Passwordless Agent Authentication

Journey

Frictionless, Secure Login to SSO

Password resets are the top agent support issue for contact centers. Agents spend approximately 11 hours a year doing password resets. Forrester estimates the average IT help desk password reset cost a business $70 and cost a large company $1 million per year. [1]

Passwords and other text or knowledge-based credentials suffer from a variety of flaws. They're inherently subject to being shared, forgotten, and stolen, which creates security risks and operational expenses. Modern hacking techniques, and methods of counteracting them with a regular rotation of passwords and one-time passcodes, have made the process more burdensome for the agent and more expensive to maintain and manage. With a global shift to working from home, the need to trust who is accessing a device and a network is more critical than ever.

Replacing passwords with facial biometrics eliminates password resets while improving IT security, eliminating friction from the agent experience and decreasing operations costs.

Easily integrated into any agent desktop, Journey's biometric SSO login replaces the username and password, either from the agent desktop camera or by having the agent scan a QR code with their mobile phone to capture their facial biometric. Biometric enrollment takes less than 10 seconds: an email to the agent's corporate email address with a URL that uses the camera to scan the agent's face to create the facial biometric. Note: the facial biometric is not a picture but a set of artifacts that cannot be reconstituted to create a face.

Passwordless Agent Authentication works for both on-prem and remote agents. This solution is fully integrated with existing SSO capabilities or can interwork with existing SSO solutions directly using SAML or OAuth.

1 Forrester Research: Best Practices: Selecting, Deploying, And Managing Enterprise Password Managers

Key Benefits

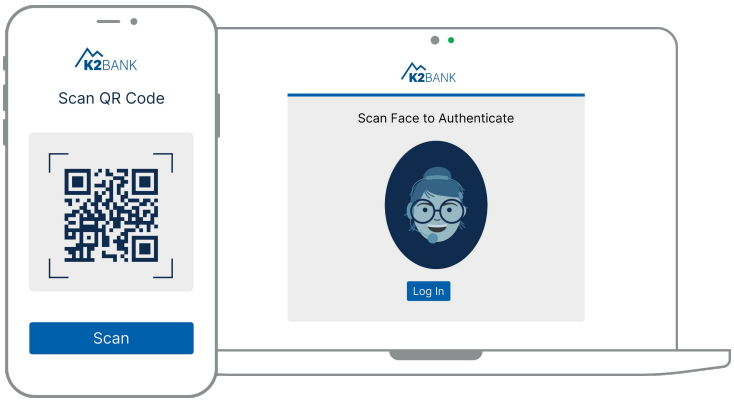
1. Eliminate password reset calls to the IT Help Desk, saving on average $70/reset
2. Employee experience with frictionless login
3. Stops credential sharing, credential stuffing, and keylogging security attacks
4. Facial biometric and proof of liveness cannot be stolen through social engineering
5. Includes identity proofing, transaction signing, and federated SSO
6. Account recovery is a simple matter of re-enrollment using the identity proofing process
7. Journey's Zero Knowledge Network® protects employee information and the security of corporate data

Security, Employee Productivity, and Operational Efficiency

Rather than relying only on something your employees **know** (like a password or employee ID, which can be lost, stolen, shared, or forgotten), Journey is making it possible to log in to corporate assets instantaneously with biometrics. With False Acceptance Rates (FAR) of up to 1:1,000,000 and the elimination of password resets, facial biometrics are the key to a radical impact on security, operating costs, data privacy, and employee experience.

Today, hundreds of millions of employees login using username and password, which creates significant vulnerability for the enterprise, and is surprisingly costly to manage. Underestimate these real and potential costs at your peril. Much is at stake: employee productivity, corporate data security, and your customers' information privacy, for starters. The theft of corporate logins has resulted in some of the most devastating data breaches in the past couple of years.

The key to tackling this vulnerability is replacing passwords with biometrics, which makes the employee and agent login fast, easy, and impossible to lose or steal. Protecting your business from fraud and reducing costs related to password resets and account recovery makes this a robust business case with a quick ROI.



If you'd like to explore how passwordless agent authentication can improve your efficiency and security, get in touch with us at info@journeyid.com.

Tangible Business Results

- **Save $70 - $80** on average for each password reset with your IT helpdesk.
- Document centric identity verification supplemented with a biometric match provides **1:million veracity**.
- Logging in takes **less than 1 second**, and avoids low-security knowledge based authentication, which can be easily lost or stolen.
- **Bolster compliance** with consumer data privacy regulations, banking regulations, and internal quality and security measures.
- **Easy integration** with no code or low code options, and scalable to even the largest enterprises globally.
- Thousands of document IDs accepted and easy to create a template of a corporate ID for document centric **verification anywhere in the world**.