

SOLUTION BRIEF

Entrust IDV Integration With Okta Workforce Identity



Verify the Real Person Behind Every Employee Account

Overview

Entrust and Okta protect the workforce by verifying the real person behind every high-risk action – not just their credentials. By integrating Entrust's AI-powered biometric and document verification with Okta Workforce Identity, organizations can gain an additional layer of identity assurance at the moments employees are most vulnerable: onboarding and account recovery (password recovery, account unlock, and authenticator enrollment or unenrollment). Administrators enforce real-world identity proofing through the Okta account management policies they already manage.

The Challenge

As organizations shift toward a borderless, remote-first workforce, the traditional Know Your Employee (KYE) model has reached a breaking point. Protecting the business is no longer about guarding a physical building; it's about having certainty that the person behind the screen is who they say they are.

That certainty is harder to achieve as AI-driven fraud outpaces the manual, high-cost processes used to fight it. When verification is slow and expensive, it holds employees back and, more critically, leaves the enterprise exposed to identity-based breaches. For organizations running Okta Workforce Identity, policy already determines when a credential change requires additional assurance. Entrust adds the identity proofing that confirms the person behind the request.

Rising AI-driven fraud and sophisticated attacks:

The surge in identity theft, synthetic fraud, and account takeovers proves legacy security and manual processes can't keep pace with AI-driven threats. By weaponizing generative AI to create highly convincing deepfake hires, "ghost" employees, and realistic social engineering scripts, fraudsters are finding the path of least resistance into the heart of the enterprise, turning trusted employees and IT help desks into unintended entry points.

Operational inefficiency and high IT costs: Manual identity processes increase operational costs and workload for IT teams. When staff spend time on routine tasks like verifying employees or resetting credentials, it creates support delays that stall employee productivity. These bottlenecks prevent IT from focusing on high-value initiatives that move the business forward.

High-friction employee experience: Redundant identity checks in legacy systems create frustrating hurdles at the moments employees need access most, from their first day of onboarding to every account recovery event. New hires can face delays while waiting to verify their identity, while account recovery challenges can keep employees from getting back to work quickly.

Benefits

- **Stops identity-based attacks at the moments employees are most vulnerable**
- **Frees IT from manual identity checks with Okta policy-driven automation**
- **Accelerates workforce access with a verification experience employees trust**



The Solution

Entrust integrates AI-powered biometrics and document verification directly into the Okta moments where identity assurance matters most. Okta policy determines when verification is required, Entrust IDV verifies the real person, and Okta enforces the result. By replacing manual identity checks with policy-driven verification, organizations stay ahead of sophisticated, AI-driven threats while improving operational efficiency and the employee experience.

HIGHLIGHTS

Benefits

Stop identity-based attacks at the most vulnerable moments: Secure the most vulnerable stages of the employee lifecycle by verifying the real person – not just their credentials. Anchoring identity to a government-issued ID and a biometric liveness check neutralizes AI-driven threats such as deepfakes, synthetic identities, and “ghost” employees. Verification is applied at onboarding and at every account recovery event, so credential changes proceed only when the real employee is confirmed.

Free IT from manual identity verification with Okta policy-driven automation: Replace costly, high-risk help desk calls with self-service identity verification enforced through Okta’s account management policies. Employees resolve password recovery, account unlock, and authenticator enrollment or unenrollment on their own, without a ticket or a callback. Automating these high-volume tasks allows IT teams to scale security operations while accelerating the time it takes to verify users and restore access.

Accelerate workforce access with a verification experience employees trust: From onboarding to account recovery, provide fast, frictionless verification at the moments that matter most. Entrust’s AI-driven verification returns a decision in seconds, so employees complete the check and move on rather than waiting on someone else to confirm who they are. The verification flow feels like a natural extension of the Okta sign-in experience. New employees gain verified access on day one, and employees can quickly restore access when account recovery is required.



The Entrust Difference

Entrust provides a high-assurance identity foundation that secures workforce moments most vulnerable to impersonation. By bridging the gap between physical identity and digital access through integration with Okta Workforce Identity, Entrust enables a secure, borderless workforce. This approach anchors every policy decision in a verified, real-world identity.

We build the documents we verify: Entrust has manufactured passports, national IDs, and driver's licenses for governments around the world for decades. That means every verification is anchored in authoritative, first-party knowledge of how genuine identity documents are made and secured.

Multi-layered defense against deepfakes, spoofs, and injection attacks: Stop advanced identity threats with iBeta-validated, ISO 30107-3 PAD Level 1 and Level 2 conformant liveness detection. Entrust blocks printed photos, screen replays, and 2D and 3D masks, and detects digital injection attacks and AI-generated deepfakes in real time, confirming that biometric data comes from a live, physically present person.

Flexible biometric options to stop account takeover: Account recovery is one of the most targeted moments for account takeover. Entrust offers three biometric authentication methods rather than limiting administrators to one: Face Authentication for fast, real-time face match, Motion Authentication for the highest-assurance moments, and Biometric Passkeys for FIDO2-based, phishing-resistant authentication, so administrators can match the method to their organization's security posture and compliance requirements.

Intelligence-led fraud prevention: Our in-house Fraud Lab replicates emerging attack patterns across document and biometric fraud, from forged documents and synthetic identities to deepfake selfies. These insights continuously strengthen our unified fraud engine, helping organizations detect evolving threats before they reach scale.

AI-driven verification in seconds: Entrust's award-winning AI-driven verification returns a clear pass or fail decision in seconds, automatically. This speed matters most when employees can least afford to wait: at account lockouts, password recovery, and day one onboarding. Faster verification lifts completion rates so identity checks stay consistent across the workforce.

Global reach with equitable verification for every employee: Our solutions can verify identities across 195 countries with more than 2,500 government-issued document types, backed by decades of experience navigating regional document standards and regulatory requirements. Built-in bias mitigation ensures fair, high-assurance biometric outcomes across all demographics, so every employee gets the same accurate experience regardless of where they are.



Key Features



Enforce verification through the Okta policies you already manage:

Entrust deploys through Okta's account management policies using a standards-based OIDC integration, so administrators define when verification is required and for which users, entirely within Okta.



Confirm identity at onboarding and every account recovery event:

A government-issued ID scan and biometric liveness check establish the employee's identity at onboarding, and the same policy-driven flow verifies them at account recovery moments including password recovery, account unlock, and authenticator enrollment or unenrollment.



Verify employees without inheriting their sensitive data: ID images and biometric captures are processed by Entrust and are not included in the response sent to Okta, so the organization's Okta tenant never holds sensitive identity data. Configurable retention policies support GDPR, NIST IAL2, eIDAS 2.0, and regional privacy requirements.



An experience designed for the moments that matter most: Whether it's a remote hire on day one or a locked-out employee who needs access now, the experience stays simple from start to finish. Employees verify quickly and get back to work.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.