LastPass ••• |
by LogMeIn

Solution Overview

LastPass MFA offers a passwordless experience for users

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 80 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 secure biometric authentication while simplifying the login experience for employees. LastPass MFA ensures the right users are accessing the right data at the right time, without any added complexity across web and legacy applications, VPN and workstation. With a unique security-by-design model, LastPass MFA ensures biometric data remains private and secure, while leveraging biometric and contextual factors to identify and authenticate users - even if they are offline. LastPass MFA offers a passwordless 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 biometric factors like fingerprint or face ID. The device also proves who they are behind-the-scenes with contextual 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 includes a step-by-step guide for a seamless deployment; no additional training or services required. LastPass MFA delivers security quickly while saving time and resources on password resets and access issues.

Adaptive authentication

Fingerprint and face ID biometrics

Location, device and time-based security controls

Seamless deployment, management and experience

Web and legacy apps, VPN and workstation

Frictionless user experience

Extra security shouldn't be a blocker for employee productivity. LastPass MFA secures every access point – from legacy to cloud apps, VPN and workstation. LastPass MFA authenticates users seamlessly across all their devices, for flexibility in how your organization manages authentication.

Centralized, granular control

Protect your business with an extensive list of contextual 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, legacy, on-premise apps, VPN and workstation, 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.

These features deliver the control IT needs and the convenience users expect:

Adaptive authentication	Combine biometric and contextual intelligence to build individual user profiles and adapt authentication to different scenarios.
Biometric authentication	Authenticate users based on who they are with factors such as fingerprint and face ID.
Contextual policies	Leverage location, device ID and IP address contextual policies to verify the legitimacy of a login attempt.
Central admin dashboard	The admin dashboard gives IT a unified view of access across the business and centralizes management of users, policies, reporting and more.
Extensive integrations	LastPass MFA manages authentication for cloud, legacy and on-prem apps, VPN and workstaiton to secure critical business resources in a single interface.
Detailed security reports	Tie actions to individuals with automated, detailed reporting that helps your business maintain compliance.

Visit www.lastpass.com/multifactor-authentication to learn more