LastPass •••|

FACT SHEET: FEDERATED LOGIN

Simplify Access for Employees with Federated Login

Deliver what your employees have been asking for—a simplified login experience—with LastPass' cloud-based federated login. Employees can log in to LastPass using their Identity Provider's credentials: Microsoft Active Directory Federation Services (ADFS), Microsoft Azure Active Directory, Okta, Google Workspace (previously G Suite), PingOne, PingFederate, or OneLogin. LastPass increases security for your business, while providing a convenient, passwordless login for employees.

Microsoft Active Directory · Microsoft Azure · Google Workspace · okta · onelogin by ONE IDENTITY · Ping Identity.

Automate employee provisioning and deprovisioning

Simply onboard employees to LastPass with account creation that doesn't require an additional password. Federated login enables employees to register and login to their LastPass account because it's automatically provisioned through your Identity Provider, reducing time spent onboarding employees and ensuring no data departs as employees do.

Broader adoption throughout the organization

Eliminating the sign-up process and the need for another password gives employees immediate, simple access to the secure accounts they need to do their work and removes previous login frustrations. By federating with LastPass, your business will benefit from higher adoption rates and meet your password security goals faster.

Proprietary security architecture

LastPass uses a proprietary and highly secure method of distributing, storing and uniting encrypted keys to ensure the Identity Provider password is never shared with LastPass—and kept safe from hackers and bad actors. In addition, LastPass maintains a zero-knowledge infrastructure throughout the encryption and authentication process.

Passwordless experience

Zero-knowledge security model

Easier onboarding

Multi-key storage and encryption

Learn More

Start a free trial of LastPass Business today.