



Securing Your Digital Life

Entrust IdentityGuard™ for Oracle

Multi-Factor Authentication Platform from Entrust Provides Security for Oracle Identity Management

Entrust IdentityGuard is a comprehensive multi-factor authentication platform for consumer and enterprise-facing applications. It provides a suite of **strong authentication** capabilities that can enable your organization to take a risk-based approach to user authentication. Entrust IdentityGuard's flexible deployment options enable you to match strong authentication methods to the level of risk associated with the different types of users, transactions, and applications within your unique environment.

Entrust IdentityGuard is integrated with the Oracle Identity Management platform, allowing Oracle users the capabilities provided by Entrust's multi-factor authentication platform, designed for use in consumer and enterprise environments. Applications accessed through the Oracle Identity Management platform can now leverage one or more of the wide range of authentication options delivered by Entrust IdentityGuard.

The integration between Entrust IdentityGuard and the Oracle Identity Management Platform is enabled by the new *Entrust IdentityGuard Strong Authentication Plug-in*.

"The solution works as follows – when a user needs to authenticate to an application, Oracle Access Manager (OAM) will determine the appropriate type of authentication required for the particular user and the operation being performed. Depending on policies configured in the Oracle Access Manager, a strong authentication front-end module will be invoked for any transaction that is deemed sensitive and needing 2-factor authentication. Oracle Access Manager will attempt to authenticate the user by consulting with the Entrust IdentityGuard Server, using the *Entrust IdentityGuard Strong Authentication Plug-in*. The user will be allowed (or denied) access by OAM based upon the results returned from the Entrust IdentityGuard Server."

The authentication mechanism used—for both user and server—could be any of the numerous mechanisms supported by Entrust IdentityGuard. For user authentication, these include:

- Machine authentication – transparent verification that the user's machine has been authorized.
- Knowledge-based – the user answers questions only he/she would know.
- Grid – user enters cell information from a grid card in the user's possession.
- Passcode list – user leverages a list of passcodes, each to be used once.
- Mobile – one-time-passcode delivered to device in user's possession (e.g. voice over phone, text message to cell phone, email).
- YASCO Time-synchronous token – a physical token that generates time-based OTP for authentication.



Product Features

- Wide range of strong user authentication options available, including physical second factor
- Integrated mutual authentication - can increase user confidence with multiple server authentication options
- Easy to integrate with both enterprise and consumer-facing applications
- Centralized policy and enforcement of a range of authenticators for increased security and management ease

Product Benefits

- Non-invasive, easy-to-use options for strong authentication can increase user trust and customer usage
- Risk-based authentication - can match strength of authentication to the transaction risk
- Can help address regulatory requirements for second factor authentication
- Help avoid phishing and other attacks
- Protect user and data privacy
- Prevent information leakage

Entrust IdentityGuard™ for Oracle

For mutual authentication, Entrust IdentityGuard provides:

- Picture and message replay
- Grid serial number/location replay

Additional authentication mechanisms supported by the Oracle and Entrust include:

User Authentication – verifying that the user is who they claim to be

- Supported user authentication mechanisms provided in an integrated solution:
 - Support for native application-based username/password – basic password for initial login and low-risk operations.
 - Digital ID (X.509 certificate) – strong cryptographic authentication

Server Authentication – displaying personalized information to the user to verify site authenticity

- Supported server authentication mechanisms provided in an integrated solution:
 - Image replay – displays personalized image to the user.
 - Message replay – displays personalized text to the user.
 - Serial number replay – displays a serial number on grid card to the user.
 - Grid location replay – displays grid coordinate information to the user.
 - Digital ID (X.509 certificate) – strong cryptographic authentication

Entrust IdentityGuard is available directly from Entrust or through authorized resellers. Please visit www.entrust.com for more information

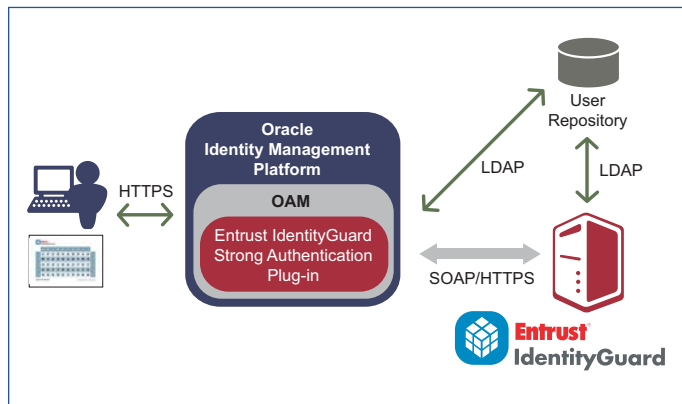


Figure: Entrust/Oracle Solution

Oracle Identity Management Partner Integration

When Oracle conducts partner integration and testing, we verify only that the software integration functions according to the partner's proposed integration plan, and that it makes appropriate use of Oracle components and integration technologies in the environment specified in the published Integration Datasheet. This process applies only to the components providing integration between the partner's software and specified Oracle component; it does not apply to or extend to the partner's software product(s). The integration is performed in a lab environment using standard versions of the Oracle product and the partner's software. The testing is product version specific, hardware specific, database specific, and operating system specific, and is conducted in English, unless explicitly noted otherwise. Similar results may not be able to be duplicated in a production environment, including where the Oracle or partner software is modified or customized upon implementation. Customers are solely responsible for the selection of all third-party software, including any integration software, used in conjunction with Oracle Identity Management and for the results of such use.

About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and e-mail security into business opportunities. For more information on how Entrust can secure your digital life, please call us at 888-690-2424, or send an e-mail to: entrust@entrust.com Visit us on the Web at: www.entrust.com.

Entrust® Securing Digital Identities & Information

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc. or Entrust Limited in certain countries. All other company names, product names and logos are trademarks or registered trademarks of their respective owners. © Copyright 2006 Entrust. All rights reserved.