Keeper Password Manager: FAQ

Q: What is a password manager?

A: A password manager is a software solution that keeps track of the passwords you choose to store in it. It is the digital equivalent of writing your important passwords down in a notebook, but more secure because it is encrypted. Most password managers also have additional features, like the ability to generate randomized passwords for you and can tell you whether your password is strong.

Q: Are password managers safe?

A: Password managers are largely considered safe in the cyber security industry.

The average person has many different accounts that all require a password. Many people who don't use a password manager have to write down all their passwords in order to remember them or they simply start reusing the same password for multiple accounts. If you don't keep your written passwords locked in a safe at all times, there is a chance that someone can steal your passwords and then access your accounts. If you reuse the same password for multiple accounts (for example, if your Netflix account and your bank account have the same password) then an attacker who gets access to your Netflix account can easy figure out how to access your bank account too.

Password managers make it easy to have different, secure passwords for every account—because you don't have to remember them. You only have to remember how to login to your password manager and then you can access all of your other passwords.

According to the National Institute of Standards and Technology (NIST), password managers provide improved security by generating unique, long, and complex passwords[1]. Furthermore, NIST states that password inputs should allow pasted input as this enables the use of password managers and increases the likelihood strong passwords will be used[2].

The Center for Internet Security also agrees that password managers improve security. If strong authentication is used to protect the password vault, the benefits a password manager brings outweigh the risk of centrally stored passwords[3].

[1] NIST SP 800-63 Digital Identity Guidelines-FAQ
[2] Digital Identity Guidelines: Authentication and Lifecycle Management (nist.gov)
[3] CIS Password Policy Guide (cisecurity.org)

Q: What if my password manager gets hacked?

A: It is important to choose a trustworthy vendor when selecting a password manager. Always research the vendor to make sure they are using security measures that follow the latest cyber security best practices. It is also worth checking to see if the vendor has been involved in any data breaches. Luckily, IOT Security has already vetted Keeper Security and determined them to be trustworthy.

If you are concerned that an attacker may have accessed your Keeper password vault, please submit a help desk ticket to be forwarded to IOT Security Operations or email **#IOT Keeper Admins** to begin an account compromise investigation.

Account Compromise Prevention Tips

- Do not leave your computer unlocked and unattended.
- Do not write down your login credentials and tape them to your computer.
- Do not share your credentials with others.
- Report lost/stolen computers to IOT **ASAP**!
- If you fall for a phishing attempt and your credentials are stolen, notify IOT **ASAP**!

Q: How does Keeper Security keep my vault safe?

A: Keeper vaults are end-to-end encrypted using Elliptic-Curve cryptography. This means that even though your vault is stored on Keeper's servers, they only store your data in encrypted form. They do not have access to your decrypted data. Each device that you log into your vault from has a locally generated and stored private/public key pair which allows you to decrypt your vault and view it. Keeper requires each device that you use to log into your vault to be approved before it can access your vault. This means that for someone to gain access to your vault, they would need to know your State password AND have access to one of your approved devices.

For more information on Keeper's security practices, see here:
https://www.keepersecurity.com/security.html

Q: Is it possible for Keeper to be hacked?

A: Any company is at risk for suffering a data breach to some degree. However, Keeper Security has not had any history of data breaches so far and they are also certified by the NIST Cryptographic Module Verification Program (CMVP) to meet the FIPS 140 standard.

Additionally, Keeper offers a government cloud version of their solution that is FedRAMP certified, which is a compliance program established by the US government that is specifically for cloud applications.

Keeper Password Manager is a zero-trust, zero-knowledge product. This means that your vault is encrypted when stored in Keeper's data center. Decryption and encryption happen on your local device. Neither Keeper nor IOT staff can go in and access your unencrypted data. Were Keeper to be hacked and have data exfiltrated, it would still require your decryption key to read.

Here is some more info on Keeper's security measures:

https://www.keepersecurity.com/blog/2022/08/03/has-keeper-been-hacked/#:~:text=Keeper%20has%20never%20been%20hacked,passwords%20and%20other%20private%20information.

Q: If I never store my passwords digitally and only keep them written down in a notebook that I keep locked up, is that safer than using a password manager?

A: This practice is not significantly safer than just using a password manager. Even if you never choose to store your passwords on your device, they are still stored somewhere. Any website that requires you to log in has your username and password stored in their database—they have to in order to verify your identity. If that website ever has a data breach, your password is still at risk of being stolen from their databases. There is no absolute way to make sure your passwords never end up online, therefore the benefits of using a password manager outweigh the risks.

Q: If my state account or computer gets compromised, is my Keeper vault compromised too? What should I do?

A: Even if an attacker knows your password, they will need physical access to a device that is approved to log into your Keeper vault. You can help prevent unauthorized access by locking your computer when you step away from it and keeping your password confidential. Do not share your password with coworkers and never leave it written down where a passerby can find it.

If your computer gets lost or stolen, IOT can remotely freeze it so that others cannot use it.

Q: Is using Keeper optional or mandatory?

A: This service is optional. Your vault is automatically created, but you can choose not to use it. IOT Security recommends using a password manager over writing passwords on paper or using easy-to-guess passwords, but it is still your choice.

Q: Can I only use my Keeper vault for work? What if I want to store my personal passwords in it?

A: Your Keeper enterprise password manager is to be used solely for state business. Examples of appropriate credentials to store in the State's password manager include:

- Credentials for State of Indiana systems
- Credentials for websites and applications that state personnel use to perform their job duties

These credentials should **only be stored in the State's password manager** and not a personal use password manager.

Some credentials are related to state business and employment but are still considered personal. These credentials are **OK to be stored in both the State's password manager and personal use password managers**. These credentials include:

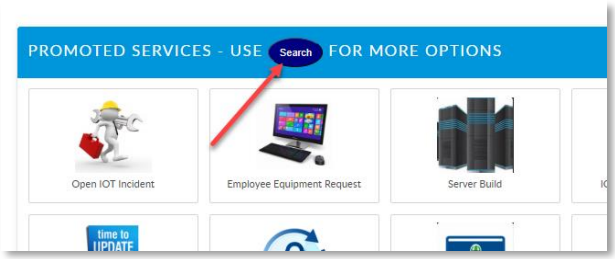
- Credentials for websites that state personnel use to access training for their job duties
- Credentials for My Active Health, My INPRS, and other Indiana employee benefits websites

No credentials that are unrelated to job duties, should be stored in the State's password manager. Examples of **inappropriate credentials to store in the State's password manager** include:

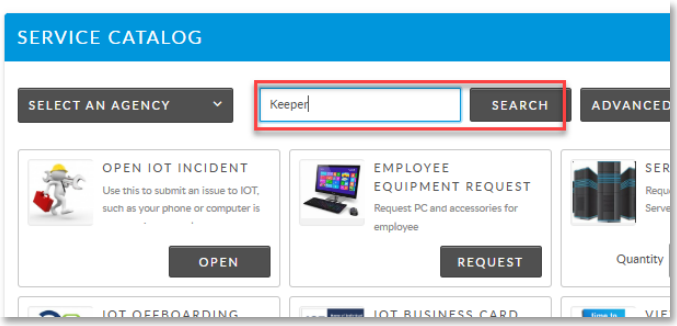
- Credentials for personal banking accounts
- Credentials for personal email accounts
- Credentials for personal social media accounts
- Credentials for personal TV and media streaming applications

Personal passwords should be stored in a separate password manager. As part of our purchase agreement with Keeper, State of Indiana users are allowed to set up a personal use Keeper Family Plan for free. You can setup you free Family Plan by going to the ASM Self Service Portal.

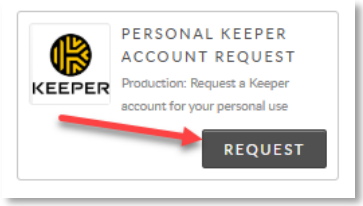
Click on the **Search** button:



Search "Keeper":



Then, click **Request** and fill out the form.



Email **#IOT Keeper Admins** if you need help with this process.

Q: Can I use Keeper on my phone?

A: The Keeper mobile app can be used on any mobile device currently registered with Ivanti. You should see the app in the Apps@Work tab of the Ivanti app on your device.

Q: Why can't I access my Keeper vault from my home computer?

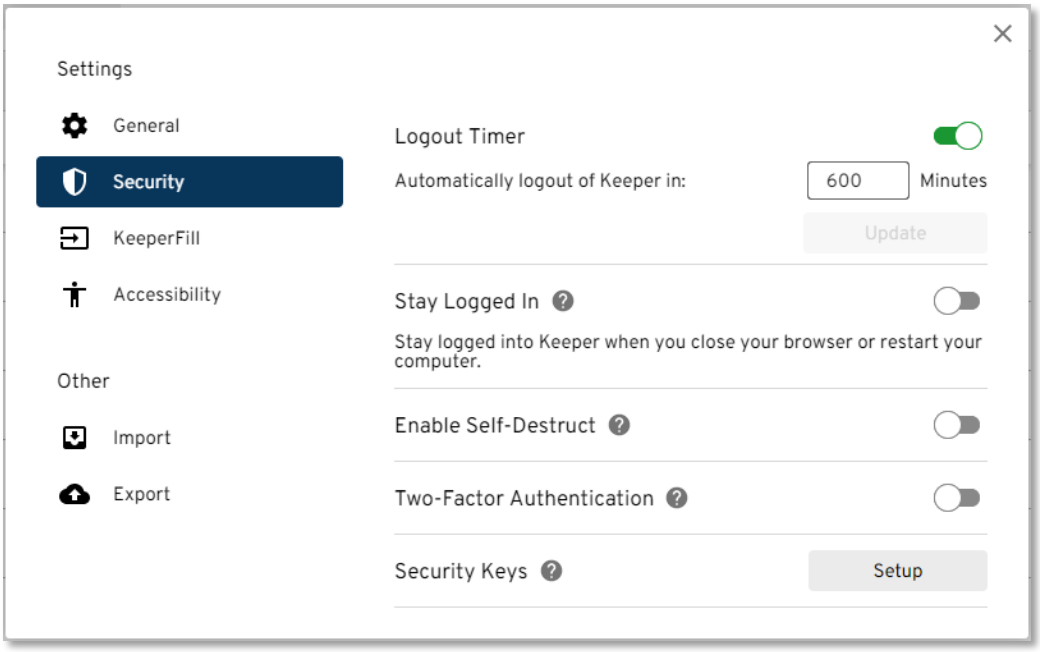
A: Your enterprise Keeper vault is only accessible from IOT-managed devices. IOT cannot monitor, secure and triage unmanaged devices and it would therefore be risky to allow a vault containing State of Indiana passwords to be accessed from an unmanaged device. This helps protect your vault from unauthorized access.

Q: Why can't I use KeeperFill in an Incognito browser?

A: Incognito browsers hide your identity (*to a certain degree—the browser won't see what you are doing, but your organization and internet service provider still can*). Keeper cannot verify your identity and give you access to your vault from an Incognito browser.

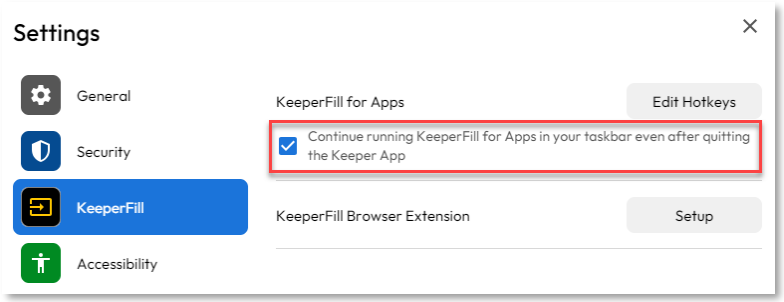
Q: The Keeper desktop app keeps signing me out and prompting me to sign back in. Is there a way to adjust my logout timer?

A: In the desktop app, click on your account name in the top right corner, then Settings. Click on the Security tab and enter the number of minutes you would like for Keeper to stay logged in. The maximum amount allowed by IOT Security is 600 minutes. This will allow you to stay logged into Keeper for 10 hours before being logged out again.



Q: How do I stop the Keeper desktop app from logging me out when I close it?

A: In the desktop app, click on your account name in the top right corner, then Settings > KeeperFill.



If you want Keeper to run in the background after you close the window, make sure the below option is checked. This will prevent you from being logged out when you close the window. If you want to disable this feature, make sure it is unchecked.

Q: How do I set up autofill for my desktop apps?

A: See here for instructions on KeeperFill for Apps: https://docs.keeper.io/en/user-guides/keeperfill-for-apps

Q: Why can't I set a master password for my Keeper account?

A: Keeper utilizes a feature called Single Sign On (SSO), which allows you to sign into Keeper using your State of Indiana account instead of creating a separate username and password just for Keeper. SSO has a lot of benefits, including:

- End users don't have to manage additional passwords and multifactor authentication methods, reducing end user burnout/overwhelm.
- Individual application owners don't have to worry about managing identity related processes (password policies, MFA, password resets, user verification, etc.).
- Administrating sign in options can be left to employees who specialize in Identity and Access Management (IAM).
- Fewer IAM policies have to be managed and they can be placed in a centralized location, resulting in improved security.
- SSO reduces users' ability to bypass security controls and allows more security customization than what is available "out of the box" for individual applications.

Q: Can IOT see the records stored in our vaults?

A: Keeper is a zero- trust, zero knowledge product. User vaults are encrypted and decrypted on their local device and an administrator will not be able to access or read what is stored in in them. Neither State of Indiana nor Keeper Security has access to users' records.

The only way an IOT Keeper administrator can access your vault is if they transfer your vault to another state account and then log into that account to access the vault. While the Account Transfer feature does give the administrator the ability to migrate the entire contents of the vault to another user, it does not give the administrator the capability to access the vault whenever they feel like it. The vault being transferred has to be locked first and after the contents are transferred the account is deleted. The end user will receive a notification when their account is locked by the administrator as well as when it's transferred and deleted.

IOT Keeper administrators are responsible for providing account access, but the responsibility of managing the records contained within a user's vault is solely theirs. The scope of Keeper is to provide a more secure password management alternative to having to remember/write down/reuse complex passwords. Users will still need to practice good password hygiene as outlined in the IRUA.

Document Version History

Author	Modification	Date
Cheri Walker-Owens	Document version 1 published.	4/24/2023
Cheri Walker-Owens	Updated answers.	1/16/2025