans: **Teams**, which includes features such as 2FA, admin control and unlimited shared vaults for **\$3.99/user/month**; and **Business**, which includes features such as activity logs and usage reports for **\$7.99/user/month**. **1Password** also offers an Enterprise plan for large enterprises.





**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. This holds true 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 it quickly sees what accounts hackers may have compromised with a handy security score screen. Dashlane will alert you if a security breach has been 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**

SYNC ACROSS DEVICES: Dashlane could get inspired by LastPass, which recently included the “sync across devices” in their free plan.

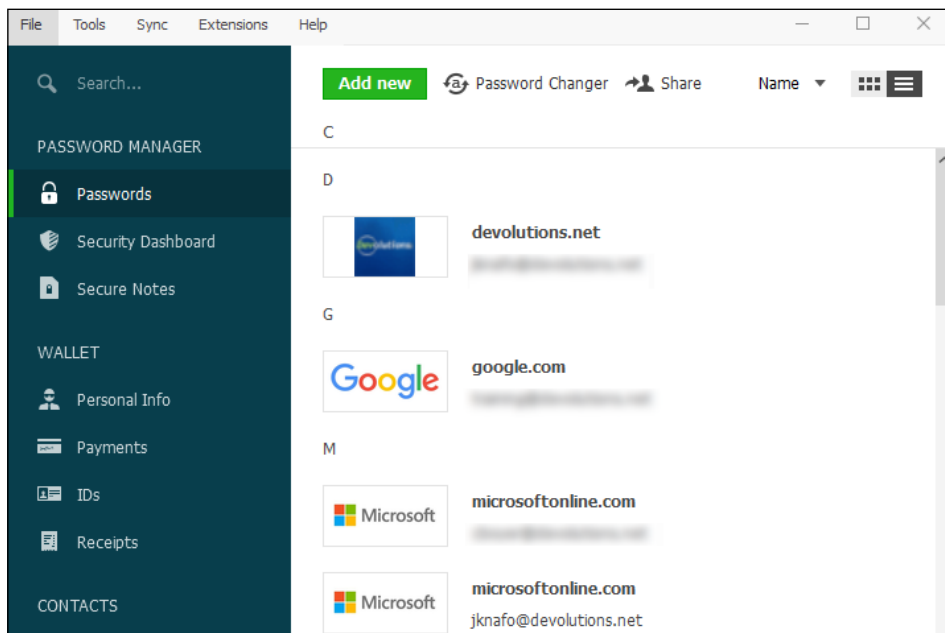
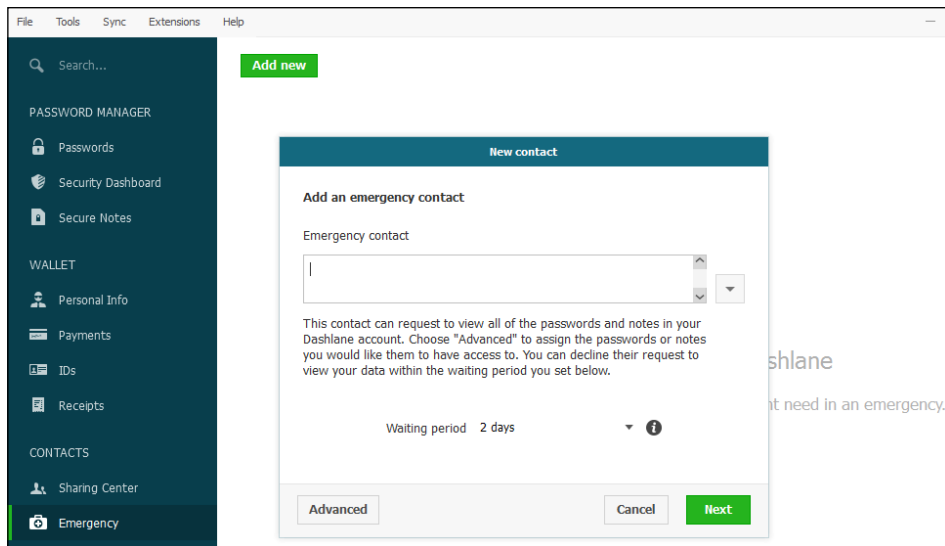
COST: Dashlane can be expensive if you wish to use features like syncing and remote account access.

 **WHO IT'S FOR**

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



Dashlane **Free works on one device**– either Mac or PC. You can share up to 5 logins with other users and store up to 50 accounts. Dashlane Premium costs **\$3.33/month** and allows unlimited passwords on unlimited devices, plus Dark Web Monitoring and secure VPN.



Passwordstate

**PASSWORDSTATE IS A WEB-BASED SOLUTION FOR SECURE PASSWORD MANAGEMENT,
AND IT IS DESIGNED 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 better support of MSP. This would allow 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 **\$45/license/user** (the price lowers as you add more users).

The **Enterprise license is \$5,170**, and if you wish to have a Global license with all the perks, it will come up to **\$13,700**. They also offer a High Availability Module, which runs as read-only on a failsafe server for **\$1,570**.

Passwordstate v8.0 (build 8058)

PASSWORDS HOSTS ADMINISTRATION

Search Password Lists or Folders ...

Tools

- Account Discovery
- Password Generator
- Password Resets in Progress
- Self Destruct Message

Customers

- Infrastructure
 - Active Directory Accounts
 - ESXi Accounts
 - Linux Accounts
 - McAfee IPS
 - Oracle Database Tier
 - Out of Band Management Cards
 - RSA Logins
 - SQL Server
 - Teamviewer Accounts
 - Windows Resources
 - Wkstn Admin Accounts
- Personal Password Lists
- Personal Websites

Password Generator

Please use the various tabs below to specify options for your Personal Password Generator options.

generate passwords | alphanumeric & special characters | word phrases

Use settings from: Windows (20-25 char.)

Number of Passwords: 15

```

BVj4NDG695^SQ@Kp0H73PgXclq
k=u^Tca/#3pzw(UxZ)@De<-n6l
PS8H<ctOX<TC=fU5ozV5nw2Hf
t@)c&lDg<v2y!^X8HoWKF)33mGRN(47w
OQp)mq98=JAG7T8^5Siv&VL+Zg0!mieR
hW/3Nz@%-5qm0f5Dl(B>kpel
U+HTL=3R0uQ>w_VX^9f8^+hbjdA%4@-5
R9!^!z2vc3L-bXnTK5d)j^E+<
rUp4zF89KR]x>0_QkagWM1LmIVNF8%vbu
1%AdilXn2(EY)v4M7^ywZTRU3_#05KjQ
Zs0]D3vgb^omF>gz[dH(AIW=
O)HkMq5[E[ASNQh+iY)^lkg
<yLl+IMSWTSDm5-j54_QqwB03JK>G2
XYVPBw1]T5xkNjF-cj2hZi<G
Pj6!+_MZ%G(bQ#*lq5DC=7n3<a)3
  
```

Passwordstate v8.0 build 8058

PASSWORDS HOSTS ADMINISTRATION

Search Password Lists or Folders ...

Tools

- Account Discovery
- Password Generator
- Password Resets in Progress
- Self Destruct Message

Customers

- Infrastructure
 - Active Directory Accounts
 - ESXi Accounts
 - Linux Accounts
 - McAfee IPS
 - Oracle Database Tier
 - Out of Band Management Cards
 - RSA Logins
 - SQL Server
 - Teamviewer Accounts
 - Windows Resources
 - Wkstn Admin Accounts
- Personal Password Lists
- Personal Websites

Passwords Home

Search Passwords

Actions	Title	Tree Path	User Name	URL	Password	Password Strength
	blankpassw	(Customer)Centos/Service Accounts			opps	★★★★★
	Band on MM	Infrastructure/Out of Band Management Cards	band			★★★★★
	McAfee NDM Web Console	Infrastructure/McAfee IP				★★★★★
	McAfee IP	Infrastructure/McAfee IP				★★★★★
	root account on server	Infrastructure/ESXi Acco	root			★★★★★

Recent Passwords

Favorite Password Lists

Password Statistics

Passwordstate v8.0 (build 8058)

PASSWORDS HOSTS ADMINISTRATION

Search Password Lists or Folders ...

Tools

- Account Discovery
- Password Generator
- Password Resets in Progress
- Self Destruct Message

Customers

- Infrastructure
 - Active Directory Accounts
 - ESXi Accounts
 - Linux Accounts
 - McAfee IPS
 - Oracle Database Tier
 - Out of Band Management Cards
 - RSA Logins
 - SQL Server
 - Teamviewer Accounts
 - Windows Resources
 - Wkstn Admin Accounts
- Personal Password Lists
- Personal Websites

Auditing Graphs

Please select the appropriate filters below, and then click on the 'Refresh' button.

Graph Filters

Platforms: All Web Mobile API Windows Service Browser Extension

Audit Activity: Site Location: Duration:



KEEPER IS ONE OF THE MOST DOWNLOADED PASSWORD MANAGERS AND SECURE DIGITAL VAULTS. IT PROTECTS AND MANAGES YOUR PASSWORDS ON SMARTPHONES, TABLETS AND COMPUTERS.

WHAT WE LOVE

KEEPER DNA: Most password management applications support 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.

BREACHWATCH: BreachWatch monitors the dark web for breached accounts then alerts you so you can take action to protect yourself against hackers.

DIGITAL VAULT: Keeper allows users to attach photos and videos in addition to passwords. Users can take pictures of their passports or credit cards and store them in their vault without having to save those pictures in their phone or camera, thereby 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 compared to other password managers. A sleeker and friendlier user interface would definitely help.

SYNC ACROSS DEVICES: Just like Dashlane, Keeper could look to LastPass and include "sync across devices" in their free plan.

WHO IT'S FOR

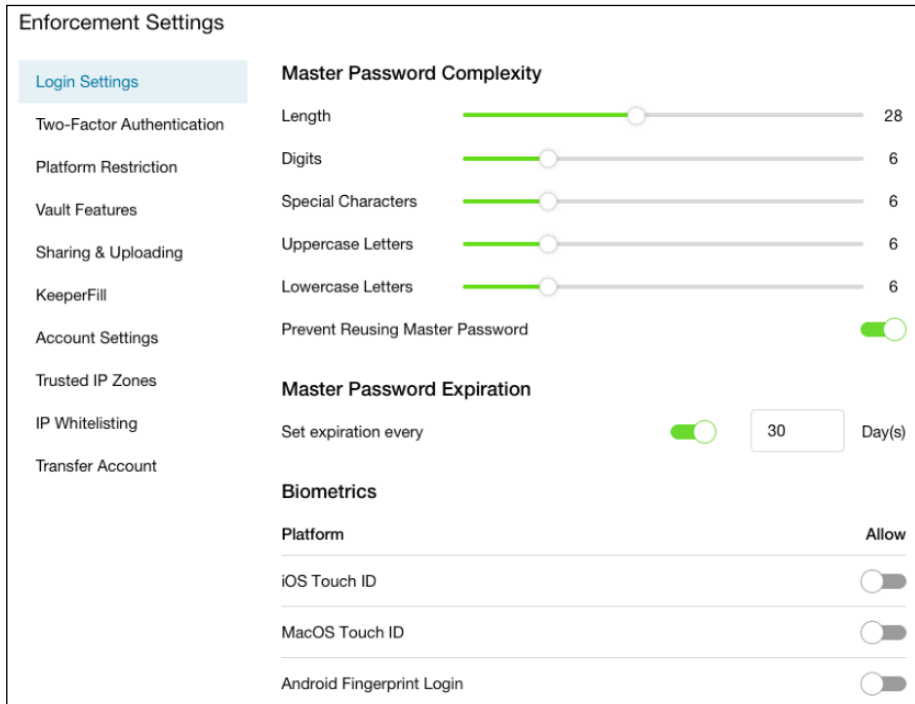
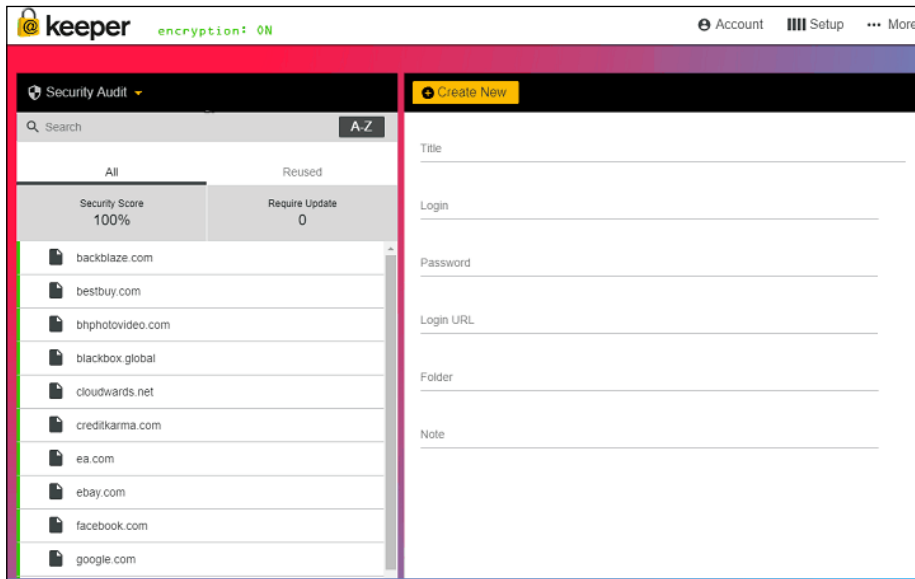
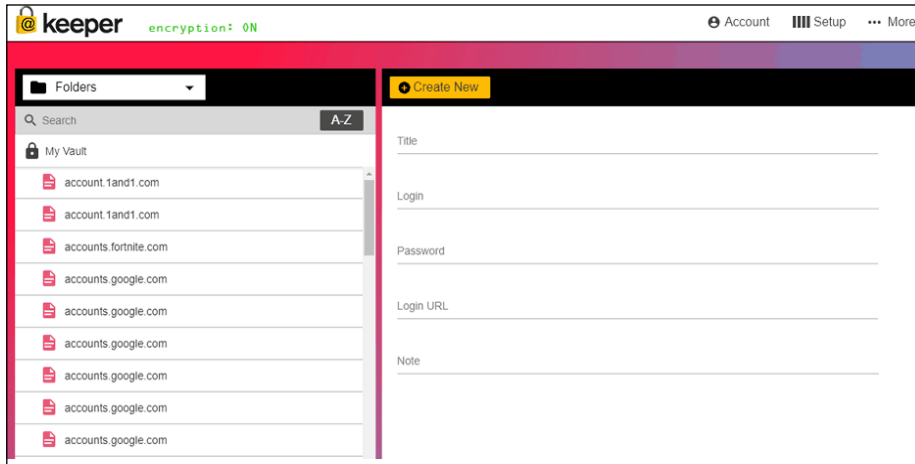
Keeper is best suited for **small businesses** and for **personal use**. It's also an application that offers a better experience on the mobile app than on the desktop application.



Keeper can be downloaded for free, giving you access to their basic functionalities on one device with no backup protection.

Keeper has different plans for individuals and for businesses. The Individual plan will cost you \$2.50/month/user, or you could go with their Family plan at \$5.00/month for up to 5 users.

For businesses, they offer two plans: the Business plan, which costs \$2.50/month/user; and, for those who need AD integration, the Enterprise plan costs \$3.75/month/user.





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 provides users with three sync method options: synchronization through their cloud servers, local Wi-Fi or manual. 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 with this method is that your data will never be on the cloud, thus making it even more secure since 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 the 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 donate 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

SECURE SHARING: Some other password manager software allow you to securely share passwords with colleagues or friends without them ever being able to see the plain text passwords. At the moment, Sticky Password doesn't offer this secure sharing feature.

REPORT LISTS: The password strength report only indicates your weakest password. Sticky Password could benefit from a security audit feature that includes weak and duplicate passwords, as well as help for users to automatically create new, more secure ones.

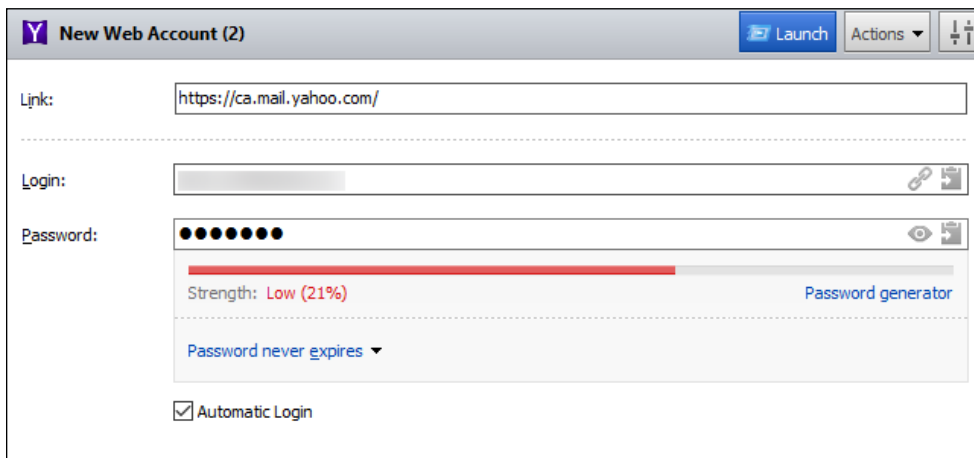
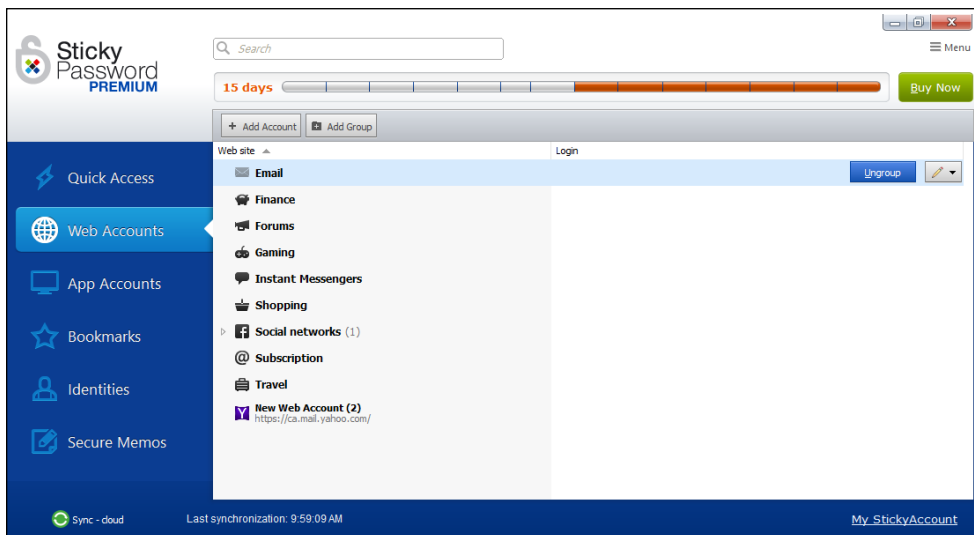
WHO IT'S FOR

With its biometric authentication and easy portability, Sticky Password is perfect for **personal use** and for **smaller companies**.



Sticky Password is free to use for their basic functionality, as this will not include the cross-device syncing.

The Premium edition can be installed for **\$29.99** per year. A Lifetime license is also available at a one-time rate of **\$119.99**.



DEVOLUTIONS PASSWORD SERVER OFFERS A HIGHLY-SECURED VAULT THAT FEATURES ENTERPRISE-GRADE PASSWORD MANAGEMENT FOR ALL YOUR BUSINESS USERS.

WHAT WE LOVE

ROLE-BASED ACCESS CONTROL: Devolutions Password Server is built on the concept of a role-based security system which allows for the creation of a granular protection system, providing the flexibility to manage more permissions.

REAL-TIME NOTIFICATIONS: If a user accesses or modifies a password that is shared with the entire team, you will immediately get notified by email from the Devolutions Password Server notification engine.

DETAILED REPORTS: Create custom, printable usage reports to see which passwords were accessed, who accessed them, and when.

DEVOLUTIONS WEB LOGIN: The Devolutions Web Login browser extension, which is available for Chrome, Firefox, IE, Edge and Opera, can automatically capture passwords and credentials from any websites. It can then directly inject the credentials into the websites with just one click for easy automatic web login.



Devolutions Password Server offers three different subscription plans: the **Team Edition**, which supports up to 15 users for **\$499.99/year**; the **Enterprise Edition**, which supports up to 50 users for **\$1,999**.

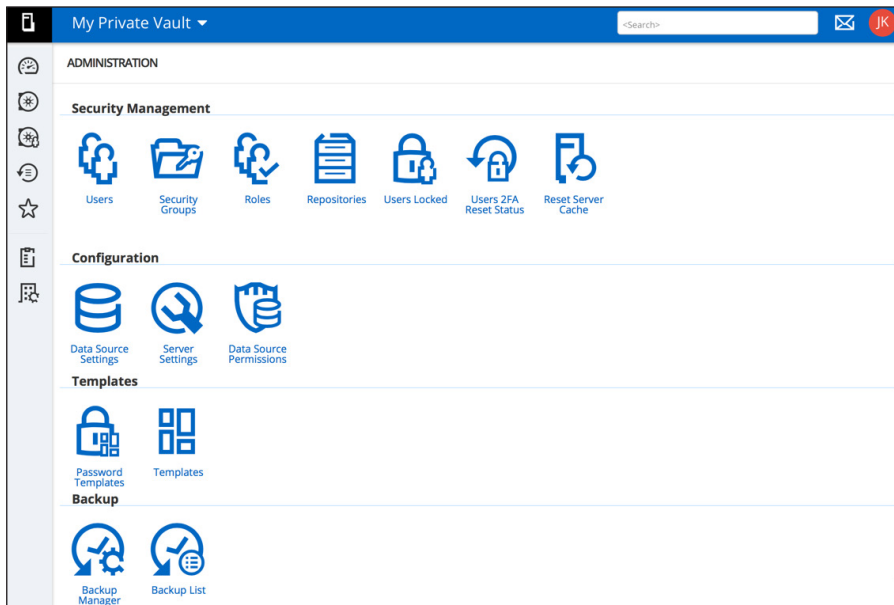
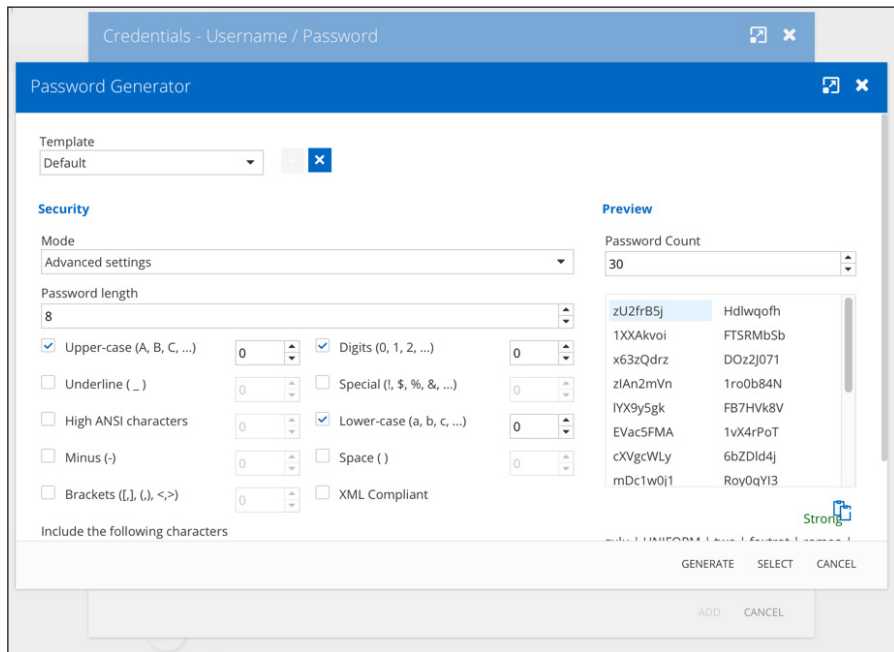
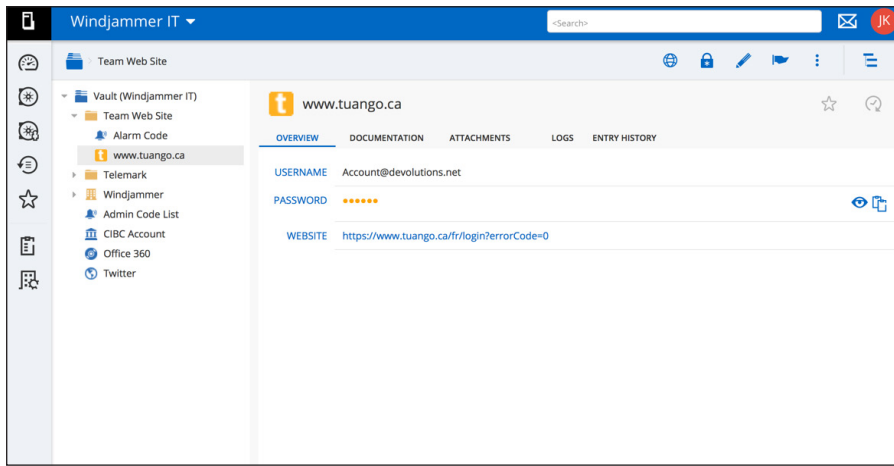
WHERE IT NEEDS IMPROVEMENT

2FA IN TEAM EDITION: Devolutions Password Server provides multiple two-factor authentication options, but 2FA isn't supported when buying a Team Edition. To have the extra layer of protection you'll need the Enterprise or the Platinum Edition.

CLIPBOARD BUFFER TIMEOUT: Some other password managers provide a functionality where the clipboard buffer is cleared automatically after a predefined timeout so that passwords cannot be pasted by accident. It would be a plus for Devolutions Password Server to support such a feature.

WHO IT'S FOR

With its highly-secured vault offering enterprise-grade password management and its simplified web interface, Devolutions Password Server is the **perfect solution for any organization** that wishes to ease password management for all their business users. Devolutions Password Server is designed for enterprises only; it is not designed **for single users**.





ROBOFORM IS AN INEXPENSIVE PASSWORD MANAGER THAT HAS BEEN ON THE MARKET FOR THE LAST 16 YEARS AND OFFERS A TON OF OPTIONS.

WHAT WE LOVE

SECURE SHARING OF CREDENTIALS: RoboForm allows you to share a single entry or an entire folder with another user, so long as they have RoboForm installed and you have matching RSA keys. This means you can feel free to securely share without the risk of exposing sensitive data in the process.

ROBUST FORM FILLING: RoboForm deserves a big thumbs up for their auto-fill and browser capture feature. On every application, it's always right on target when you enter your credentials, even on non-standard login forms.

HIGH LEVEL OF SECURITY: RoboForm offers a high level of security with its industry-standard AES-256 encryption for your data. Information is encrypted locally on your device and then sent to RoboForm over a TSL/SSL channel, making it almost impossible to intercept or decrypt. If that wasn't enough, your data also goes through 1,000 rounds of PBKDF2 hashing, protecting you from brute force attack. RoboForm is a zero-knowledge provider, meaning they never see what you're storing.

GREAT SUPPORT: In the past, RoboForm has been criticized for their support, but that is a thing of the past. It now offers a great help center and starter's manual for answering common questions. You can contact them by email, and they also offer callbacks. Callbacks can be requested on any support issue and a representative will get back to you quickly.

WHERE IT NEEDS IMPROVEMENT

USER-FRIENDLINESS: RoboForm offers too many options that don't pertain to the vast majority of users. It also might just have too much power. Power is usually a plus, but as the saying goes: too much is like not enough. In this case, it makes the experience geek friendly, but no very user-friendly.

WEB ACCESS AND CLOUD BACKUP ARE PREMIUM FEATURES: It would be nice to have such features as web access, cloud backup and sync between multiple devices included in the free version.

WHO IT'S FOR

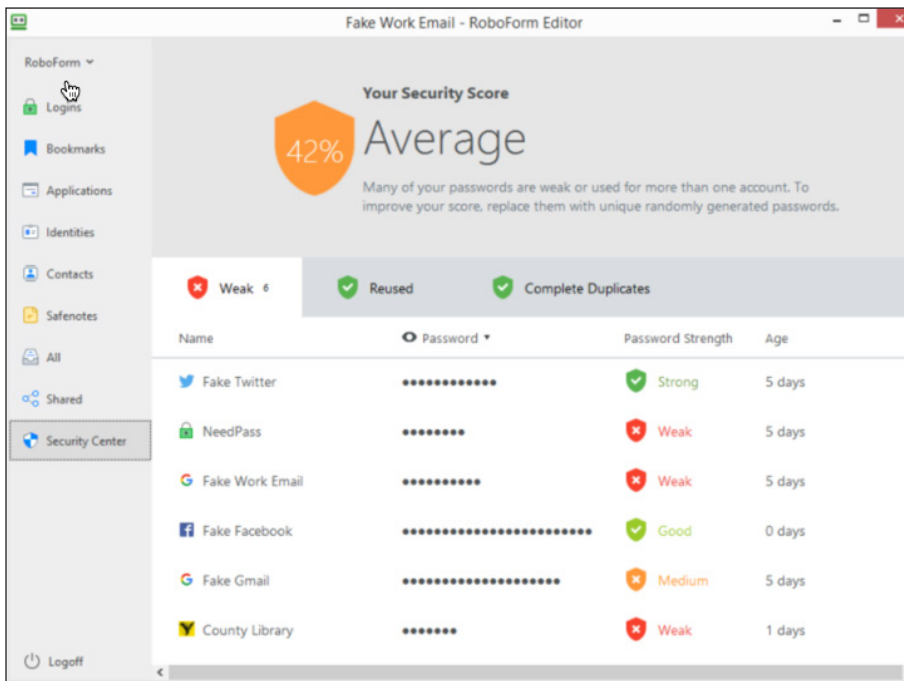
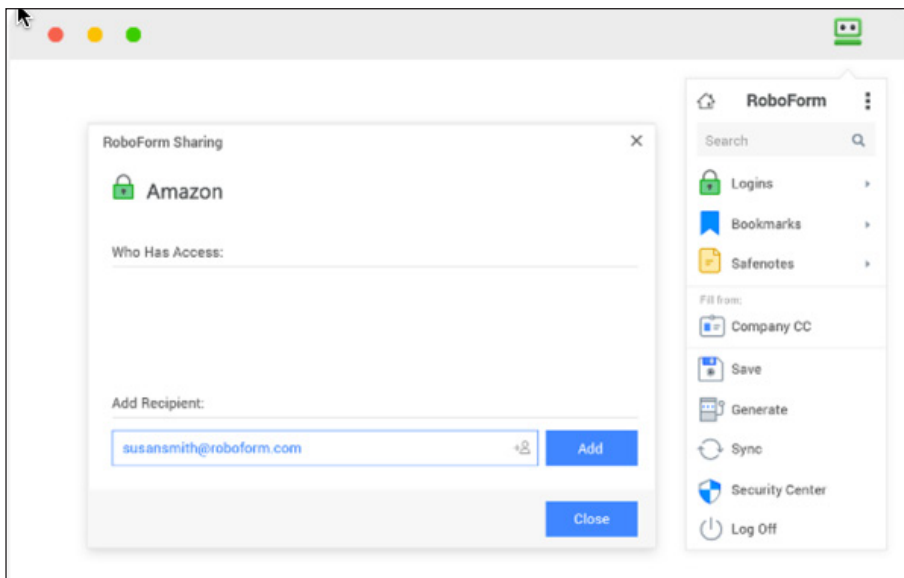
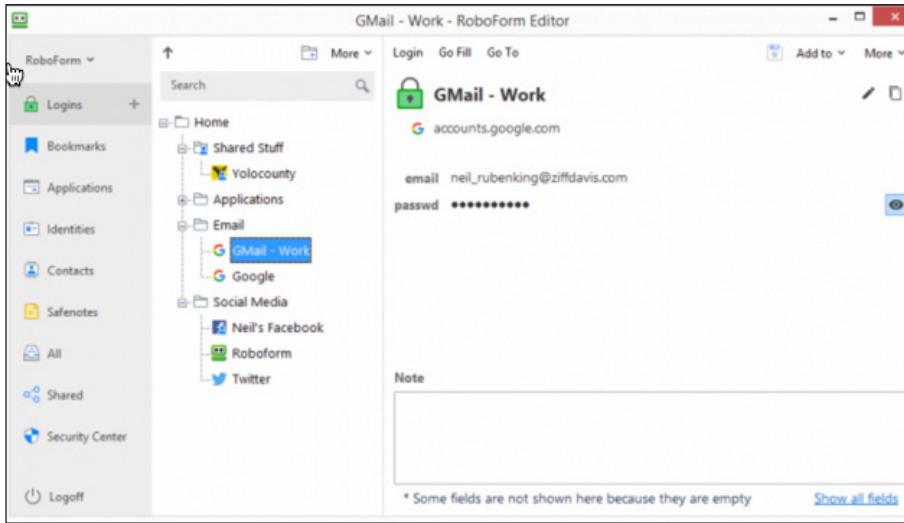
RoboForm is the password manager that **techies would love** but that may **overwhelm non-techies**. Besides that, RoboForm is a solid and inexpensive password manager.












RoboForm offers a **free plan** which is for a single user on a single device. It then offers three sets of licenses. The **Individual License** will run you **23.88\$ for a 1-year plan, \$64.44 for a 3-year plan and \$99.50 for a 5-year plan.**

You then have the **Family License** which is good for up to 5 users. The **1-year plan is \$47.75, the 3-year plan is \$128.85 and the 5-year plan is \$199.00.**

Finally, RoboForm offers a **Business License-for 30 users** which would come up to **\$1,048.50 for a 1-year plan, \$2,695.50 for a 3-year plan and \$3,892.50 for a 5-year plan.**



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

	 Lastpass	 KeePass	 1Password	 Dashlane	 Passwordstate	 Keeper	 Sticky Password	 Devolutions Password Server	 RoboForm
Offline Mode	✓	✓	✓	✓	✓	✓	✓	*	✓
Two-Factor Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓
Browser Integration	✓	✓	✓	✓	✓	✓	✓	✓	✓
Autofill Forms	✓	✓	✓	✓	✓	✓	✓	✓	✓
Password Generator	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security Alert	✓	✓	✓	✓	✓	✓	✓	✓	✓
Portable Application	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mobile Application	✓	✓	✓	✓	✓	✓	✓	*	✓
Security Audits	✓	✓	✓	✓	✓	✓	✓	✓	✓
Import Passwords	✓	✓	✓	✓	✓	✓	✓	✓	✓
Export Password	✓	✓	✓	✓	✓	✓	✓	✓	✓
Single Sign-On (SSO)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Password Sharing	✓	✓	✓	✓	✓	✓	✓	✓	✓
Integrated Database	✓	✓	✓	✓	✓	✓	✓	✓	✓
On-Premise	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cloud Based	✓	✓	✓	✓	✓	✓	✓	✓	✓

* Remote Desktop Manager is required for this feature.

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!