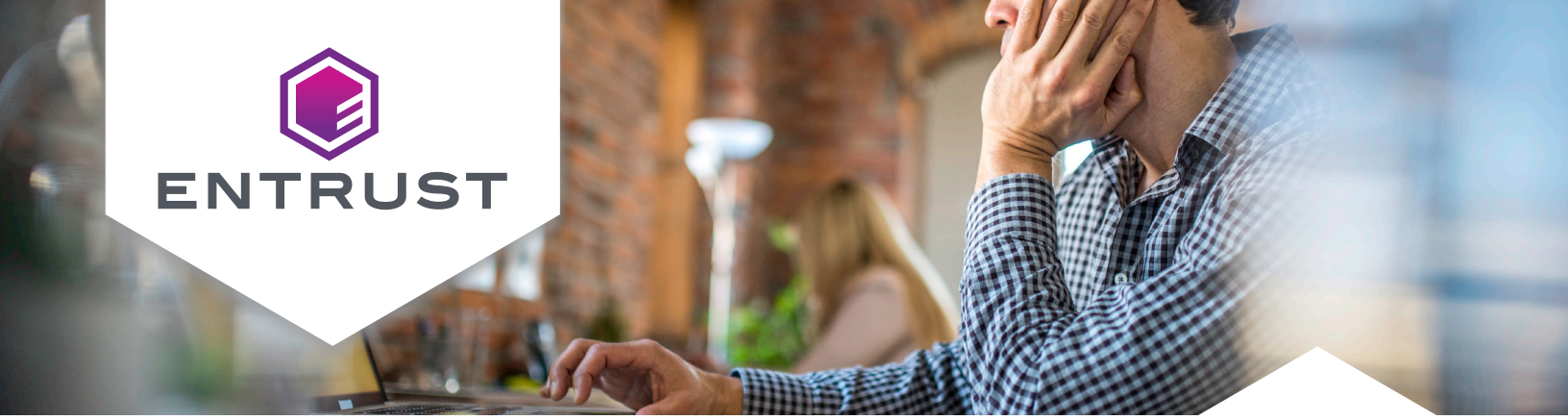


Entrust Identity Enterprise

HIGHLIGHTS

One platform for enterprise IAM use cases

Identity Enterprise is the integrated identity and access management (IAM) platform that addresses a full suite of workforce, consumer, and citizen use cases. It brings 25+ years of proven expertise supporting high assurance Fortune 500, government, and consumer banking applications with continued innovation and agility. Identity Enterprise sets the benchmark for large organizations with thousands and even millions of users that are seeking a Zero Trust approach. Identity Enterprise can be deployed on-premises or as a virtual appliance.

Identity Enterprise is part of the Entrust Identity portfolio that also includes Identity as a Service for cloud-based IAM and Identity Essentials for workforce IAM in Windows-based environments.

Identity Enterprise at a glance

	Workforce	Consumer/Citizen	Deployment
Identity Enterprise	High assurance credential-based authentication; Physical smart card issuance; Passwordless login	Secure portals; Multi-factor authentication (MFA); Adaptive risk-based access; Digital Citizen ID	On-premises; Virtual Appliance

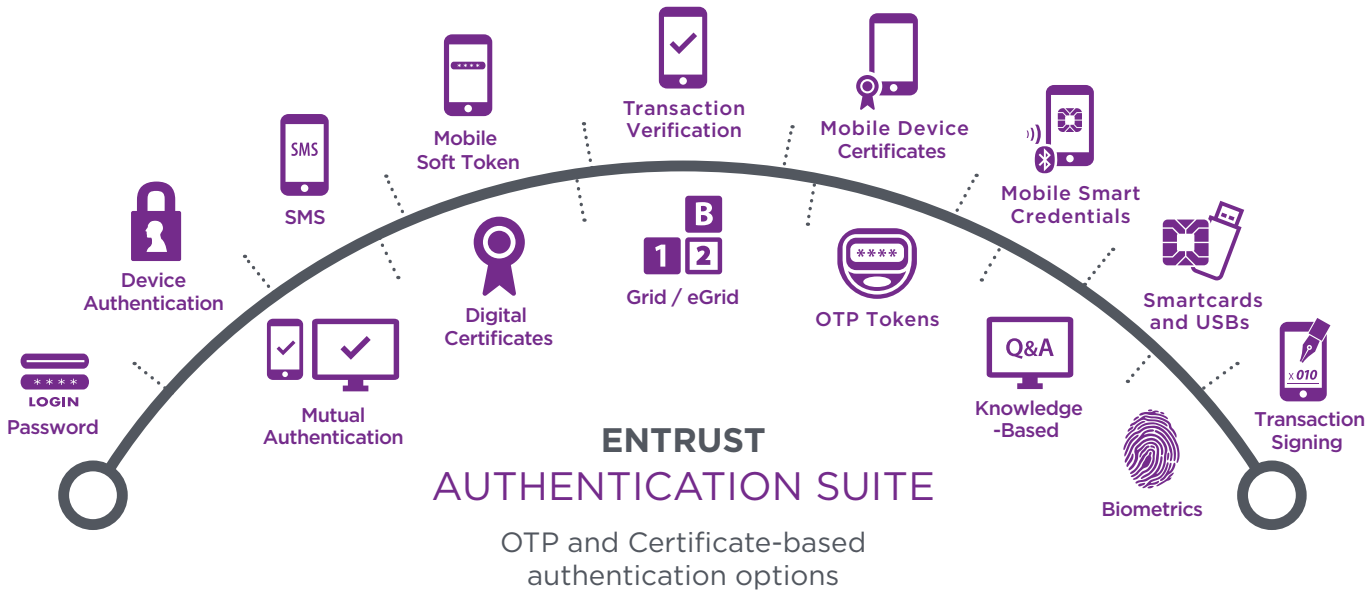
- Realize a Zero Trust framework
- Secure workforce, consumer, and citizen identities with high assurance use case coverage including credential-based access, smart card issuance, and best-in-class MFA
- Limit user friction with adaptive risk-based authentication, passwordless login, and cloud app federation
- Manage security, risk, and compliance
- Implement, manage, and scale easily with full active-active configuration, mobile SDK, and cloud migration options

Entrust Identity Enterprise

KEY CAPABILITIES

Best-in-class multi-factor authentication (MFA)

Support for an unrivalled number of authenticators, including OATH tokens (for authentication and transaction signing), mobile push, mobile data signatures, and grid cards.



High assurance credential-based authentication

Option to use 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).

Third-party CA support

Direct integration with Entrust and Microsoft CAs, including key recovery. As well, Identity Enterprise supports the Entrust CA Gateway, so you can use the CA of your choice.

Smart card and token issuance

Issue smart cards and tokens individually or in bulk with X.509 certificates or PIV containers. Identity Enterprise provides this functionality centrally with Print Module or allows authorized users to do this through their workstations.

Entrust Identity Enterprise

KEY CAPABILITIES (CONTINUED)

High assurance credential-based access with data encryption

Option to leverage the high performance and security of modern HSMs to encrypt your data at rest. Native support for nShield on-premises, hosted, or as a Service options, as well as support for Thales Luna Network HSM.

Secure access to cloud applications

Deploy Identity Enterprise's Federation Module for federated and SSO applications, including Office 365 using SAML.

Adaptive risk-based access and authentication

Offer an added level of security when conditions warrant, like a user logging in for the first time from a new device, at an abnormal time of day, or from a different geolocation. Go a step further and check if devices have the fingerprint of known bad devices by enabling Device Reputation. As well, Identity Enterprise supports an extensible risk engine so you can integrate your preferred risk analyzer to enrich each authentication and transaction decision.

Passwordless login

Credential-based passwordless workstation login. Passwordless options for consumers include using smartphone biometrics or FIDO tokens with BYODs.

Identity proofing

Optional integration to support self-service consumer and citizen digital identity verification for fast, secure onboarding with Identity Enterprise.

Digital citizen identity

Option to improve the security and efficiency of government services with the ability to issue trusted citizen identities for border crossing, licensing, voting, and more.

Secure portals

Secure access to customer and partner portals.

Email and file encryption, document signing

Through integration with the major MDM vendors including Microsoft, IBM, and VMware, Identity Enterprise 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.

Entrust Identity Enterprise

KEY CAPABILITIES (CONTINUED)

Self-service password resets

Ability for users to be able to securely reset their own passwords, meaning no downtime and no IT overhead.

Mobile SDK

Identity Enterprise uses the Entrust Identity mobile SDK so you can embed IAM directly into your applications and brand as your own if desired. Use our Mobile Smart Credential SDK to develop your own passwordless and document signing applications.

Cloud deployment options and migration

Keep your options open. On-premises-based Identity Enterprise might be the right solution right now, but you may also be looking toward a cloud future. You can move Identity Enterprise into Amazon AWS, Microsoft Azure, or other cloud providers via a cloud-based virtual machine (VM). Alternatively, we offer easy-to-use tools to quickly migrate all of your Identity Enterprise users and data to Identity as a Service when you are ready for the cloud.

ISG Identification Systems Group

Identification Systems Group
www.IdentificationSystemsGroup.com
info@identificationsystemsgroup.com
888.964.6482