Password Management with Advanced Multi-Factor Authentication (MFA)

When poor passwords cause 80 percent of data breaches,1 it's clear that passwords alone won't protect your business. How can you ensure critical information is secure without adding friction for users? Employees understand the need for security, but they expect technology to be simple, convenient, and fast. As a result, businesses are more challenged than ever to secure passwords and manage authentication across a remote hybrid environment without disrupting end users.

LastPass reduces friction for employees while increasing control and visibility for IT with a password management and multi-factor authentication solution that is easy to manage and effortless to use. With combined password management and multi-factor authentication, businesses can secure all web logins, while adding a layer of security on other endpoints to lock down every access point to their business.

LastPass Business

LastPass Business delivers Password Management to empower employees to generate, secure, and share credentials seamlessly, while providing valuable insight and control to Admins and ensuring protection through LastPass' zero knowledge security infrastructure.

LastPass Advanced Multi-Function Authentication

LastPass Multi-Factor Authentication secures every access point to your business. From cloud and legacy apps to VPN and workstations, LastPass MFA adds an additional layer of security on top of your endpoints to maximise security.

Secure Password Vault

Built with strict security standards, we keep millions of accounts safe—encrypting data locally so even we can't see your passwords.

All-in-one Solution

Generate strong passwords, store account info, autofill logins, share credentials, and more with one easy-to-use solution.

Regular Audits and Penetration Tests

LastPass engage trusted, world-class, third-party security firms to conduct routine audits and annual testing of the LastPass service and infrastructure.

At-a-Glance

LastPass stores your most sensitive data and information, security and privacy are non-negotiable. Communicating clearly, transparently, and frequently on data security and privacy is critical to earning your trust.

Key Benefits

Centralised Administration
Provides users with oversight and control over user access, policies, and password strength across the organisation.

Cross-platform access
Synchronises the vault across all devices and browsers, including desktop, mobile, and web.

Enhanced Security
Includes multifactor authentication (MFA) options like biometric and context-aware MFA, passwordless login via the LastPass Authenticator, and alerts for compromised accounts through dark web monitoring.

User-friendly experience
Aims to reduce friction for employees with features like one-click logins and passwordless access, while still maintaining strong security.

Integration
Integrates with other identity and access management tools, such as AD, Azure AD, and Okta, for simplified onboarding and offboarding.

Contact Wycom:

Location:
1/20 Donaldson St,
Wyong NSW 2259

Call Us:
02 4351 1361

Email Us:
info@wycom.com.au

Website:
www.wycom.com.au

Published: October 2025

LastPass Features

Feature	Details
Central Admin Console	The admin dashboard offers automated user management, policies, diagnostic dashboards and more.
Universal Password Management	Simplify access to all apps as well as generate and automatically capture, store, and fill credentials for any login.
User Integrations	Automate onboarding and offboarding, group management, federate, and more with AD, Azure AD, Okta, OneLogin, Google Workspace, PingOne, PingFederate, or a custom API.
100+ Security Policies	Enforce best practices and control password behaviour across the business
Detailed Security Reports	Tie actions to individuals with automated, detailed reporting that helps your business maintain compliance. Dive even deeper with SIEM integrations including Splunk and Azure Sentinel.
Secure Password Sharing	Give teams a flexible, safe way to share access to apps without sacrificing accountability or security.
Dark Web Monitoring	LastPass monitors your employees accounts and sends them an alert if information is compromised to keep their accounts safe.
Advanced Multi-Factor Authentication	Access to the LastPass Authenticator application that secures cloud and legacy apps, VPNs, and workstations with passwordless access. Granular geofencing, time and IP address policies to enable admin control and increase security.
Single Sign-On	Make critical business tools accessible to employees with simplified access to up to three cloud applications
Families as a Benefit	Employees will be provided a personal LastPass account, including 5 additional licenses to share with their family or friends, granting password protection with LastPass

Additional Features

Feature	Details
LastPass Advanced Single Sign-On	LastPass Single Sign-On simplifies employee access to an unlimited number of cloud applications, while streamlining provisioning cloud applications for IT– all in the same application that they trust to store their passwords. With single sign-on for top priority apps, and password management to capture and secure everything else, LastPass protects every access point and conveniently connects employees to their work.

Wycom Technology Pty Ltd
ABN: 63 150 235 144
Phone: 02 4351 1361 **Email:** info@wycom.com.au
Website: www.wycom.com.au