How Proximia Takes You *Truly* Passwordless

Most “passwordless” solutions still keep passwords in the background. Proximia removes them from the user experience entirely.

This guide explains how Proximia delivers true passwordless authentication across Windows, modern apps, and even legacy systems — and why our approach is fundamentally different from password managers, SSO tools, and traditional “passwordless” products.

Why Passwordless Hasn’t Meant Password-Free — Until Now

Many tools promise “passwordless,” but behind the scenes they still rely on passwords — either stored in a vault, routed through SSO, or held as fallback credentials. This creates a false sense of passwordless security while preserving the largest attack surface: the human handling of credentials.

Proximia takes a different approach.

Passwords are:

- Reused, phished, stolen, and shared
- A top cause of breaches and session compromise
- A major drain on IT through resets and MFA lockouts
- A daily productivity tax on employees

Proximia Delivers True Passwordless

Proximia replaces the user's relationship with passwords entirely — at Windows login, across cloud applications, and even inside legacy systems.

True Passwordless Windows Login

No user ever sees, types, or knows a Windows password.

They authenticate with:

- A biometric (integrated or external camera, or mobile device)
- A trusted proximity device (XiFi Card or phone)

Where the OS requires password-format credentials, Proximia generates and manages them invisibly.

Unified, Enterprise Credential Handling

Proximia manages credentials centrally and injects them automatically when applications launch.

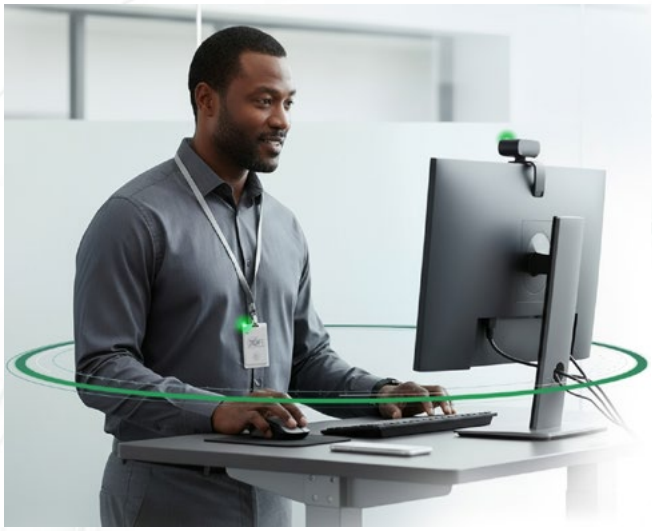
- Users never type or manage passwords
- IT controls credential rotation and mapping
- Works across web, local, thick-client, and on-prem apps

Continuous Protection After Login

Unlike traditional systems that "trust" a session once it begins, Proximia continuously verifies:

- **Presence:** the user is still physically there
- **Proximity:** their trusted device is active and nearby
- **Mutual trust:** both user and device re-verify each other

If proximity is broken, the session locks instantly.



What Makes Proximia Different

With Proximia, users never know or create passwords

Proximia eliminates passwords from the user experience entirely. Authentication happens through biometrics bound to a trusted device. No credentials to remember, type, or forget.

Where legacy systems require them, Proximia auto-generates, rotates, and injects them. Invisible to users and useless to attackers.

- No password vault to breach
- No credentials to phish
- No fallback to passwords during outages
- No user-known secrets to reuse or share

Password managers and SSO still depend on passwords

Password managers

- Auto-fill real passwords
- Store them in a vault (a high-value target)
- Still require passwords for legacy apps
- Expose credentials to phishing if users are tricked

SSO

- Simplifies logins but still uses passwords underneath
- Pushes passwords into legacy systems during federation
- Falls back to passwords during outages or MFA exceptions

Proximia delivers true passwordless with no fallback

Proximia delivers passwordless authentication without the safety net of hidden passwords. Users authenticate with biometrics and proximity, not phone-based tokens or codes.

- No user-known password exists to fall back to
- Biometrics plus proximity, not phone-only MFA
- No fallback passwords for attackers to phish
- Continuous authentication protects sessions, not just login events

Traditional “passwordless” still falls back to passwords

Most modern passwordless offerings

- Use phone-based authentication or tokens
- Still require passwords as a fallback when something fails
- Depend heavily on a phone (creating operational gaps)
- Do not protect the user *after* login

Proximia is the only system that solves modern *and* legacy authentication

Proximia functions as an enterprise-grade credential vault built for complex environments. System-managed and invisible to users, it delivers a seamless experience while legacy systems get the credentials they require.

- Automatic credential injection
- System-generated, rotating passwords
- Scripting support for custom workflows
- Consistent experience across cloud, on-prem, and offline systems

Legacy apps break other passwordless solutions

Legacy systems still require username and password fields, local login stores, and shared departmental credentials. This creates gaps that other passwordless solutions cannot bridge.

- Users fall back to manual password entry
- Credentials get shared or written down
- Passwordless rollouts stall at legacy boundaries

Proximia delivers continuous authentication, not point-in-time checks

Proximia continuously verifies presence by binding identity to a trusted device. Sessions stay protected from login to logout, not just at the front door.

- Auto-lock when users walk away
- Protection against tailgating and shared workstation misuse
- Session hijacking prevention
- Token replay attack protection

Most MFA verifies once, then goes blind

Traditional MFA and passwordless systems verify the user once at login. After that, the session is unprotected.

- No awareness of whether the user is still present
- Sessions remain open when users walk away
- Shared workstations expose active sessions to misuse
- Attackers can hijack or replay tokens after login

WHY THIS MATTERS

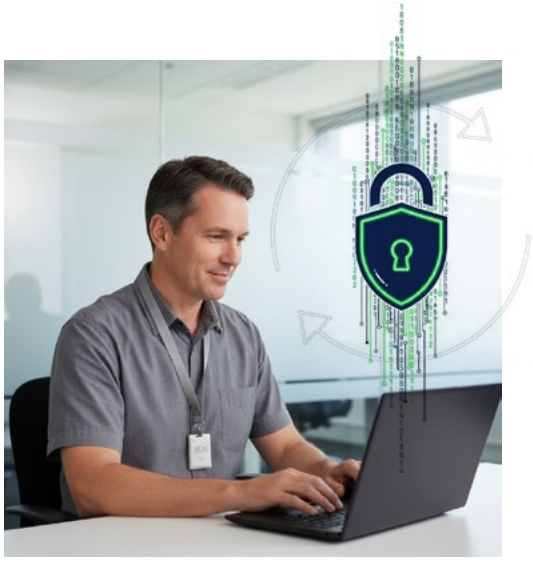
The Technical Truth About “Passwordless”

Some systems still require passwords at the protocol level

Certain Windows flows, RDP, LDAP, and legacy clients need password-format credentials. But that doesn’t mean users have to deal with them.

With Proximia, users never know, manage, type, or reset passwords. Behind the scenes, Proximia:

- Generates credential-format secrets only when needed
- Rotates them automatically
- Encrypts and injects them without user involvement
- Ensures temporary secrets expire before attackers can use them



THE RESULT

True Passwordless Across the Entire Ecosystem

With Proximia, organizations achieve:

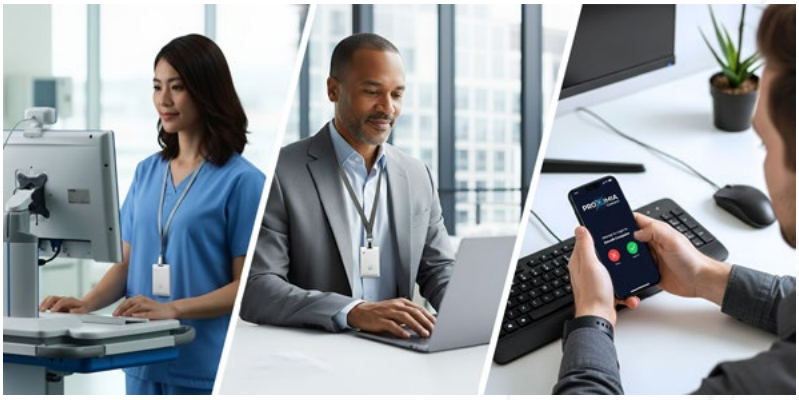
Zero user-managed passwords (Windows + apps)

Phishing-resistant authentication by design

Continuous, presence-aware session protection

Unified login experience across cloud, on-prem, offline, and legacy systems

Faster access with dramatically less IT overhead



This is not just a better login.

It’s a fundamentally different identity model.

Proximia eliminates passwords from your workforce — not just hides them.

	Password Managers/SSO	Traditional "Passwordless"	**Proximia** True Passwordless
User Passwords	Stored in encrypted vaults	Hidden but exist in backend	**Never exist - users never create passwords**
How It Works	Auto-fills passwords for users	Phone app generates tokens	**Cryptographic keys + biometrics**
Authentication Methods	Master password + MFA	Phone-dependent (SMS/Push/App)	**Flexible: camera, phone, or badge**
Legacy System Support	Injects actual passwords	Requires separate password management	**Generates temporary system credentials**
When Primary Method Fails	Manual password entry	Falls back to passwords	**Alternative biometric or badge**
Session Security	Password sent at login	One-time verification at login	**Continuous proximity verification**
Attack Surface	Vault breach exposes all passwords	Password fallbacks, session tokens	**Only public keys (useless to attackers)**
IT Overhead	Manage vaults, password policies, resets	Manage tokens, MFA exceptions	**No password management needed**
Phishing Risk	Master password can be phished	Fallback passwords can be phished	**Nothing for users to give away**
Shared Workstations	Complex to manage	Limited support	**Seamless user switching**
Compliance Burden	Password rotation, vault audits	MFA exceptions, fallback tracking	**Automatic audit trail, no exceptions**
User Recovery	Password reset, security questions	Password reset or backup codes	**Biometric re-enrollment**

Take the next step toward true passwordless.

Protect your workforce. Simplify your stack. Eliminate the risk.

TRUE ZERO TRUST ARCHITECTURE

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

PROXIMIA®