LastPass •••|

PRODUCT OVERVIEW

Secure your Identity Provider with LastPass Advanced MFA

As businesses move to support a hybrid workforce and cybercrime continues to rise, securing all entry points to a business is crucial to reduce the risk of a successful data breach. However, passwords alone won't secure your business. With 80% of data breaches being due to weak or reused passwords, businesses require an additional layer of security to ensure their sensitive information remains secure.

By adding Advanced MFA on top of your LastPass Business solution, your business can secure all access points with multi-factor authentication to reduce the risk of a successful breach. Advanced MFA ensures that all endpoints – including, VPNs, workstations, cloud & legacy apps, and identity providers – remain secure.

Securing Azure Active Directory & Active Directory Federated Services (ADFS)

With Advanced MFA, your business can add a second layer of authentication on top of your employee logins to Azure AD or ADFS to ensure that only the right individuals are accessing these resources. As many businesses rely on their identity providers for secure access to sensitive information, ensuring that this access is secured with multi-factor authentication is a best practice recommended by experts. Once granted access to Azure AD or ADFS, nefarious actors would be able to access a wide range of configured applications – risking data loss or sensitive information becoming exposed.

By adding multi-factor authentication on top of an identity password, your employee will be prompted on a secondary device to confirm their identity – reducing the risk of a successful data breach.

LastPass Advanced MFA

LastPass Advanced MFA 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 maximize security.

	ADVANCED MULTI-FACTOR AUTHENTICATION
Price	$3 user/month
Overview	Provide multi-factor authentication protection on the password vault, single sign-on applications, VPNs, workstations, and third-party identity providers with the LastPass Authenticator application. Additional passwordless policies, such as geofencing and IP address policies.
Reporting	Automated, detailed reporting on MFA user and admin activity
Biometric	Authenticate users based on who they are with factors such as fingerprint and face ID
Authenticators Supported	LastPass Authenticator
Authentication Methods	Biometric, pin code, time based 6-digit codes, one-tap push notifications
Endpoints	LastPass Vault, cloud apps, legacy apps (Radius/LDAP), VPNs, workstations, 3rd party Identity Providers (Azure AD & ADFS)
Cloud Apps	Authentication provided
Policies	Granular geofencing, time and IP address policies to enable passwordless access to SSO apps, VPNs, or workstations.
Contextual intelligence	Intelligent authentication based on login context: location, device, and network
Adaptive authentication	Warn users on Authenticator app if login information is not aligned with previous behavior
Passwordless	By using biometrics and adaptive authentication, LastPass Advanced MFA eliminates passwords on VPN and workstations

Get in Touch

Learn more about LastPass Advanced Multi-Factor Authentication.