LastPass

PRODUCT OVERVIEW

Federated Login Services: LastPass + Google Workspace

Added security for your business, simplified access for employees, using your Google Directory

When 85% of breaches involve a human element (phishing, stolen credential, human error), employee password practices remain the weakest point in a company's security and put sensitive data at risk! Configure LastPass Business with Google Workspace (previously G Suite) to automate and scale password management, while saving time for IT to keep your Business and data secure – all without adding another password for employees to remember and manage.

With a zero-knowledge infrastructure and proprietary multi-key model, LastPass' unique cloud-based federated login adds additional layers of security, without adding complexity for your end users. Rest assured that data security is not compromised at the hands of employee convenience.

LastPass Federated Login with Google Workspace

Integrate your source of truth and simplify access. LastPass' federation services can integrate your Identity Provider, Google Workspace, into LastPass' password manager, ultimately removing a user's need for a master password to log into their vault. Through a LastPass and Google Workspace Directory Integration, you can provision your employees to streamline adding and removing users.

Once your Directory is integrated with LastPass, federate to enable a seamless login experience that provides users access to LastPass using their Google Workspace credentials.

Zero-knowledge security model

Convenient passwordless experience

Set up and secure

Benefits of Federated Login

Simplify user access
Alleviate login frustrations to simply connect employees to their work, all while leveraging technology and solutions you've already implemented at your business.

Eliminate additional passwords
Sync your directory and complete a one-time, native federation configuration so employees only need one password to unlock work—their user directory login.

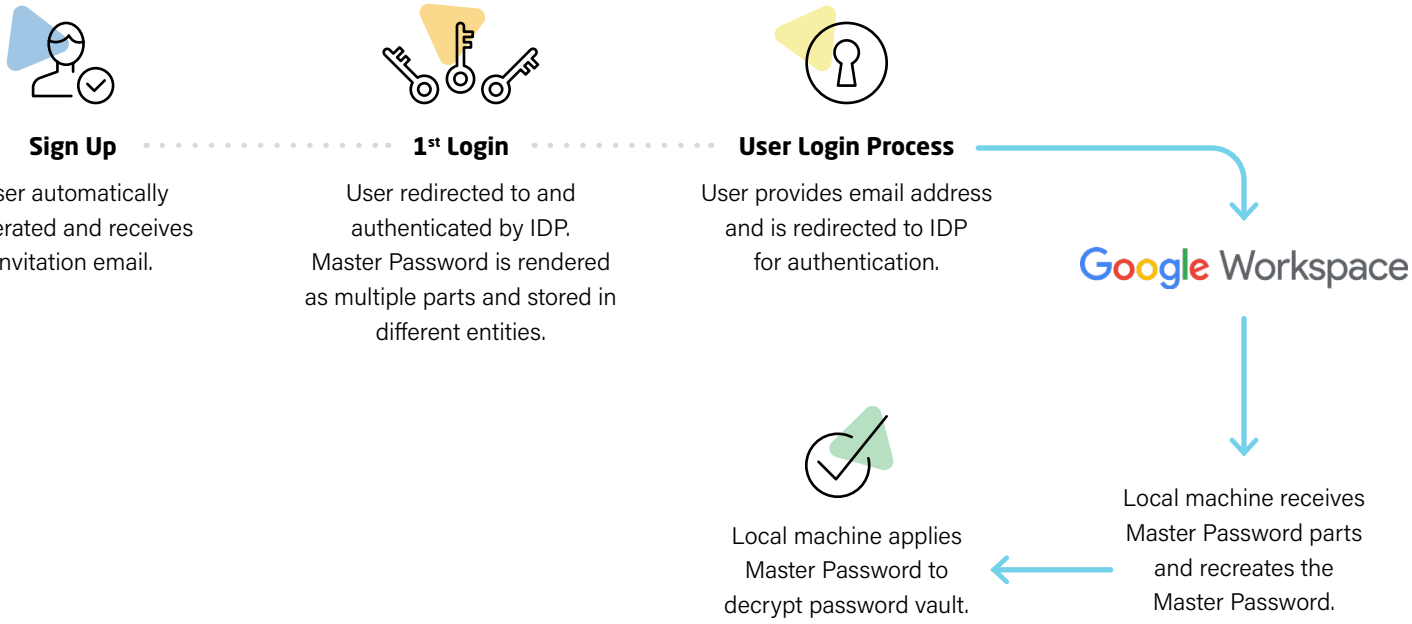
Increase adoption
Eliminating the enrollment process and the need for an additional password provides employees an immediate and extremely simple way to access the credentials they need to do their work.

Automate identity management
Save time and resources while scaling password management across your organization, by automating provisioning between your Identity Provider and LastPass. Easily ensure no data leaves your business when employees do.

Unmatched Security Model

In contrast with other approaches, LastPass has an improved technique for providing federated login to a user's vault. LastPass' federated login has a zero-knowledge infrastructure, which means that neither party (LastPass or your IDP) possess enough information to be able to access a user's vault. Instead, LastPass generates a password for a federated user, divides it into multiple parts and stores the parts in separate entities.

After successful authentication with an Identity Provider, a user's local device receives the password parts and combines them to recreate the master password. The local device decrypts the user's vault. Other than the user's local device, no single component has all the necessary information to recreate the password, thereby preserving zero-knowledge features. Moreover, the separate password parts alone are insufficient for unlocking the vault, significantly improving security and decreasing risk of breaches and hacks.



Learn More **Start a free trial of LastPass Business today.**

Sources:
1. Verizon, "Data Breach Investigations Report (DBIR)", 2021.