

Entrust & IBM Security Integration

Strong Authentication for Enhanced Identity & Access Management

Today's workforce demands easy, anytime, anywhere access to content and resources. Users increasingly utilize mobile and cloud platforms as their primary means for resource consumption.

Unfortunately, modern threats from malware, hackers and advanced persistent threats (APTs) cause organizations to restrict access, making it cumbersome for end-users. Alternatively, a number of organizations provide too much access, despite the increased threat landscape.

In order to maintain security, while making it easy for end-users, organizations need a secure and simple method to access content and resources.

By realizing the benefits of strong, identity-based security, end-users are empowered with the ability to securely access content and resources — anytime and anywhere.

Built-in integration between the Entrust IdentityGuard software authentication platform and the IBM Security Access Manager for Web — specifically for stronger risk-based authentication — enables organizations to realize the potential of secure access management and identity-based security.

Enterprise-Wide Authentication Framework

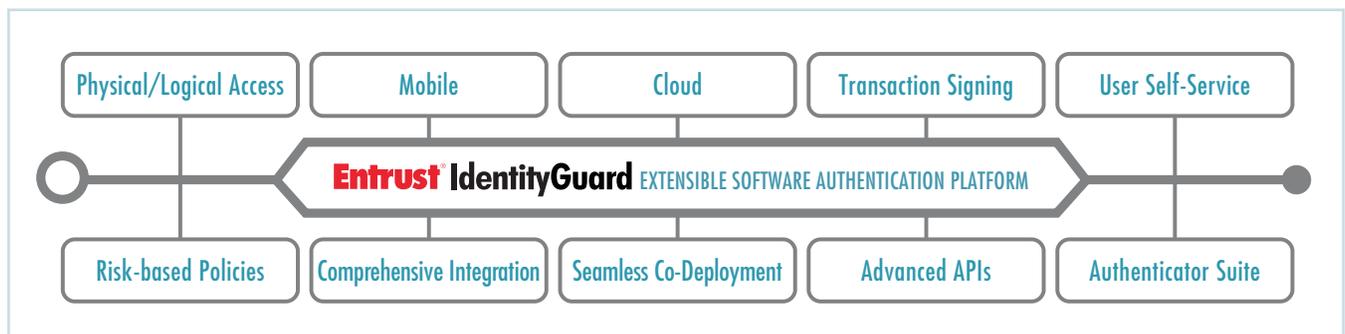
The award-winning Entrust IdentityGuard software authentication platform enables organizations to deploy strong authentication throughout an enterprise — whether for physical, logical, cloud or mobile access.

The comprehensive identity-based security framework complements IBM Security Access Manager for Web by adding strong multifactor authentication — all via simple, built-in integration.

Solution Benefits

- Leverages Entrust IdentityGuard with IBM Security Access Manager for Web to deploy proven identity-based security and authentication
- Increases end-user productivity while improving security
- Extends end-user access across mobile and cloud environments
- Offers widest range of authentication methods from a single software platform, including smartcards and mobile solutions
- Transforms mobile devices into enterprise-grade smart credentials for physical and/or logical access
- Extends to provide strong authentication in customer environments
- Protects leading applications like IP-SEC and SSL VPNs, Microsoft® Windows® desktops and enterprise Web applications like Microsoft® Outlook® Web Access
- Built on Entrust's FIPS140-2-validated cryptographic engine
- Provides broad platform support including Microsoft® Windows® Server, Sun Solaris, AIX and Linux
- Optional certificate-based authentication via cross-domain authentication service (CDAS) is available for higher-assurance security requirements

entrust.com/ibm



INTEGRATION WITH IBM SECURITY ACCESS MANAGER FOR WEB

Entrust IdentityGuard seamlessly integrates into the IBM Security Access Manager for Web solution for true risk-based authentication that's also easy to install. Proven single sign-on (SSO) capabilities are critical for protecting access to sensitive information, applications, networks and more.

As the threat landscape changes, organizations can adapt rapidly by rolling out new authenticators to mitigate the impact of a breach or emerging threat. Organizations may even use a number of authenticators to suit both usability and security needs.

The integration offers self-service capabilities that help end-users manage credentials — including enrollment and account changes — in the event an authenticator is lost or stolen.



For high-assurance security needs, both Entrust IdentityGuard and IBM Security Access Manager for Web support smartcards and the ability to manage certificates and PKI credentials.

Optional certificate-based authentication via cross-domain authentication service (CDAS) is also available.

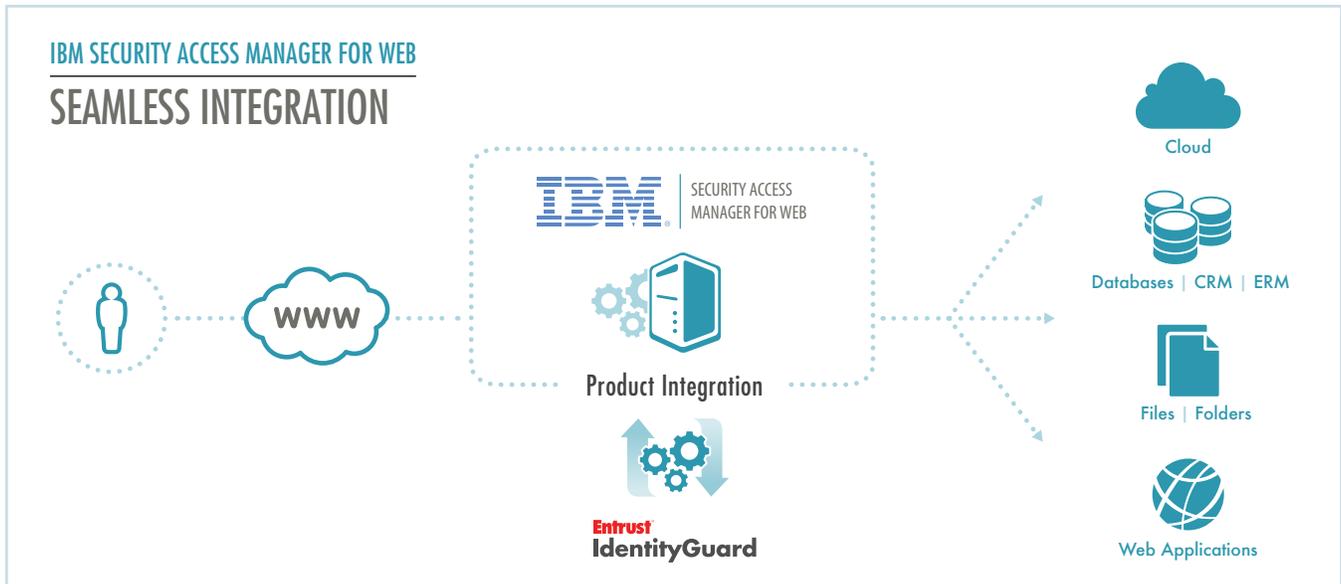


Figure 1: Integration architecture between the Entrust IdentityGuard software authentication platform and IBM Security Access Manager for Web.

ENTRUST IDENTITYGUARD SOFTWARE AUTHENTICATION PLATFORM

The award-winning Entrust IdentityGuard software authentication platform enables organizations to deploy strong authentication throughout the enterprise — whether for physical, logical, cloud or mobile access.

The framework approach not only helps manage all authentication needs, but also provides abilities unique to the market. Organizations no longer need to deploy various point products to accomplish strong authentication to achieve identity-based security.

- Deploys to a single server
- Co-deployment with existing authentication measures
- Simple integration and easy-to-use APIs to extend identity-based security to legacy or outgoing systems
- Mobile, physical and logical authentication
- Federate internal and cloud-based applications (e.g., Salesforce.com, Microsoft 365)
- Reduce cost and maximize staff efficiency with an intuitive self-service module



More Authenticators, One Platform

Entrust IdentityGuard offers the widest range of authenticators on the market — and all from a single, cost-effective software platform.

And the addition of smartcards, mobile smart credentials and digital certificates extends the platform's versatility, scalability and cost-effectiveness. This gives organizations the ability to utilize a number of different authenticators to suit their needs across multiple use cases and situations, particularly to meet specific budgets or to quickly re-deploy authenticators in real time.

Authentication Options

The solution's authentication capabilities include IP-geolocation, device, questions and answers, out-of-band one-time passcodes with transaction details for verification (delivered via voice, SMS, email or Entrust IdentityGuard Mobile), grid and eGrid cards, digital certificates (in software or on smartcards/USB tokens), mobile smart credentials and a range of one-time-passcode tokens.

Entrust also provides multiple methods of supporting mutual authentication, including picture and caption replay as well as Extended Validation (EV) SSL certificates.

Mobile Smart Credentials

A number of organizations are realizing the potential power and convenience of mobile devices as easy-to-use authenticators for internal employees accessing physical and logical resources, and customers accessing mobile and online services.

The Entrust IdentityGuard Mobile Smart Credential is an innovative mobile application that transforms a mobile device into a virtual smartcard, eliminating the need for plastic smartcards, one-time-passcode hardware tokens and even passwords.

Plus, advanced mobile smart credentials may be used with Bluetooth and near-field communication (NFC) technology for greater convenience.

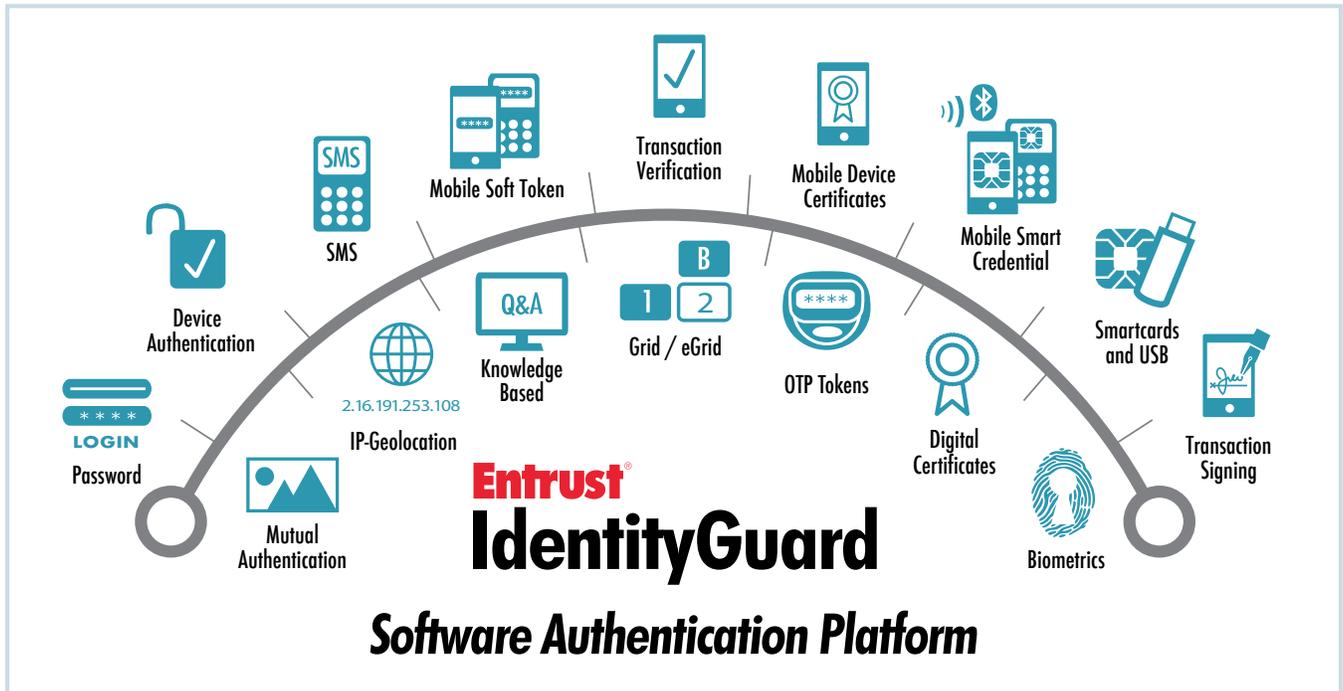


Figure 2: Entrust IdentityGuard provides one of the widest ranges of authentication capabilities on the market today.

SECURITY
ON

IBM SECURITY ACCESS MANAGER FOR WEB

Formerly IBM Tivoli® Access Manager for e-business, IBM Security Access Manager for Web helps organizations address the growing incidence of advanced Web threats and risks associated with mobile, social and cloud access while complying with security regulations. Security Access Manager for Web provides security-rich access management that enables employees, customers and partners to safely access online resources.

About IBM Security Systems Software

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-FORCE research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more.

These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

About Entrust

A trusted provider of identity-based security solutions, Entrust secures governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL. For more information about Entrust products and services, call 888-690-2424, email entrust@entrust.com or visit www.entrust.com.

More Information

For more information on Entrust IdentityGuard integration with IBM Security Access Manager for Web, contact the Entrust representative in your area at **888-690-2424** or visit entrust.com/ibm.