1Password Frequently Asked Questions (FAQ)

Alexander Rodriguez - 2024-05-23 - Comments (0) - 1Password

Getting Started with 1Password at Brown

Q. Is 1Password mandatory?

A. 1Password is not mandatory, but it is highly recommended. If you are unable to remember strong, unique passwords for every online account, then we strongly encourage the use of a password manager and our recommendation is 1Password due to its excellent security and helpful features. In today's technical environments, it's likely you have more passwords than you can remember. If this is you, then you should be using a password manager that can create and track complex passwords.

Q. Is there a risk to putting all your passwords in one place?

A. While leveraging a password manager does "put all of your eggs in one basket", the reward outweighs the risk. 1Password never has a decrypted version of any data. The only place the passwords are accessible in a usable form is on your machine. In order to gain this access, we require a Master Password, two-step authentication, and your account Secret Key when logging in on a new device. Brown performs an annual security review of the vendor to make sure that their security meets Brown requirements. Here's what 1Password says about their security model.

Q. How do I set up my 1Password Enterprise account?

A. Faculty and staff will be automatically enrolled in 1Password Enterprise and will receive an invitation email to set up their account. 1Password Enterprise is not available for students, clinical faculty, medical residents, or alumni at this time. Follow the instructions in the email to set up your account. At the end of the setup process, you will be presented with a digital Emergency Recovery Kit.

It is important for you to save the Emergency Recovery Kit in a secure location. 1Password suggests that you store your Emergency Recovery Kit in physical and digital storage. Examples of physical storage include printing out the Emergency Recovery Kit and storing it with other important documents, such as your passport or birth certificate. Regarding digital storage, 1Password suggests storing your Emergency Recovery Kit in a password-protected folder and storing that folder on a flash drive. For more information on securely storing your Emergency Recovery Kit, please refer to Where to store your 1Password Emergency Kit.

Q. How does the 1Password Families benefit work, and with whom can I share it with? Can I keep it after I leave Brown?

A. Brown has partnered with 1Password to provide 1Password Families at no cost for faculty and staff. This is a personal 1Password account granted to you that also includes five (5)

additional 1Password licenses. Once set up as a Family Manager, you can invite up to 5 additional family members or friends to join your plan through your family Dashboard so they can also use 1Password to keep their digital lives safe.

If you leave Brown, you have a few options with regard to keeping your family account. You can either transfer ownership of the family account to another member of the family or downgrade the account to an individual plan. If you choose to downgrade to an individual plan, any members you previously invited to the family account will lose access to the shared vaults and other family features. You would need to either create your own individual accounts or join another family account if invited.

For more information on how to take advantage of 1Password Families please reference the article Activate 1Password Families

Q. How does 1Password Enterprise compare to 1Password Families?
1Password Enterprise Account

- Available to currently employed faculty and staff.
- Brown controls minimum security requirements, i.e. required two-step authentication.
- Brown provides support, i.e., Master Password recovery.
- You lose access to your Enterprise account when your employment with Brown ends.
- To be used for Brown-related passwords and secrets (see 1Password Families for accounts appropriate to use for personal passwords and secrets).

1Password Families Account

- Available to currently employed Faculty and Staff. For more information, please refer to the article Activate 1Password Families.
- Can be used to store personal passwords.
- Brown cannot see nor recover these passwords.
- 1Password provides support.
- Upon the end of your employment with Brown, you get to keep your passwords and can purchase yearly renewals if desired. Refer to 1Password's website for pricing.

Q. What data does Brown have access to in 1Password Enterprise?
A. Neither 1Password nor Brown can access any passwords found in your employee vault. Administrators only have access if they are added as members to a shared vault.

Q. How do I keep my work (Enterprise) and my personal (Families) 1Password vaults separate?
A. Create two 1Password accounts with separate emails: one for work, the other for

personal use. Your personal 1Password Families account provides a 1Password vault where you can store all your personal accounts, passwords, credit card information, and more.

One way to maintain separation between 1Password Families/personal and 1Password Enterprise/work accounts is to use different browsers for each account. You can also do this with different browser profiles (within the same browser) to manage different accounts with different email addresses. Here are instructions for the three top browsers:

- Chrome: Add a person or profile in Chrome
- Firefox: Multiple Profiles
- Edge: Sign in and create multiple profiles in Microsoft Edge

For instructions on how to set up a 1Password Families Account, please refer to the "Activate 1Password Families" article.

Read more about your Families account at Claiming your 1Password Families as a perk account.

Q. Can Brown clinical faculty use 1Password? How about medical residents?
A. Clinical faculty and medical residents do not have access to 1Password Enterprise at this time.

Q. What if I already have a personal 1Password account with my Brown email?
A. If you already have a 1Password account using your Brown email address, it's very important that you migrate all your personal items out of your personal account before setting up your 1Password Enterprise account. If you set up your 1Password Enterprise account without migrating your personal items out of the personal account, several scenarios could unfold:

1. Duplicate Accounts: You may end up with two separate 1Password accounts - your personal account and the organizational account linked to your Brown email address. This can lead to confusion as you'll need to manage two separate sets of passwords and data.
2. Loss of Data Access: Without migrating the content of your personal vault, you risk losing access to any passwords or sensitive information stored exclusively there. This could be problematic if you rely on that information regularly.
3. Lengthy Manual Transfer: You may still be able to manually transfer the data from your personal vault to your Brown 1Password Enterprise account after joining the organization. However, this process can be time-consuming and might require careful attention to ensure all important data is transferred accurately.

Q. What happens to my 1Password account when I leave Brown?
A. Faculty and staff will lose access to their Enterprise Account, but will still have access to their Families Account if they decide to pay for the service.

You can find more information and help articles about Families accounts at 1Password support.

Q. I'm leaving Brown University and want to hand off some passwords. What should I do?

A. If you are leaving Brown University and have important passwords saved that pertain to your role, it's very important that they are handed off before leaving Brown. The process of handing over passwords to a coworker is easy. 1Password suggests you create a shared vault with whoever you will hand over the necessary passwords to. Once you've created the shared vault you can move the item from your employee vault into the shared vault. To do this on the desktop app, you can click and drag the item from your employee vault to the desired shared vault. To move an item in the web browser, navigate to the item and under the item title click the Share button. Within the share menu click Move/Copy and select the vault you would like to move the items to. For more information on sharing items please refer to the Move or copy items article.

Q. What do I need to do to maintain my 1Password Families account after leaving Brown?

A. Faculty and staff can renew their 1Password Families account after leaving Brown. Please refer to 1Password's website for pricing.

1Password Basics

Q. I'm trying to activate my new account, but I think I lost the email. What should I be looking for? What if I can't find it or it has lapsed?

A. Your invitation will have been sent by 1Password with the subject "Activate your 1Password account."

If you cannot find your invitation, or you've tried and it has expired, contact the OIT Service Center by submitting a ticket or emailing us at help@brown.edu.

Q. How do I change/reset my Master Password?

A. You can reset your Master Password by navigating to your 1Password profile and following the steps below:

1. Log into brownuniversity.1password.com.
2. Click on your name in the top right-hand corner, then click My Profile.
3. Select Change Password on the left-hand sidebar and follow the on-screen instructions.
4. A new Emergency Recovery Kit will be generated. Download the Emergency Recovery Kit, open it, fill out the relevant information, and save it to a secure location.
5. A congratulatory message will be displayed after you have successfully completed the changes.

6. Since you have changed your password, you will now need to log back into the 1Password desktop app with the newly created password.
7. Lastly, since 1Password is protected with two-step authentication, you will be prompted by Duo to complete authentication and login.

Q. How can I set up a browser extension, desktop application, and mobile app?
A. For the most seamless experience, it is highly recommended that you install and log in to the 1Password web browser extension and desktop application. Read the article Get to know 1Password in your browser for information on the browser extension. Read the article Get to know 1Password for Windows or Get to know 1Password for Mac for information on downloading the desktop application. Read the article Get to know 1Password for iOS/iPadOS or Get to know 1Password for Android for information on downloading the mobile application.

Q. How do I import passwords from LastPass?
A. If you are coming to 1Password from another password manager, you may already have spent a considerable amount of time storing your user names, passwords, and other data within that program or web browser. To assist with this transition, you have the ability to import your stored data seamlessly into 1Password through their desktop app. The article Transfer Items from LastPass to 1Password outlines how to export your passwords from LastPass into 1Password. You can also reference their video Import your LastPass data using 1Password's in-app importer.

Q. What happens if I forget my Master Password?
A. If you forget your Master Password for your 1Password Enterprise account, you can reach out to the OIT Service Center for assistance. If you forget your Master Password for your 1Password Families account, you can recover it using your Emergency Recovery Kit.

Q. In what ways does 1Password provide accessible functionality?
A. 1Password has enabled some common accessibility features available in both the web and desktop apps:

- Keyboard Navigation: Users can navigate through the application and access its features using only the keyboard without relying on a mouse. This includes using keyboard shortcuts for various actions.
- Screen Reader Support: The application is compatible with screen reader software, enabling users with visual impairments to navigate and interact with the interface using screen reader commands.
- High Contrast Mode: The application offers a high contrast mode, making it easier for users with low vision to distinguish elements on the screen.
- Accessible Form Fields: Form fields and other interactive elements are properly labeled and structured, ensuring they are accessible to users who rely on screen readers or keyboard navigation.

- Resizable Text and UI Elements: Users can adjust the size of text and UI elements within the application to better suit their preferences and needs.
- Color Customization: Users can customize the color scheme or contrast settings of the application to improve readability and usability based on their individual preferences or accessibility needs.
- Accessible Error Handling: Error messages and alerts are presented in a clear and accessible manner, providing guidance to users in resolving issues or completing tasks successfully.
- Focus Management: Focus is appropriately managed within the application, ensuring that keyboard users can easily identify and navigate to interactive elements.
- ARIA Roles and Attributes: The application utilizes ARIA (Accessible Rich Internet Applications) roles and attributes to enhance accessibility for screen reader users and assistive technologies.
- Responsive Design: The application is designed to be responsive and adaptable to different screen sizes and devices, providing a consistent user experience across desktop and mobile platforms.

For more information regarding accessibility features, please refer to 1Password Commitment Statement regarding accessibility.

Q. What is the Watchtower feature?
A. The Watchtower dashboard serves as your security headquarters, automatically summarizing known breaches or other vulnerabilities. You can also find Watchtower alerts on individual items if there's an issue that you need to address. Within the dashboard, you can:

- Update weak and reused passwords.
- Assess and improve your overall Security Score.
- Monitor your email addresses for involvement in data breaches and get alerts when your sensitive information is compromised.

Access the Security Dashboard and your Security Score by opening your vault, then clicking on Watchtower in the left margin menu of your employee vault. For more information visit watchtower.1password.com.

Q. How do I manage my vault?
A. See the document Get to know 1Password in your browser for information on how to manage your vault.

Q. How can I generate secure passwords?
A. 1Password can be used to both store and generate secure passwords. Generate a secure password by doing any of the following:

- Using the in-field icon – Click the Generate Password icon in the Password field.
- Using the web browser extension – Click the 1Password icon then click the Menu icon next to "+ New Item", then select Password Generator.

For step-by-step instructions, read Generate a Secure Password.

Q. What is a passkey, and how do I use it?
A. While passkeys are not currently supported by Brown for Shibboleth authentication, some other websites do support them. Passkeys allow you to create and sign in to online accounts without a password. Unlike traditional passwords, passkeys utilize technology similar to when you visit a secure website. That means every passkey has two parts: a public key and a private key. Together, they keep your accounts secure by allowing websites and apps to check that you are who you say you are.

To use a passkey, find an existing login that now supports passkeys using Watchtower or create a new account on a passkey-supported website. Depending on the website, you may need to create an account with a username and password before creating a passkey. When you choose the option to create a passkey, 1Password will offer to save it.

After creating a passkey, the next time you go to a website where you set up the passkey, you will see a prompt in the top right corner asking if you would like to sign in with a passkey. After clicking Sign In, you will immediately sign in to your account without typing a password.

If you would like to read more on passkeys, please refer to the following articles:

- Save and sign in with passkeys in your browser
- What are passkeys and how do they work?
- The passwordless experience you deserve

Q. How do I securely share a password?
A. You can share a password or other item (e.g., username or Secure Note) with another Brown 1Password user in one of two ways. The first method is through the item itself. This method will only allow you to share a single item, which can only be shared for a set amount of time. More information on this method can be found in the Securely share 1Password items with anyone article. The second method is through a shared vault, information on this method can be found in the Create and share vaults article.

Q. What are shared vaults, and how can I use them with my group to share

passwords?

A. A shared vault is a special vault that you can use to securely and easily share site password entries and secure notes with other Brown 1Password users. Shared vaults use the same technology to encrypt and decrypt data that a regular 1Password account uses but are designed to accommodate multiple users for the same folder. See How to create and manage shared vaults for your team for full details.

Q. What are some best security practices for using 1Password to ensure I get the most out of it?

A. The short answer is to ensure that all of your passwords are at least 16 characters in length and unique. For specific steps you can take, review the 1Password article How to keep your 1Password account secure.

1Password Help Guide

- Manage Your Secure Notes
- Manage Your Form Fills
- Manage Your Vault
- Manage Web Browser Extension Preferences
- Link or Unlink Your Personal Account
- Use the Sharing Center
- Generate secure passwords

For more help documents, visit 1Password support.

Troubleshooting

Q. What if I forget my Master Password?

A. The Office of Information Technology can reset your Master Password for your Enterprise account. Open a ticket with ithelp@brown.edu to reset your enterprise master password. Brown cannot assist in the recovery of your Family account, but you can do so using your Emergency Kit.

Q. Why am I not able to see my team's shared folders?

A. You won't be able to access your team’s shared vault unless someone with sharing permissions to that vault adds you as a member. Please reference Share a vault for more information.

Q. Why does the password field not auto-populate when using desktop

applications such as Microsoft Office or the VPN client (Big-IP/F5)?

A. 1Password can auto-populate log-in info on desktop apps through Universal Autofill for Mac. To enable Universal Autofill you will need to go into your Macs system settings and enable the feature. Please visit the article Use Universal Autofill in apps and browsers on your Mac for instructions on how to enable the feature. Unfortunately this feature isn't available for Windows so to solve this issue, 1Password recommends using Quick Access. Quick Access is a feature found in the 1Password desktop application that allows you to find any item without leaving the app you're working in. To open Quick Access on Windows/Linux, press Ctrl + Shift + Space and Mac Shift-Command-Space. For more information on the feature, visit their Quick Access documentation.

Related Content

- Introduction to 1Password
- Activate 1Password Families
- Transfer Items from LastPass to 1Password