

Entrust Entelligence Security Provider

Deploy Easy-to-Use Enterprise Security

Every day, employees, partners and customers access your organization's networks to exchange sensitive information, which requires protection against theft, loss, tampering and corruption when stored or while in transit.

The loss of hardware is serious, but the financial ramifications from the loss of sensitive information are even more significant. Entrust addresses these challenges with a cost-efficient desktop security solution that can be easily deployed and used.

Empowered by Digital Identities

Entrust Entelligence Security Provider is a desktop security solution that enables a variety of security capabilities including encryption, digital signatures, secure file deletion and authentication using a single digital identity. This provides customers with the ability to address a broad set of application security requirements — all from a single solution — and can help enable a security infrastructure that is easy to administer and manage.

Entrust Entelligence Security Provider's integration with the Microsoft® Windows® security architecture extends protection to enterprise applications in a way that is easier to deploy and manage.

Entrust Entelligence Security Provider for Windows is designed to automatically manage and protect digital identities used by Windows-based applications for encryption, digital signatures and authentication.

Entrust Entelligence Security Provider for Outlook complements Security Provider for Windows by simplifying the delivery of secure messages from the desktop. It also can improve performance of secure messaging by transferring secure email processing to the Entrust Entelligence Messaging Server, with virtually no impact to the end-user.

Product Benefits

- **Rapid, efficient deployment** – experience faster security deployment with a thin client that is customizable for organizational security policies
- **Improved enterprise security** – protects users' digital identities and enforces centrally controlled security policies to help prevent unauthorized access to sensitive information
- **Seamless and transparent management** – automate the entire lifecycle management of the user digital identity through self-service enrollment to transparent renewal
- **Reduce total cost of ownership** – improve your return on investment (ROI) when compared to other solutions, using automatic and transparent security management
- **Enhances Microsoft Windows security framework** for digital IDs from any certification authority (CA)

Technical Features

- Flexible digital ID enrollment methods (both manual and automatic)
- Centrally managed policies and controls
- Flexible key protection including local file, central server, smartcards and USB tokens
- Automatic digital ID management, including updates, revocation and recovery
- FIPS 140-2-validated Security Kernel
- NIST-approved Path Discovery and Validation
- Right-click file encryption

- Password encryption with self-extracting option
- Automatic secure file deletion with white/blacklists
- Simplified management of Microsoft EFS keys (e.g., Auto-enroll, Recover, Backup)
- Auto-configure other applications to use correct certificates (e.g., Microsoft® Outlook®, VPN, EFS, IIS, etc.)
- CRL and OCSP revocation support
- CA Agnostic: Thin client can be deployed with CA from any leading vendor

Complementary Entrust Products

Entrust Intelligence Messaging Server

Integrates with the Entrust Intelligence Messaging Server to transfer the secure email processing tasks from the client to the server to improve performance and simplify the end-user experience.

Entrust Intelligence Group Share

Provides automatic, transparent and persistent encryption of data stored in network folders. The solution leverages the digital ID managed by Security Provider for authentication and key protection.

Entrust Intelligence Secure Desktop for Mac

Provides a desktop security solution for the Mac O/S by enabling a variety of security capabilities, including encryption, digital signatures and authentication — all using a single digital identity.

Entrust Intelligence Solo

Using encryption and digital signature technology, the solution provides easy and secure data exchange between Entrust enterprise customers and their third-party partners via a personal, self-signed digital ID.

Cryptographic Algorithms Supported

- AES (128-, 192- and 256-bit)
- DES, Triple DES
- RSA (512-, 1024-, 2048- and 4096-bit)
- IDEA 128
- CAST (40-, 64-, 80- and 128-bit)
- SHA-1
- SHA-2 (256, 384, 512)
- ECC (EC-P-256, EC-P-384 and EC-P-521)

Platforms Supported

- Microsoft® Windows® 7 All 32- and 64-bit editions
- Microsoft® Windows® XP SP2, SP3 Professional/Home/Tablet — All 32- and 64-bit editions
- Microsoft® Windows® Vista™ SP1, SP2 — All 32- and 64-bit editions
- Microsoft® Windows® Server 2003 SP1, SP2 — All 32- and 64-bit editions
- Microsoft® Windows® Server 2003 R2 SP1, SP2 — All 32- and 64-bit editions
- Microsoft® Windows® Server 2008 SP1, SP2 — All 32- and 64-bit editions
- Microsoft® Windows® Server 2008 R2 — All 64-bit editions

Note: The above list excludes Itanium-based operating systems.

Smartcards, Tokens & Middleware Supported

- SafeNet, Inc.
- ActivIdentity
- Aladdin Knowledge Systems, LTD.
- Any smartcard supporting Microsoft Base Smartcard CSP

About Entrust

A trusted provider of identity-based security solutions, Entrust empowers 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.

Entrust® Securing Digital Identities & Information