LastPass by LogMeIn

Security Model Snapshot

"Understanding the LastPass architecture is why I've completely switched my entire solution for managing passwords over to LastPass."

Steve Gibson
Security Researcher
Gibson Research Corporation

What does it mean that LastPass is encrypted?

LastPass keeps your data safe by never having access to your unique key – your master password.

LastPass is like a box filled with all the information you want to keep safe – like passwords, important documents and credit card information. You lock the box and keep the key. You send us the box for safekeeping.

The next time you want the box, you use your key to unlock it. Only you have the key, so only you can unlock the box.

How does it work under the hood?

When setting up your account, you create a unique master password. Using PBKDF2, your master password is used to generate two things: an authentication hash and an encryption key. The authentication hash is further protected, then sent to LastPass. Every time you log in, we check what you've submitted against the authentication hash to confirm your master password. The encryption key is plugged in to a strong encryption algorithm that's used to encrypt your LastPass vault. Only when the vault is encrypted is it synced with LastPass. LastPass safeguards your encrypted vault, sending it back to you anytime you need your passwords and keeping updates synced. LastPass is designed to keep sensitive data safe using a zero-knowledge security model.