



ENTRUST



Entrust Workforce Identity and Access Management (IAM)

Secure your organization with phishing-resistant, high assurance identities, enhancing security while optimizing workforce efficiency and compliance.

Overview

Entrust's Workforce Identity solution secures and manages employee identities across both on-premises and cloud environments. It integrates advanced technologies and processes to authenticate, authorize, and verify users, ensuring appropriate access to corporate resources. This solution is integral to an identity-centric security strategy, leveraging principles of Zero Trust and least privilege to block unauthorized access and significantly reduce the risk of insider threats and data breaches. Entrust's Workforce Identity serves as a critical component in maintaining robust security and operational integrity.

BENEFITS

- Protect against account takeover attacks
- Implement secure access controls aligned with Zero Trust principles
- Real-time risk assessment with adaptive controls
- Support secure, flexible, remote, and hybrid work environments
- Reduce costs with streamlined identity management

KEY FEATURES

- Phishing-resistant passwordless MFA
- High assurance authentication and ID verification
- Risk-based adaptive step-up authentication with AI-driven facial biometrics for enhanced identity verification
- Secure privileged actions such as MFA/password reset
- Effortless UX with single sign-on
- Seamless and secure end-to-end digital onboarding includes identity verification and digital signing capabilities
- Reduce costs with streamlined identity management

Learn more about Workforce Identity at [Entrust.com](https://www.entrust.com)



Entrust Workforce IAM

Benefits

Our Workforce Identity solution strengthens organizational security posture by providing comprehensive identity management across all user access points. By employing advanced authentication methods such as biometrics, risk-based authentication (RBA), and certificate-based technologies, it ensures high assurance, phishing-resistant security, effectively mitigating the risk of credential theft and unauthorized access. This integrated approach streamlines user experience while enforcing strict security and compliance standards.

HIGHLIGHTS

Phishing-Resistant Passwordless MFA and Single Sign-On

Entrust enables organizations to provide a complete passwordless experience with high assurance, phishing-resistant options like FIDO2, passkeys, and certificate-based authentication for both users and devices. This approach ensures seamless login while helping to protect against account takeover (ATO) attacks. Users can choose from a wide selection of MFA authenticators, from mobile push notifications to hardware tokens and grid cards, and enjoy single sign-on (SSO) capabilities for an enhanced user experience, including offline authentication methods and one-click access to all applications.

Risk-Based Adaptive Authentication

Our solution employs a managed risk engine that evaluates contextual information, including IP address, time-of-day/day-of-week login, travel velocity, transaction details, behavioral biometrics, and more to calculate a risk score for user authentication. Based on this score, users may be prompted to use different two-factor authentication (2FA) methods or blocked if the risk score exceeds a pre-defined risk level threshold.

Digital Onboarding

Revolutionize employee integration with a secure, end-to-end digital onboarding experience. Entrust leverages advanced identity verification services supporting over 6,000 government-issued IDs from 195 countries, alongside presenter verification and liveness checks to prevent fraud and detect deepfakes. Phishing-resistant passwordless MFA and AI-driven biometrics ensure precise authentication, accelerating onboarding while helping to meet compliance requirements and enabling secure digital signing.

AI-Driven Identity Verification

Harnessing advanced AI technology, Entrust's identity verification processes deliver superior accuracy and heightened fraud prevention. Our AI-driven facial biometrics are phishing-resistant, verifying the identity of users with confidence, thereby significantly mitigating risks associated with impersonation, identity fraud, and deepfakes. This robust defense protects against modern cyber threats.



Entrust Workforce IAM

Comprehensive IAM

Entrust provides a comprehensive suite of IAM capabilities, including advanced identity verification, secure access management, and digital signing. These integrated features streamline administrative processes, reduce operational costs, and strengthen security protocols. By automating routine tasks and enforcing consistent security measures across all user interactions, this solution enhances operational efficiency, strengthens protection, and facilitates compliance with regulatory standards.

Enhance Your Existing Identity Provider (IdP)

Our workforce solution seamlessly integrates with your existing IdP solutions, delivering high assurance identities with a suite of advanced features. Leveraging certificate-based authentication (CBA), risk-based authentication (RBA), and AI-driven facial biometrics, the platform secures privileged actions like MFA setup and password resets. This comprehensive approach enables passwordless access and mobile authentication, streamlining the user experience and consolidating security processes. Additionally, step-up authentication adds an extra layer of security to sensitive operations, reducing risk and operational costs through efficient self-service options.

Securing Cloud Access With VPN and RADIUS

Entrust Workforce Identity enhances the security of cloud applications through seamless integration of VPN and RADIUS authentication. The VPN creates encrypted tunnels for remote devices, ensuring secure connections to the corporate network from anywhere. Complementing this, RADIUS (Remote Authentication Dial-In User Service) authentication adds an extra layer of security by verifying user credentials before granting access to network resources. Together, this robust combination ensures that only authorized users can access cloud applications and vital corporate assets, safeguarding your data and operations.



Entrust Workforce IAM

Features



Phishing-Resistant Passwordless MFA With Adaptive Risk-Based Authentication.

Our solution combines FIDO2, passkeys, and certificate-based authentication with AI-driven facial biometrics for robust security. An adaptive risk-based authentication (RBA) system uses a configurable risk engine to analyze contextual data like IP addresses and behavioral biometrics, adjusting security measures dynamically. Depending on the risk level, it may require additional authentication or block access, enhancing user assurance and fraud prevention.



Global Identity Verification (IDV) With AI-Driven Facial Biometrics.

Entrust's Global IDV uses AI-driven facial biometrics to enhance identity verification and fraud detection. This technology accurately detects synthetic manipulations, such as deepfakes, ensuring reliable authentication of international documents. It streamlines security processes like MFA resets and privileged access control, improving the integrity and efficiency of high-security operations.



Single Sign-On. SSO streamlines user access to multiple applications with a single set of credentials, enhancing productivity and reducing cognitive load on users. This minimizes password fatigue and related security risks.



Out-of-the-Box Integrations. Pre-configured integrations enable seamless connections to existing enterprise identity systems, streamlining federation and reducing implementation times. This feature supports quick and efficient integration, simplifying IT workflows and improving user access management across various identity platforms.



Enhancement for Existing Identity Providers (IdPs). Organizations can bolster the security of their existing IdPs with Entrust's solutions. This includes integrating certificate-based authentication, risk-based adaptive authentication, and IDV with facial biometrics for secure privileged and out-of-band access scenarios.



Learn more at
[entrust.com](https://www.entrust.com)



ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223