PROXIMIA®

18x Faster Access Than Traditional MFA



PROXIMIA
Face + Silent Second Factor

~2 Seconds

up to **34 Seconds** saved per login

Password Only	**6x** Slower ~8-12 Seconds .9 FTE	**153** Hours saved per month
Password + Push MFA	**10x** Slower ~15-20 Seconds 1.6 FTE	**275** Hours saved per month
Password + OTP (App/SMS)	**18x** Slower ~24-36 Seconds 3 FTE	**519** Hours saved per month

Estimates based on 250 users, 10 logins per day / per user, 22 business days per month

Timing based on internal testing under standard conditions: Proximia users utilizing an integrated camera for bioauthentication and the XiFi™ Card for second factor. Referenced login time ranges come directly from Microsoft Security Blog (2019), Duo Security Authentication Timing Report (2020), Google Security Blog (2021), FIDO Alliance UX Study (2022), and NIST SP 800-63B Usability Guidance. For calculation purposes, the upper end of each industry-published timing range was used to reflect realistic real-world workflows rather than best-case conditions. Actual results may vary based on device performance, network latency, workflow patterns, and security policy requirements.

The Hidden Cost of Passwords and MFA is Massive

Logins are only the start. Password resets, lockouts, MFA prompts, account recovery workflows, and breach containment consume huge amounts of time—and the burden hits both users and IT. **Proximia eliminates these slowdowns everywhere** they occur.

Eliminate 100% of Password Reset & Lockout Tickets

~1,826
hrs/month saved from login & IT workload

~11
FTE of productivity reclaimed per month

20-50%
fewer IT support tickets

Lower
breach likelihood & response overhead

Take your time back!

~40 hours lost to cognitive recovery = user productivity

Every login event creates ~30–90 seconds of cognitive recovery time as users reorient to the task they were performing.

~30 hours of user & IT time lost to resets & MFA lockouts

Today's MFA means support tickets. **Password resets + MFA lockouts create ~660 hours per month in avoidable IT handling and user downtime.**

~13 hours of IT time lost to security alerts & reviews

Identity alerts consume time — even when no breach occurs. **IT spends ~150–300 hours monthly on suspicious logins and activity.**

Estimates are per day; based on 250 users, 10 logins per day / per user, 22 business days per month

Referenced estimates come directly from Gartner Service Desk Benchmarks, Forrester IAM Study, Microsoft ITID Telemetry Reports.

Fastest Access. Highest Security.

Proximia delivers unmatched convenience and continuous protection—reducing wasted login time while increasing compliance and user satisfaction.

TRUE ZERO TRUST ARCHITECTURE

proximia.com | **sales@proximia.com**
(844) GET-PROX or **(844) 438-7769**

PROXIMIA®

© Proximia, all rights reserved.