LastPass ••• | MFA

Solution Overview

LastPass MFA is a smarter way to authenticate

Authentication solutions are evolving rapidly as businesses transition to a cloud-centric, BYO-focused workplace. Employees understand the need for security, but they expect technology to be simple, convenient and fast. With decreased visibility and increased complexity, IT is more challenged than ever to manage authentication across a hybrid environment without disrupting end users.

When poor passwords cause 81 percent of data breaches, it's clear that passwords alone won't protect your business. How can you ensure critical information is secure, without adding friction for users? Two-factor authentication (2FA) is a great starting point, but a one-size-fits-all authentication approach does not work when users have different behaviors, personal devices, levels of access and attributes.

LastPass MFA protects your business with today's leading technology while simplifying the login experience for employees. LastPass MFA goes beyond standard 2FA to ensure the right users are accessing the right data at the right time, without any added complexity. With a unique security-by-design model, LastPass MFA ensures biometric data remains private and secure, while leveraging human and hidden factors to identify and authenticate users. LastPass MFA offers an intuitive multifactor experience that's easy for admins to deploy and effortless for employees to adopt.

Adaptive authentication that adapts with users

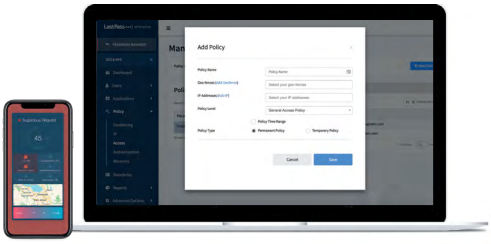
By combining biometric and contextual intelligence, LastPass MFA proves a user's identity with a combination of factors, without increasing the friction of the login experience. The user proves they are who they say they are with human factors like face, fingerprint ID, voice, and iris. The device also proves who they are behind-the-scenes with hidden factors like phone location or IP address, all while providing a passwordless experience.

Passwordless access

Passwords are an unending source of frustration and risk. Using biometrics and adaptive authentication, LastPass MFA can eliminate passwords and streamline employee access to work applications to improve productivity.

Simple deployment for IT teams

LastPass MFA is quick and easy for IT to deploy, with no additional training or services required. LastPass MFA delivers security quickly while saving time and resources on password resets and access issues.



Zero-knowledge security model

Adaptive authentication

Simple deployment & management

Comprehensive security controls

Version 2 | 版一
www.version-2.com

Hong Kong
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

Taiwan
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

Frictionless user experience

Extra security shouldn't be a blocker for employee productivity. LastPass MFA secures every access point – from legacy, mobile and cloud apps to on-premise applications. LastPass MFA authenticates users seamlessly across all their devices, allowing IT to pick and choose authentication methods – from SMS to push to adaptive – for ultimate flexibility and support for all use cases.

Centralized, granular control

Protect your business with an extensive list of policies to manage users at an individual, group and organizational level. Set granular policies, like specifying an app that can only be accessed from certain locations or at certain times. Everything is managed from a centralized, easy-to-use admin dashboard.

Plug-and-play integrations

Automate user provisioning by integrating with user directories like AD, Azure AD, Okta and OneLogin. With easy setup and minimal day-to-day management, LastPass MFA scales as your business evolves.

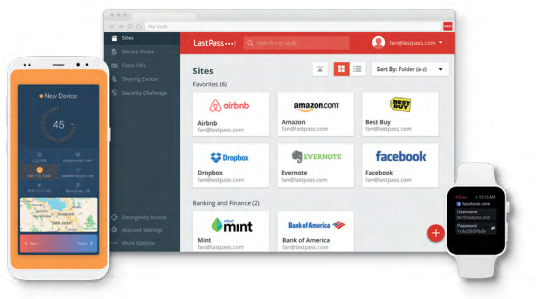
All-in-one authentication solution

With support for cloud, mobile and legacy on-premise apps, LastPass MFA manages authentication for every critical business application from a single interface. IT teams can centrally manage authentication across the organization with visibility into every login, from one platform.

Security by design

LastPass MFA is built to keep data private and secure. Biometric data is encrypted at the device level and never leaves the user's device. It's never stored in a central location that could be compromised, protecting biometric data from server-side attacks.

Contact us today to learn more.



Version 2 | 二版
www.version-2.com

Hong Kong
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

Taiwan
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw