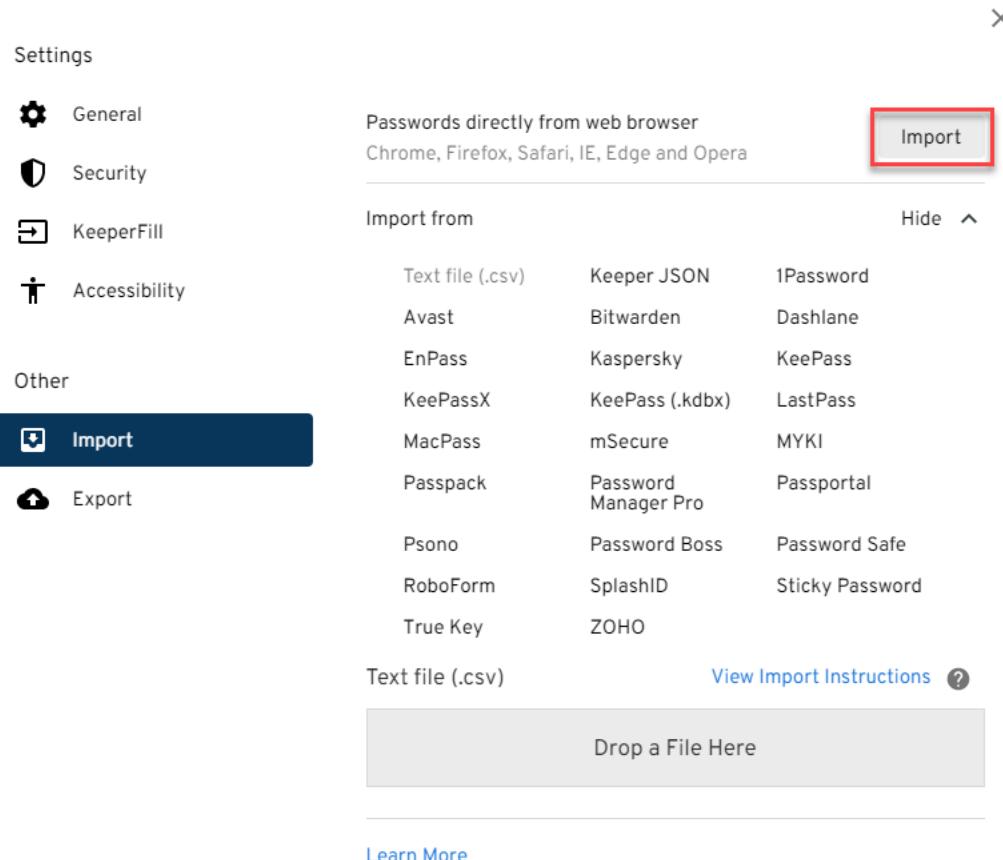


Guide: Keeper Password Manager

This step-by-step guide will walk you through setting up Keeper Password Manager on your machine. Keeper allows you to store passwords securely in a vault and auto-fill the passwords on any website you want. You can also access passwords on your mobile device and store 2FA rotating codes if you have those for accounts. We set up Keeper to use single sign-on authentication with your M365 Business Premium License to make it as easy as possible.

1. You will receive an email invitation to keeper, click on the link to accept the invitation and enter the verification code you were provided in the email. It will log you in using your tcevt.com credentials.
2. You can import any existing saved passwords from your browser by downloading and running the import tool. This is recommended. If you don't do it right away, you can do it later in the vault website by going to settings (in the top right under your email address) -> import as shown below.



The screenshot shows the 'Settings' page of the Keeper Password Manager. On the left, there's a sidebar with icons for General, Security, KeeperFill, Accessibility, and Import (which is highlighted with a blue background). Below that is an 'Other' section with an Export icon. The main content area has a heading 'Passwords directly from web browser' with 'Chrome, Firefox, Safari, IE, Edge and Opera' listed. To the right of this is a 'Import' button, which is also highlighted with a red box. Below this is a table of import sources, with 'Text file (.csv)' and 'Keeper JSON' as the first two options. At the bottom, there's a 'Text file (.csv)' input field with a 'Drop a File Here' placeholder, a 'View Import Instructions' link, and a 'Learn More' link.

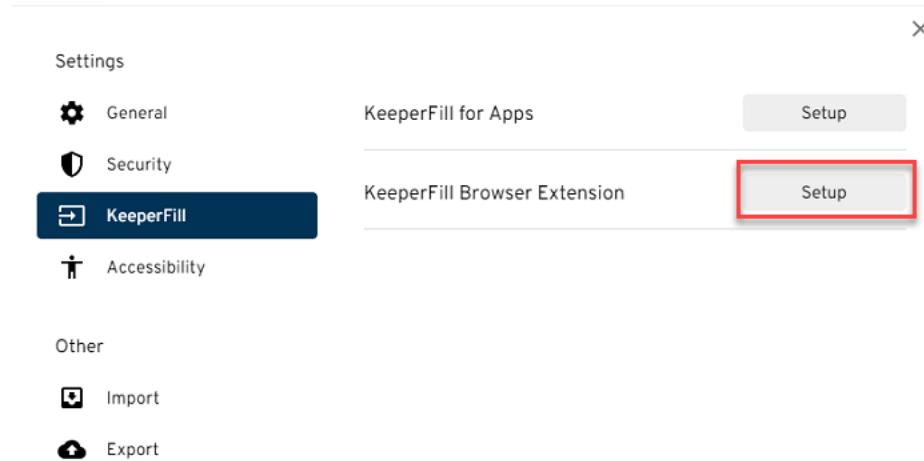
Import from	Hide	^
Text file (.csv)	Keeper JSON	1Password
Avast	Bitwarden	Dashlane
EnPass	Kaspersky	KeePass
KeePassX	KeePass (.kdbx)	LastPass
MacPass	mSecure	MYKI
Passpack	Password Manager Pro	Passportal
Psono	Password Boss	Password Safe
RoboForm	SplashID	Sticky Password
True Key	ZOHO	

Guide: Keeper Password Manager

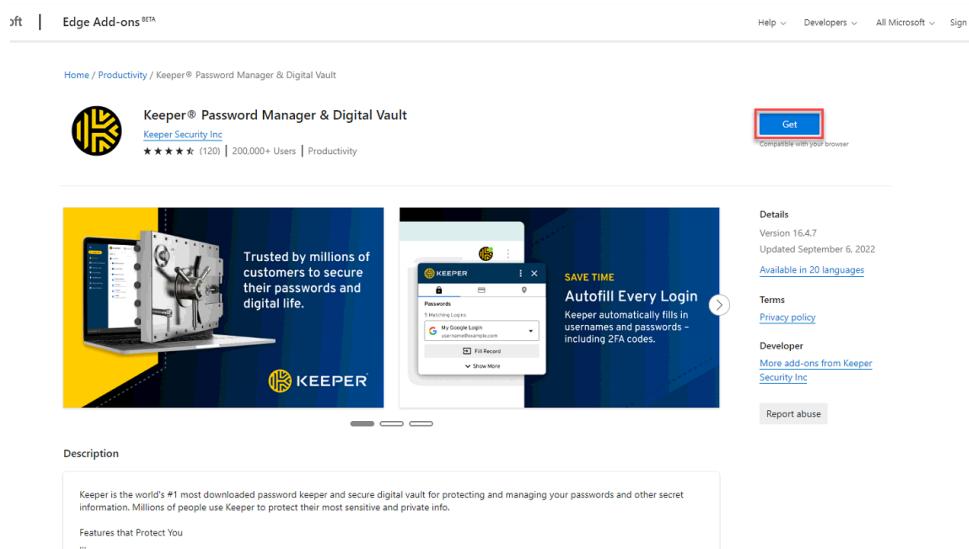
3. The next step will be to add the Keeper Password Manager browser extension to your browser. This guide will use Microsoft Edge as an example. Click on your email on the top right and select settings.



4. Go to KeeperFill then select setup next to KeeperFill Browser Extension.



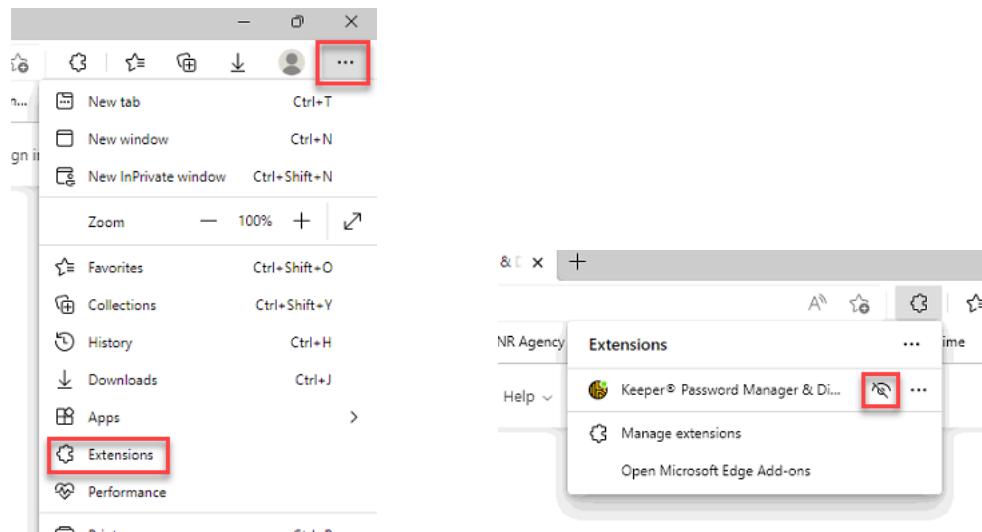
5. You'll be taken to the browser extension page to install it.



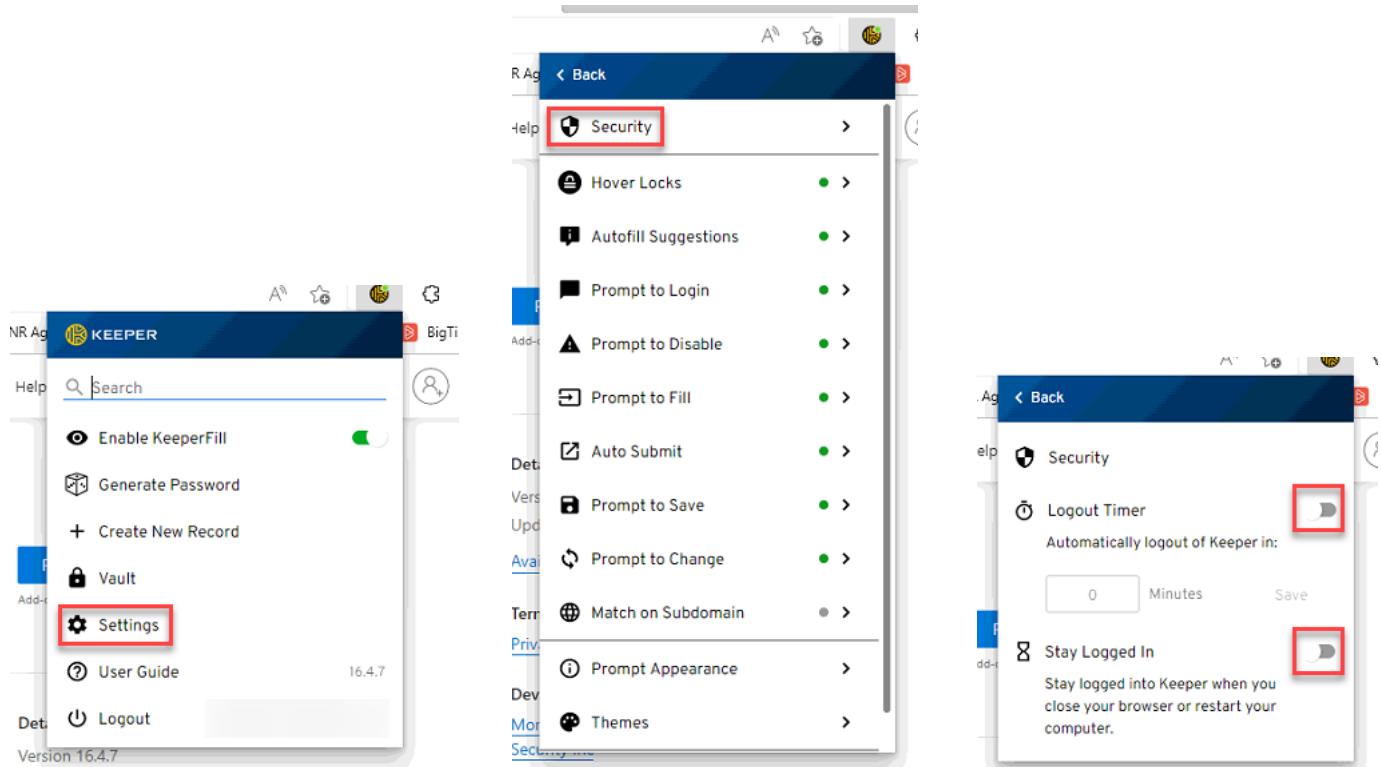
The screenshot shows the Microsoft Edge Add-ons page for the Keeper® Password Manager & Digital Vault extension. The extension has a 5-star rating and over 200,000 users. The 'Get' button is highlighted with a red box. The page also displays a description of the extension, including its features like password management and digital vault, and a screenshot showing it integrated with a browser.

Guide: Keeper Password Manager

6. To keep the extension visible all the time in your top bar, click the 3 dots in the top right and then extensions. Click on the eyeball icon to make it visible all the time.

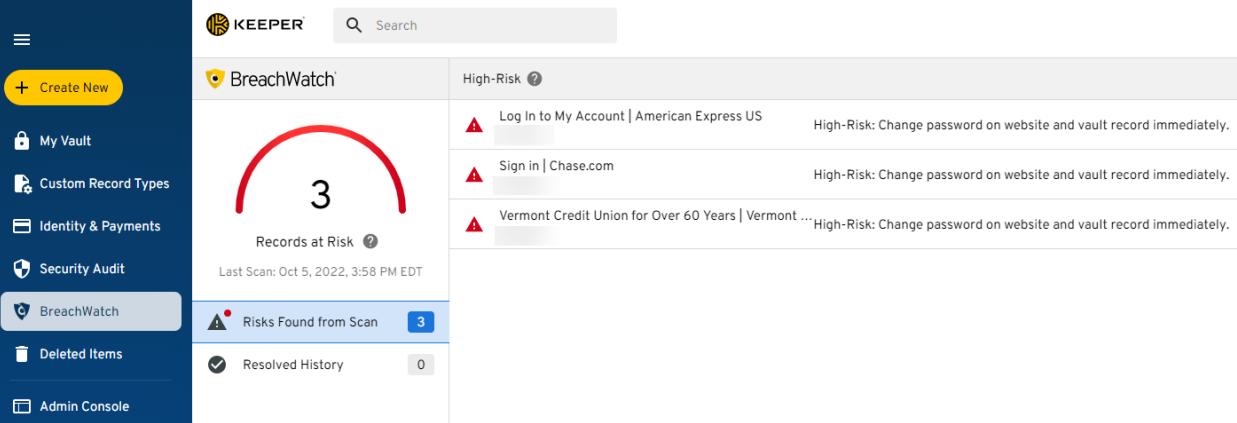


7. You can click on the browser extension now and go to settings to adjust how often it times on before needing to re-authenticate, or you can leave it activated all the time, by going to settings -> Security.



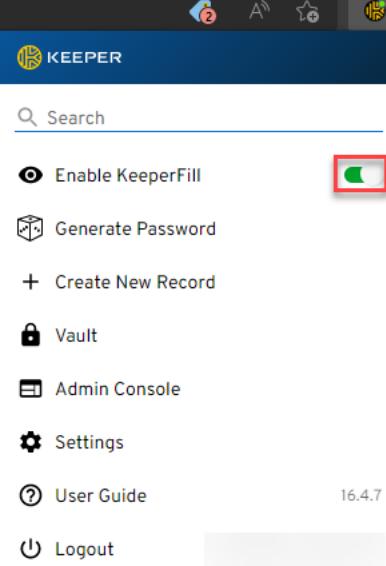
Guide: Keeper Password Manager

8. Part of your Keeper subscription includes “BreachWatch” which will monitor your username/password combinations on the dark web or in known data breaches to alert you if your information is available to threat actors. It is a good idea to change your password for these accounts to be as safe as possible online.



The screenshot shows the Keeper web interface. On the left, a sidebar menu includes options like 'Create New', 'My Vault', 'Custom Record Types', 'Identity & Payments', 'Security Audit', 'BreachWatch' (which is selected and highlighted in blue), 'Deleted Items', and 'Admin Console'. The main content area is titled 'BreachWatch' and shows a 'High-Risk' status. It features a red semi-circular progress bar with the number '3' in the center, indicating the count of records at risk. Below the bar, it says 'Last Scan: Oct 5, 2022, 3:58 PM EDT'. A table lists three items as 'High-Risk': 1. 'Log In to My Account | American Express US' with the note 'High-Risk: Change password on website and vault record immediately.' 2. 'Sign in | Chase.com' with the note 'High-Risk: Change password on website and vault record immediately.' 3. 'Vermont Credit Union for Over 60 Years | Vermont ...' with the note 'High-Risk: Change password on website and vault record immediately.'

9. Keeper has the ability to auto-fill your passwords, change your passwords for you, or generate new secure passwords when trying to increase your personal security posture. If the interface feels too intrusive to your browsing, you can disable the KeeperFill by clicking on the extension and disabling it.



The screenshot shows the Keeper extension menu in a browser toolbar. The menu items are: 'Enable KeeperFill' (with a green switch icon, which is highlighted with a red box), 'Generate Password', '+ Create New Record', 'Vault', 'Admin Console', 'Settings', 'User Guide 16.4.7', and 'Logout'.

More information is available for all the features Keeper can provide in the Keeper end user guide located here: [Keeper End-User Guides - User Guides](#). You can always reach out to us at Arrowhead Tech with any problems as well.