DATASHEET

Entrust IDV Integration With Microsoft Entra Verified ID

Build Digital Trust Across Your Workforce

OVERVIEW

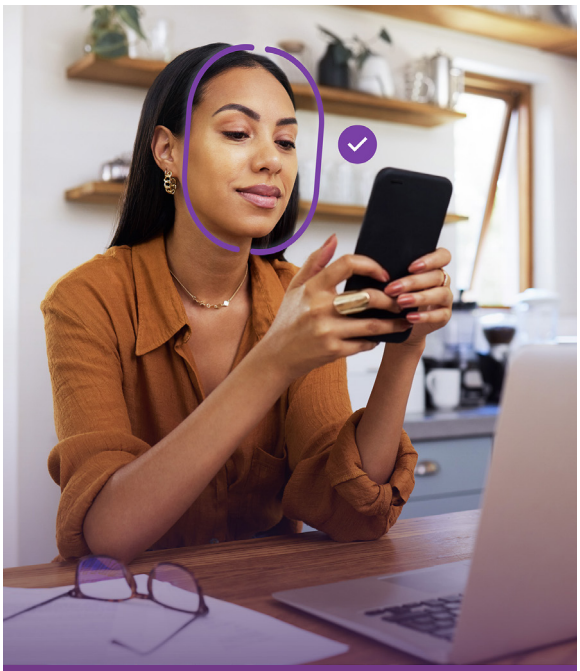
Entrust and Microsoft protect the workforce by bridging world-class identity proofing with a decentralized, privacy-first framework. By integrating Entrust's AI-powered biometric and document verification with Microsoft Entra Verified ID, organizations can establish a high-assurance foundation to secure high-risk moments across the employee lifecycle.

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 is about having certainty that the person behind the screen is who they say they are.

This certainty is harder to achieve as AI-driven fraud outpaces the manual, high-cost processes used to fight it. When security measures are slow and expensive, they create a high-friction experience that stalls employee productivity and – more critically – leaves the enterprise vulnerable to massive data breaches.

Rising AI-driven fraud and sophisticated attacks:
The surge in identity theft, synthetic fraud, and account takeovers proves legacy security and manual processes cannot keep pace with AI-driven threats. By weaponizing generative AI to create highly convincing deepfake applicants, "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.



Benefits

- Establish trust with high-assurance identity verification
- Drive operational scalability through identity automation
- Deliver a frictionless employee experience

ENTRUST
SECURING A WORLD IN MOTION

Operational inefficiency and high IT costs: Manual identity processes drive up 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.

Fragmented and high-friction employee experience: Legacy systems often force employees to navigate redundant identity checks and repetitive data sharing, creating unnecessary hurdles in their daily workflows. Employees now expect a modern experience that allows them to move through the enterprise with ease – from seamless onboarding to enabling instant access to resources.

The Solution

Entrust integrates best-in-class, AI-powered biometric and document verification with Microsoft Entra Verified ID to establish a foundation of digital trust. This partnership secures high-risk moments across the employee lifecycle with real-world identity proofing, protecting critical resources from unauthorized access. By moving beyond legacy passwords and manual verification, organizations can stay ahead of sophisticated, AI-driven threats while improving operational efficiency and the employee experience.

HIGHLIGHTS

Benefits

Establish trust with high-assurance identity verification: Secure the most vulnerable stages of the employee lifecycle by anchoring digital trust with government-issued IDs and biometric data. Binding a physical identity to a digital credential neutralizes AI-driven threats such as deepfakes and "ghost" employees. This ensures that high-privilege actions are gated by a biometric check, providing assurance of the employee's identity.

Drive operational scalability through identity automation: Modernize the help desk by transitioning from manual identity verification to a secure, automated self-service framework. This integration eliminates the delays of manual password resets and physical ID checks. Automating these high-volume tasks allows IT teams to scale security operations while accelerating the time it takes to verify and provide access to users.

Deliver a frictionless employee experience: Enable an intuitive user journey that provides seamless, immediate access to essential systems and resources. Using a "Verify Once, Use Everywhere" model, employees receive a portable Verifiable Credential in their Microsoft Authenticator app, ending repetitive data sharing and redundant identity checks. This decentralized approach respects employee privacy while boosting productivity with instant, verified access.

The Entrust Difference

Entrust provides the high-assurance foundation to secure critical enterprise infrastructure and mission-critical systems. By bridging the gap between physical identity and digital access through integration with Microsoft Entra Verified ID, Entrust enables a secure, borderless workforce. This approach moves beyond simple authentication to establish a permanent, verifiable trust anchor.

Anchor digital trust with best-in-class document and biometric verification: Fight deepfakes and synthetic fraud with superior liveness detection and automated document verification. Our multi-layered defense ensures every digital credential is anchored to a verified, live human being.

Enforce privacy-first security through decentralized data sovereignty: Minimize data liability and help ensure compliance through a "Privacy by Design" architecture where users own their credentials and sensitive PII is purged after verification.

Expand global reach with equitable identity verification: Support a global workforce with coverage across 195 countries and 2,500+ document types, featuring built-in bias mitigation to ensure fair and inclusive biometric outcomes for all employees.

Deliver a frictionless identity journey across the employee lifecycle: Establish a permanent trust anchor with a one-time ID and biometric scan that flows into Microsoft Authenticator, for easy authentication for high-risk actions.

KEY FEATURES

Identity-anchored credential issuance: Following a successful document and biometric check, a digital credential is issued to the Microsoft Authenticator app, cryptographically binding employees to their real identity.

Seamless integration with Microsoft Entra Verified ID: Automate workflows and secure high-risk moments by matching live biometric checks against the user's verified identity anchor.

Privacy-first security: User-controlled architecture ensures privacy and consent. Once verified, users own their credentials and have control over the information to be shared. Help meet GDPR and other compliance requirements while minimizing data liability.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION