

How Proximia Delivers **True** **Passwordless** Security



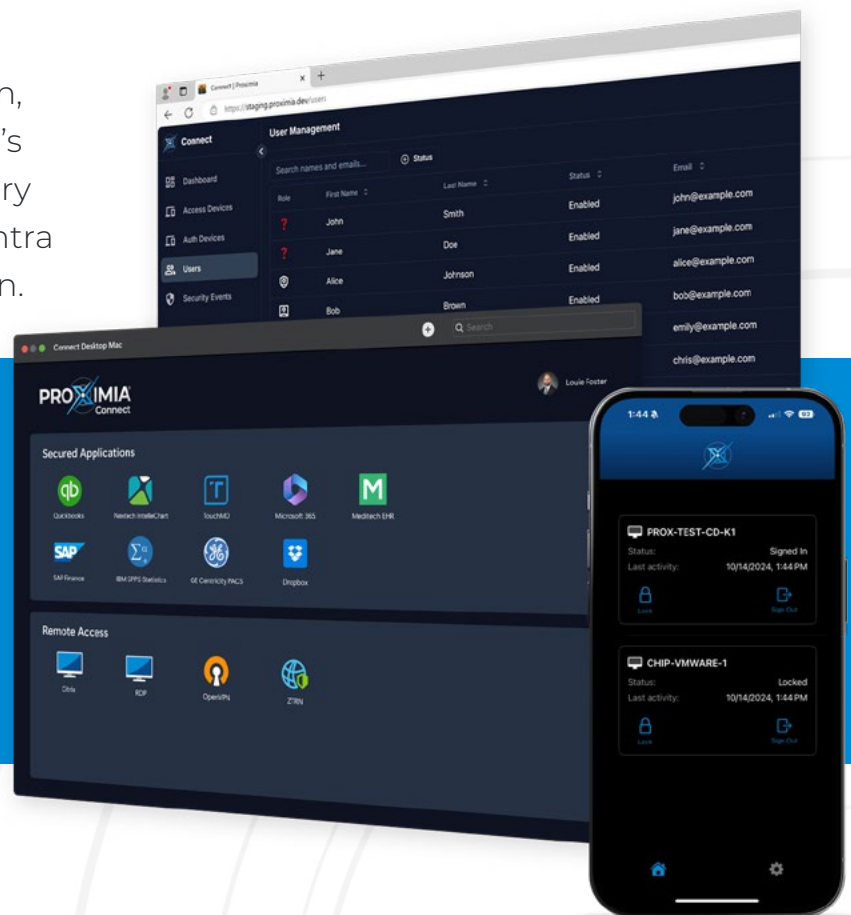
How Proximia Delivers True Passwordless Security

Passwords are inadequate for modern cybersecurity. Passwords place a heavy load on IT with constant resets and lockouts, misuse issues, and risky password practices, while also frustrating end users. This translates to significant friction and a cumbersome experience for users and IT staff.

Proximia Connect enables true passwordless login across your entire ecosystem, without limiting access to any single platform or technology suite. Passwordless access is supported across multiple environments, including Windows for both online and offline scenarios, single or multiple users, and across various operating systems, synchronizing with accounts in Microsoft, Google, and HR systems.

Proximia supports Single Sign-On (SSO) through robust authentication and authorization protocols like OAuth, OpenID Connect (OIDC), and SAML. It's also compatible with essential directory services, including Active Directory, Entra ID, LDAP, and supports user federation.

By utilizing advanced biometric triggers, mutual trust, dynamic proximity, and persistence, Proximia redefines what it means to deliver a truly passwordless experience without the need for users to know and manage their passwords.



Device-Agnostic Authentication and Security

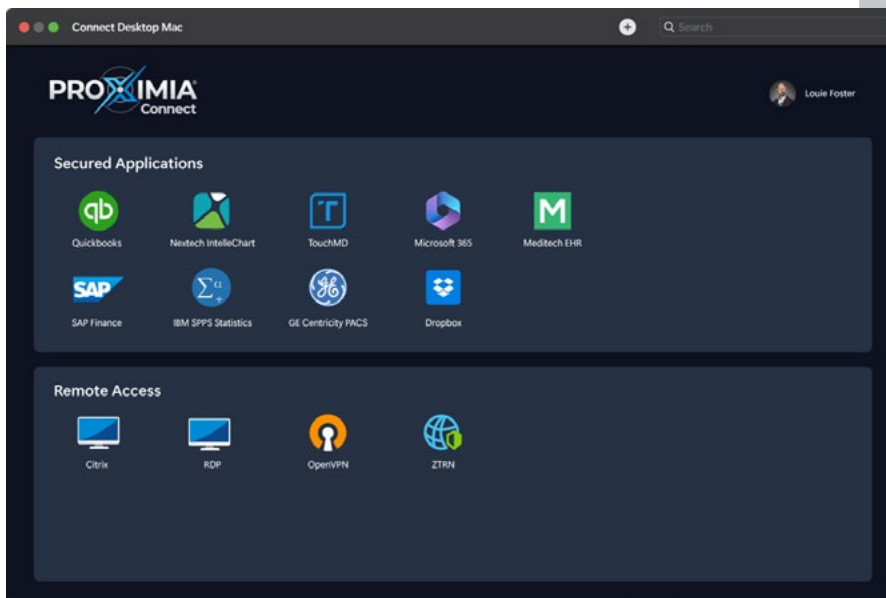
Proximia leverages biometrics such as facial recognition and proximity through various devices, including smartphones, smart wearables, and webcams, to authenticate users securely. By remaining device-agnostic and untethered to specific platforms, **Proximia delivers unparalleled flexibility, seamlessly integrating with existing systems while adapting to emerging technologies.** This approach ensures secure, adaptable protection for today and readiness for tomorrow's advancements.



Seamlessly Extend Passwordless to Legacy Systems

Although legacy systems rely on passwords, Proximia manages these credentials within its secure framework to ensure a passwordless experience for the end user. Legacy applications, by definition, cannot adopt modern authentication technologies like OAuth, OIDC, SAML, or user federation.

Proximia addresses this by handling authentication invisibly in the background, interacting with the legacy system on the user's behalf, **while extending its full protections – biometric triggers, dynamic-proximity, mutual trust, and persistence – to legacy system authentication.** This approach effectively mitigates the risks of credential stuffing, phishing, and other password-based attacks, while maintaining a smooth user experience.



Achieving Passwordless Security Without Adding Complexity

A centralized administration console simplifies IT management, allowing administrators to efficiently manage user profiles, access requests, and compliance protocols. Proximia's login functionality is fortified against modern threats, such as brute force attacks, clickjacking, cross-site forgery, and SQL injection, with all credentials encrypted in transit and at rest.



By eliminating static credentials, businesses reduce their attack surface, streamline compliance, and provide a more seamless user experience. Proximia's adaptive, passwordless approach integrates effortlessly with both modern and legacy systems, delivering on the promise of advanced, **Zero-Trust authentication without complexity or compromise.**

