Entrust Datacard™

Entrust IdentityGuard Mobile Push Authentication for VPN and Web Access

Simply Better Two Factor Authentication

Whether you are in healthcare, financial services, government, manufacturing and technology or another sector, addressing regulatory compliance and breach threats means you need to secure employee access to company networks and applications. While hardware tokens have been adequate, you realize the cost and management burden of this dated technology is high and your user communities continue to be frustrated with having to carry tokens and type-in lengthy one-time-passcodes when authenticating.

Entrust IdentityGuard Mobile with "push notification" makes secure access VPN and Web applications easier than ever – for both users and for IT support. Users simply access VPN or web applications and instantly their mobile phone alerts them to verify login using the IdentityGuard Mobile application – a quick review and click of the "OK" buttons secures their session and lets them get on to business with ease and confidence.

Delight Users With Simple, Convenient Authentication

While strong authentication is needed, legacy approaches get in the way of business with issues such as lost tokens, frustrating login experiences and tedious IT provisioning and user support issues. Entrust transforms mobile devices into secure, simple to use, always in hand authenticators. And, VPN access is just the beginning.

Transform Your Business

Entrust IdentityGuard Mobile is far more than a replacement for hardware tokens. It gives you the ability to secure mobile initiated VPN sessions, access to third party cloud/ SaaS applications and makes it possible to confirm business critical transactions "out-of-band" to defeat malware-based session riding attacks.

Reduce IT Cost & Complexity

Leveraging mobile eliminates the need to purchase dedicated and often costly hardware tokens and simplifies user provisioning and management as users already know how to download and update mobile applications. Entrust's broad range of self service features makes enrollment and activation a breeze.

Invest Wisely – Invest Once

Authentication solutions seem to be popping up everywhere these days. However, most solutions are limited to a few use cases and don't have the pedigree earned through decades of Identity-based security experience. With Entrust, while you may only have one need today – our solution will grow with you as new user communities and projects come on board.

Entrust Datacard Local Partner

ELLIOTT DATA SYSTEMS, INC.

St. Louis, MO
17825 Edison Ave
Chesterfield, MO 63005
(636) 386-8400

Memphis, TN
5045 Covington Way
Memphis, TN 38134
(901) 372-4600

www.elliottdata.com

Solution Benefits

- Easy, convenient for end-users by enabling them to leverage their mobile devices
- Reduce costs and confidently migrate away from legacy hardware tokens
- Simplify IT management by empowering users with mobile-based user self-provisioning
- Strong authentication with patent pending out of band transaction verification to defeat advanced session riding attacks
- Flexibility to support users without mobile offering the broadest range of authenticators on a single platform including: mobile authenticators, physical or electronic grid cards, KBA, adaptive authentication, and even hardware tokens for those who don't like change
- Migrate with ease – with Entrust you can co-deploy alongside a legacy solutions such as RSA and migrate users as hardware tokens expire.

Entrust IdentityGuard Mobile Push Authentication – How It Works

Authentication with the simple action of a quick mobile acknowledgement

Entrust IdentityGuard Mobile seems so simple on the surface, not of end users but is rooted in the most advanced security approach to defeating account takeover attacks. When the user logs into the virtual private network, instead of being asked to answer challenge questions or enter an OTP value on their PC, IdentityGuard sets up a secure session to their mobile device and prompts the user to confirm that they do want to securely log-in. With a simple "OK" acknowledgement, their VPN session is then established on their PC.

Users who are accessing corporate networks / applications on their mobile phones and tablets can also take advantage of the same feature. They simply initiate their VPN session and the Entrust IdentityGuard server sends a notification to their device to confirm the login. A quick toggle to the mobile application allows them to review and confirm the action. No OTPs to enter, no challenge questions to answer – the user experience is quick and simple so employees can get on with business with ease and confidence.

Mobile Authentication is just the beginning

Entrust understands that focusing on today's need is top priority but all too often investments in new technology lead to a "buyer's remorse" a few months down the road when new business requirements emerge. Our mobile solution suite is designed to address all of your mobile needs from securing mobile devices and access right through to leveraging mobile for advanced use cases such as physical building access and even logging onto Windows workstations.

Seamless upgrade for existing IdentityGuard Customers

As an existing IdentityGuard customer, we know you value the extensive platform of capabilities to meet your diverse needs and use cases. As always, with Entrust your investment is well protected and soft tokens you use today can be upgraded to Mobile Push at no extra cost and with minimal IT impact.

ENTRUST MOBILE SECURITY SOLUTIONS

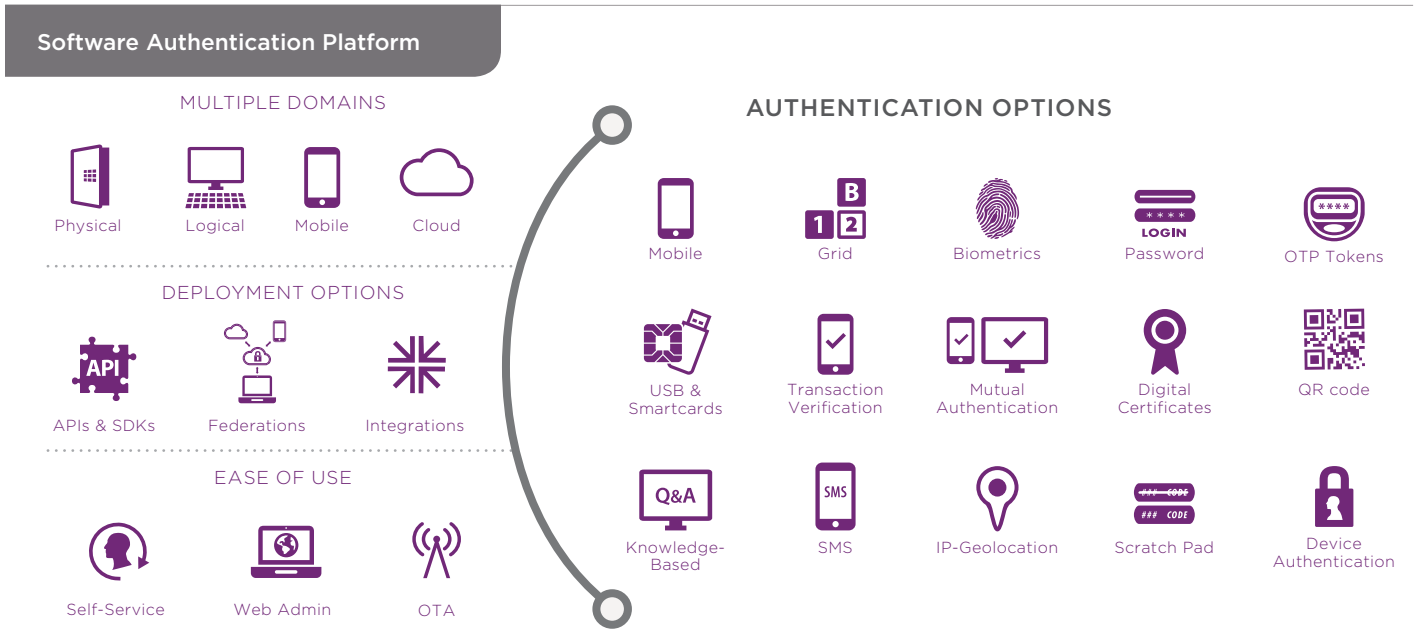
IDENTITIES, DEVICES & TRANSACTIONS

- STRONG AUTHENTICATION
- DEVICE CERTIFICATES
- MDM INTEGRATION
- DESKTOP MALWARE PROTECTION
- MOBILE SMART CREDENTIAL
- TRANSACTION-SIGNING
- APPLICATION PROTECTION

Entrust IdentityGuard: Your Enterprise Authentication Platform

Entrust IdentityGuard is a next-generation identity-based security framework that serves as the foundation for your current and evolving digital identity needs. With rich, contextual policy management, security can automatically adapt according to access requirements or the risk in a given transaction — across diverse users and applications

Entrust's software authentication platform does not impact normal user behavior or back-end applications, speeding deployment and helping to save money. Entrust IdentityGuard affords the flexibility for specific authenticators to be defined on a per applications and/or group basis so you can tailor security to the use case and risk situation. Simple policy change can seamlessly adjust the authentication behavior of all applications virtually instantly. Without the need to re-architect applications, you have the agility to proactively protect what matters most.



One platform - Many use cases

Entrust's management framework is unique in the market and drives significant value for todays connected enterprise. The solution enables organizations to deploy strong, risk-based authentication to properly secure employee access, privileged user accounts and even customer and partner access to company portals

- 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
- Deploys to a single server
- Co-deploy with existing two factor authentication solutions for a smooth migration
- Simple integration and easy-to-use APIs