Entrust Identity for Workforce

A more secure and productive workforce

- Essentials
- Enterprise
- as a Service

ENTRUST

SECURING A WORLD IN MOTION

OVERVIEW

A modern IAM platform

Today's distributed workforce needs to be able to work anywhere with secure access to any app – cloud or on-premises – from any device. Unlike legacy identity and access management (IAM) solutions that assume an outdated security perimeter concept, Entrust Identity applies a modern identity-centric Zero Trust approach for a more secure and productive workforce.

THE OPPORTUNITY

A comprehensive workforce solution

Entrust Identity covers the spectrum of workforce IAM solutions, including:

- Best-in-class multi-factor authentication (MFA) and VPN protection for Windows-based environments with Identity Essentials
- High assurance credential-based authentication deployed on-premises with Identity Enterprise
- High assurance credential-based authentication deployed in the cloud with Identity as a Service

As well, Entrust Identity offers workforce IAM solutions to support a range of organization sizes, from SMBs with 50 users to large enterprises with 1M+ users.

Entrust Identity for Workforce IAM

	Core Use Cases	Deployment Option
Identity Essentials	Best-in-class MFA for Windows-based organizations; Remote access protection (VPN Clients, Cloud applications etc.)	On-premises
Identity Enterprise	High assurance credential-based authentication; Physical smart card issuance; Passwordless Access	On-premises, Virtual appliance
Identity as a Service	High assurance credential-based authentication; SSO; Passwordless Access and SSO	Cloud

Entrust Identity supports an unparalleled number of workforce use cases and deployment options including:

- High assurance credential-based access for enterprise and government workforces
- Single sign-on (SSO) with cloud deployment model
- High assurance credential-based/FIDO-compliant passwordless access with SSO
- Best-in-class multi-factor authentication (MFA) supporting a breadth of use cases and authenticators including soft token, hard token, mobile, grid card, SMS, push, and OTP
- Adaptive risk-based access and authentication with fine grained control
- Identity Proofing and workflow orchestration
- Self-service password resets
- Device reputation analysis
- Email signing and encryption, file encryption, and document signing
- Mobile software development kit (SDK)
- Available out-of-the-box integrations, SAML/OIDC, and REST APIs for administration & authentication
- Flexible deployment options: cloud, managed service, on-premises, virtual appliance

HOW IT WORKS

Workforce use cases

High assurance credential-based access

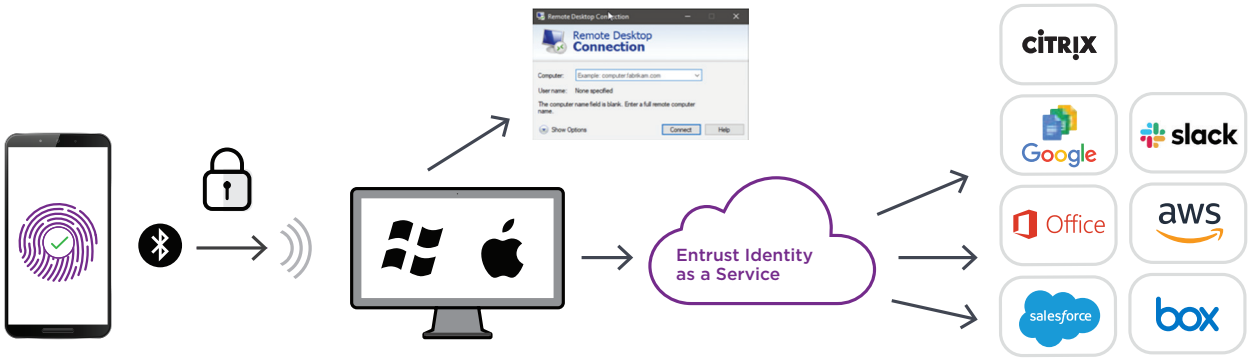
Entrust Identity provides the option of using digital certificates (PKI) for a higher level of security when and where warranted. This can be either a physical smart card or a virtual smart card that is provisioned on an iOS or Android device. The latter implementation is referred to as Mobile Smart Credential (MSC).

Single sign-on (SSO)

Legacy federation and access management systems are ill-suited to controlling user access in hybrid cloud/on-premises environments without a lot of manual provisioning posing a security risk. As well, users are often remiss to keep track of multiple URLs and credentials, leading to poor habits like password reuse and recycling that further compounds the security risk. Single sign-on (SSO) resolves these challenges by providing workers with one set of credentials to securely access any app (cloud or on-premises), while also making it easy for IT teams to securely manage user credentials. Entrust Identity as a Service federates with Cloud apps via standards like SAML and OIDC.

Credential-based/FIDO-compliant passwordless access with SSO

Arguably, the single largest vulnerability facing IT departments today is the employee password. Credential-based passwordless access provisions a digital certificate (MSC) on to the worker's phone, transforming it into their trusted workplace identity. When the phone is unlocked via biometrics or a secure PIN, the worker is logged into their workstation and applications when in close proximity and logged out when not. A secure frictionless experience for all, and no more password resets.



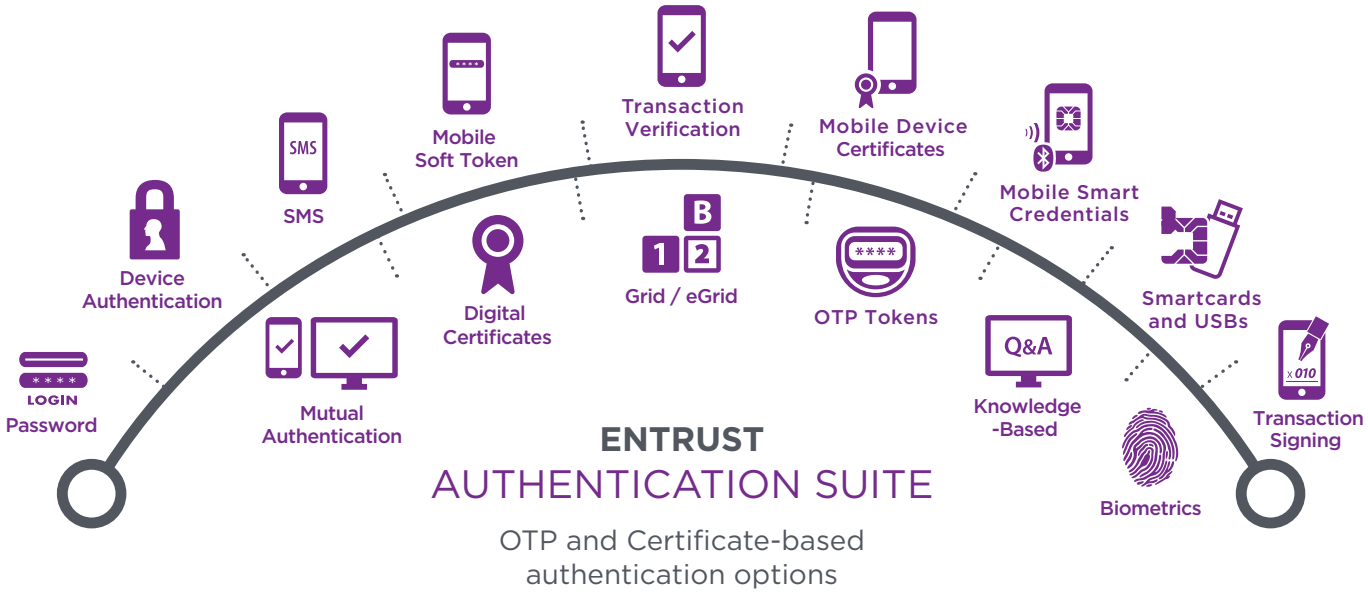
1. Use Biometric with mobile device to login
2. Leverage existing customer PKI/On demand Entrust PKI
3. Single Sign-on to all apps without need to re-authenticate

Benefits

- Simplified Deployment
- PKI-based - High Assurance
- Ease of Use - Biometric-based
- Email Signing & Encryption

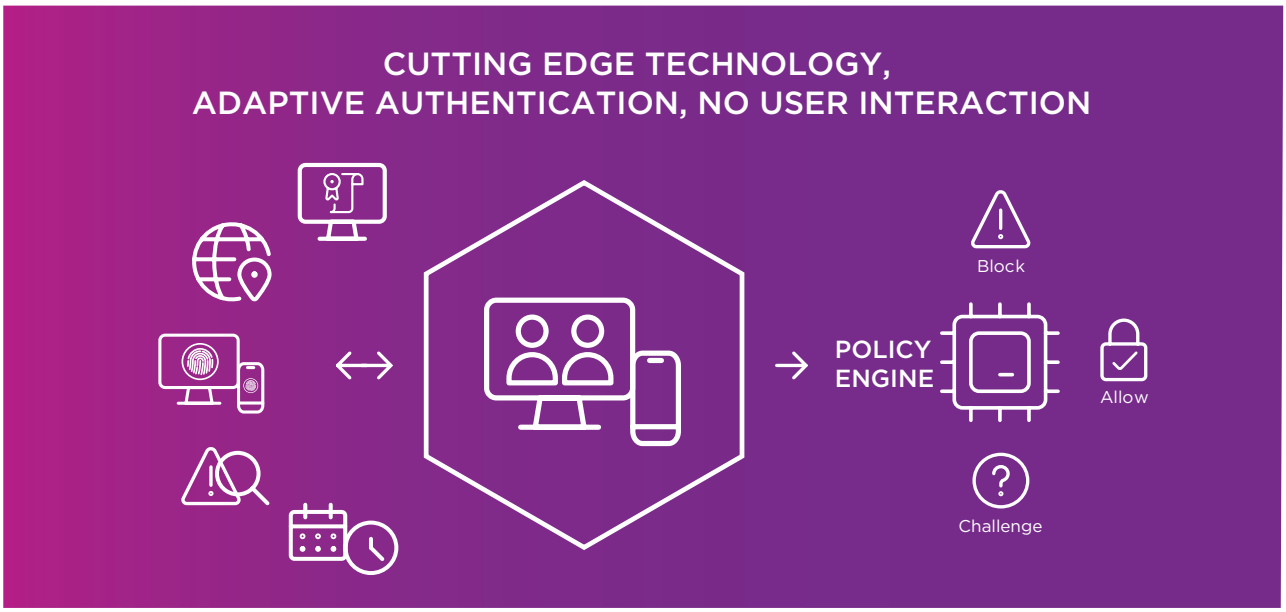
Multi-factor authentication (MFA)

Entrust Identity provides high availability and large-scale capability MFA with support for an unrivalled number of authenticators including FIDO tokens, mobile push, and grid cards. As well, Entrust Identity leverages smart phone biometric authenticators including fingerprint and facial recognition and provides a built-in soft facial recognition option if the smartphone does not have native biometric capabilities.



Adaptive risk-based access and authentication

Entrust Identity's adaptive risk-based engine provides an added level of security when conditions warrant, like a worker logging in for the first time from a new device, at an abnormal time of day, or from a different geolocation. Requiring additional authentication like a mobile push notification only for these situations minimizes worker friction while also protecting corporate resources.



Identity proofing and workflow orchestration

As more workforces become distributed and remote, the need to verify the identities of employees, contractors, and partners from afar increases. Our Identity Proofing solution provides fully digital identity verification for your workforce. The worker captures a high-resolution image of their government-issued ID, which is tested forensically and authenticated against a global database of 6000+ different government ID types, and takes a selfie to confirm that the person presenting the ID is the person who owns it. Liveness detection checks ensure the selfie is real, not a photo of a photo. Once authenticated, the worker can be onboarded and granted access to appropriate resources with complete workflow orchestration.

Self-service password resets

Password resets are a source of annoyance for IT help desks and users alike, not to mention the cost of lost productivity for both groups. Entrust Identity provides the ability for users to be able to securely reset their own passwords, meaning no downtime and no IT overhead. Better yet, go passwordless.

Device reputation analysis

To prevent the compromise of valid credentials, it is recommended to check the reputation of the device being used to access corporate resources first, especially in BYOD situations. Entrust Identity provides this option, with access to a database of over 6.5 billion devices connected to the internet to determine reputation. Checks include determining if the device is using a TOR-based browser or proxy, is jail broken or a rooted device, or has been used for debit or credit fraud along with account opening and access velocity. Device Reputation is included with Identity Proofing.

Email and file encryption, document signing

Through integration with the major MDM vendors including Microsoft, IBM, and VMware, Entrust Identity ensures workplace communications are secure with email and file encryption. MDM vendor integration supports secure workplace transactions with email encryption, file encryption, and document signing.

Mobile SDK and available integrations

Entrust Identity provides a mobile SDK so you can embed IAM directly into your workforce applications and brand as your own if desired. The portfolio offers proven out-of-the-box integrations including with all the major VPN vendors, SAML/OIDC, and APIs. As well, Entrust Identity works with your existing Microsoft environment, including Active Directory (AD), Active Directory Federation Server (ADFS) , Azure AD for user synchronization, and ActiveSync Device Provisioning to protect unauthorized devices from accessing users' email. For credential-based use cases, Entrust Identity is able to leverage certificates issued by Microsoft's CA.

Entrust Identity Solution Matrix for Workforce IAM

	Identity Essentials	Identity as a Service	Identity Enterprise
MFA	✓	✓	✓
SSO		✓	Via Federation Module (SAML)
High assurance credential-based access (certificates)		✓	✓
Physical smart card issuance			✓
High assurance credential-based/ FIDO-compliant passwordless access with SSO		✓	
Passwordless login		✓	✓
Adaptive access	Policy-based	Risk-based	Risk-based
Identity proofing		✓	✓
Self-service password resets	✓	✓	✓
Device reputation		✓	✓
Email and file encryption		✓	✓
Document signing		✓	✓
ADFS	✓	✓	✓
Azure AD Integration		✓	
ActiveSync Device Protection	✓	✓	
IT platform requirements	Windows	N/A	Windows/Linux
Mobile SDK	✓	✓	✓
Number of users	<5000	Unlimited	>5000
Deployment	On-premises	Cloud	On-premises

Flexible deployment, broad capabilities

Entrust Identity can be deployed in the cloud, on-premises, or as a virtual appliance. As well, Entrust works with Managed Service Providers to deliver Entrust Identity as a managed service.

Entrust Identity:

- Complements your existing IT infrastructures and workflows vs. seeking to replace
- Delivers the widest support of VPN, cloud and on-premise based applications
- Provides the option for certificate-based authentication which also supports the industry's only real high assurance passwordless solution
- Offers a mobile platform with one modern unified app that works across the portfolio
- Provides available out-of-the-box integrations, SAML/OIDC, and APIs
- Includes a mobile development kit so you can embed authentication directly into your own apps and brand as your own as desired
- Offers access to the industry's largest MDM ecosystem, including Microsoft Intune, MobileIron, Citrix, and VMware AirWatch
- Ensures easy IT implementation and efficient operation with point-and-click provisioning and policy management, and self-service password resets

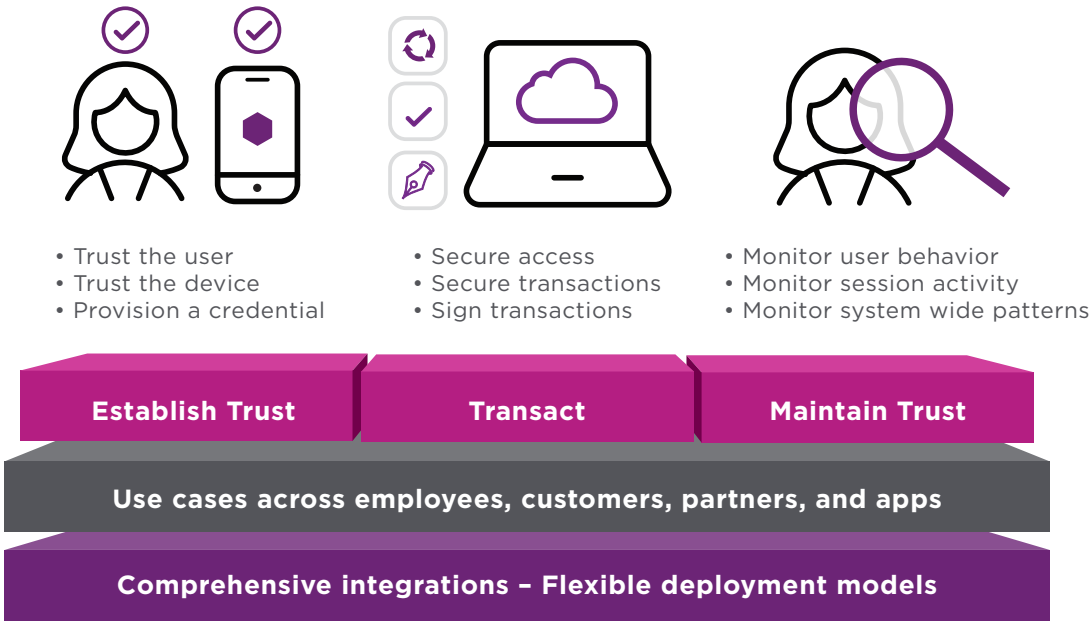
Mobile-first approach

Entrust Identity applies a unique approach to mobile, with a layered model to establish trust in the device and user first before enabling access. It then applies adaptive step-up authentication to ensure this trust is maintained over time.

OUR SOLUTION

Entrust Identity portfolio

Entrust Identity is the IAM portfolio that provides the flexibility and scalability you need to stay ahead of the ever-evolving threat landscape and realize a Zero Trust framework. Beyond workforce IAM, Entrust Identity also supports consumer and citizen use cases.



THE ENTRUST DIFFERENCE

A leader in IAM

With 25+ years of digital identity expertise and 50+ years of security innovation, Entrust is an identity and access management leader. Our high assurance solutions are proven with Fortune 500s and governments and are deployed by 10K+ customers around the globe. Entrust Identity secures digital identities and corporate assets, while also improving workforce productivity and removing friction for consumers and citizens.

For more information

888 690 2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust secures a rapidly changing world by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com