onelogin by ONE IDENTITY

PRODUCT DATASHEET

# OneLogin Multi-Factor Authentication

Simple, secure authentication for all your users

With brute-force and phishing attacks on the rise[1], implementing strong authentication can mean the difference between successfully blocking a potential attack or falling victim to a devastating data breach. Simply relying on a username and password alone to verify a user's identity does not provide adequate protection for the applications and data that are critical to running your business.

**OneLogin Multi-Factor Authentication**

OneLogin Multi-Factor Authentication (MFA) prevents unauthorized access to critical corporate data by prompting users for an additional factor before they are granted access. Quickly enable seamless yet secure authentication experiences by enforcing security policies, like password complexity and IP restriction, and user-friendly authentication factors, such as SMS or OTP push. Protect your entire business with MFA or start by securing your most critical applications first.

## KEY BENEFITS OF ONELOGIN MULTI-FACTOR AUTHENTICATION

### Defend against account compromise

Dramatically improve your security posture by adding MFA in front of corporate applications to protect against unauthorized access obtained through brute force and phishing attacks.

### Choose your own factors

OneLogin helps organizations select the right authentication factor for their users. Choose from a variety of factors including:

- OneLogin Protect
- SMS
- Voice
- Security Questions
- Email MFA
- Biometric Factors via WebAuthn
- 3rd Party Factors (Duo, RSA SecurID, Symantec, etc.)

### Deploy flexible security policies universally

Enforce strong, sophisticated authentication with granular policies for different users and apps. Add risk-based SmartFactor Authentication™ to adjust MFA requirements, while still protecting users against cyber attacks.

### Enable quick & simple end-user authentication

Provide a seamless MFA experience for your users to encourage adoption and decrease support requests. Authentication options like biometrics and OTP push alleviate painful MFA.

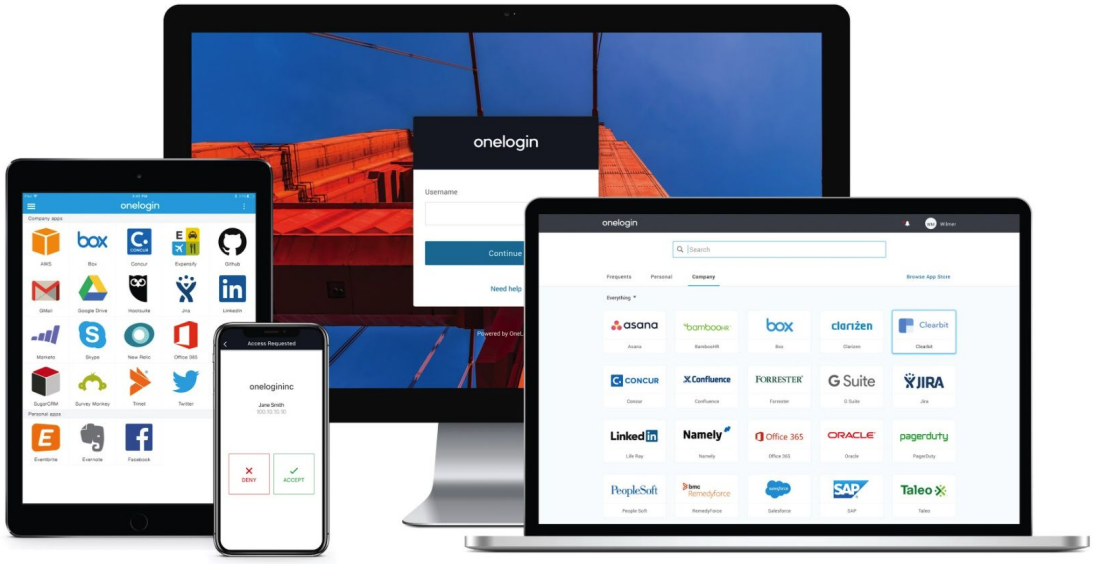
### Gain visibility into new login attempts

Access our standard and custom reports or stream events in real-time to SIEM tools to monitor login activity and track failed authentication attempts, the type of factors used to authenticate, plus much more.

"The team could deliver an effective replacement for the 2FA solution we already had. This meant the previous expensive, aging software and hardware tokens could be removed and the integration of cloud systems move ahead."

**NEIL DAVISON** | IT Director, Farrer & Co

*1. According to the 2020 Verizon Data Breach Investigations Report, over 80% of breaches within hacking involve brute force or the use of lost or stolen credentials.*
*2. SmartFactor Authentication is a separate offering that includes all MFA features with the addition of risk-based authentication. Learn more at onelogin.com/product/smartfactor-authentication*




## ONELOGIN MULTI-FACTOR AUTHENTICATION FUNCTIONALITY INCLUDES:

| | |
|---|---|
| **Diverse Authentication Factors** | Choose from a variety of authentication factors, including OneLogin Protect, SMS, Voice, Security Questions, Email MFA, and biometric factors through WebAuthn, such as Windows Hello on PCs and TouchID on Macs, for even stronger protection. |
| **OneLogin Protect** | OneLogin Protect, our free mobile OTP app, provides a seamless, integrated user experience for MFA. Instead of manually entering a time-based code, users simply accept the push notification and automatically get access. |
| **Granular Security Policies** | Assign MFA security policies to individual users or specific applications to protect sensitive data. Additionally, specify which authentication factors are required per the user or app policy. |
| **Multi-MFA Configuration** | Define multiple configurations of an authentication factor per tenant. For example, two configurations of OneLogin Protect for different user groups, one allowing backup/restore, and another one disallowing backup/restore. |
| **Password Blacklist** | Block keywords and strings to prevent employees or customers from using common or insecure passwords schemes that are easily compromised. |
| **Authentication APIs** | OneLogin provides a rich set of APIs, such as MFA registration and Generate Token APIs, allowing you to flexibly manage and add enterprise-grade MFA to any application. |
| **Third Party Integrations** | OneLogin also supports commonly-used authentication factors like Duo Security, RSA SecurID, Symantec, Google Authenticator, and Yubikey. |

**Over 2,500 enterprise customers globally secure their applications with OneLogin**

AAA AIRBUS pandora Steelcase STITCH FIX