Entrust® Securing Digital Identities & Information

SECURITY ON

Entrust Entelligence Messaging Server

Email & eStatement Encryption

Core to an identity-based security strategy, Entrust Entelligence Messaging Server streamlines and simplifies the methods to secure email communication through encryption.

The email security solution makes it easy to safely communicate with external business partners and customers. It is shipped as a turnkey appliance and delivers standards-based email encryption capabilities in a comprehensive platform.

Entrust Entelligence Messaging Server automatically secures both user-to-user communications as well as electronic statements. And it is easy to deploy and maintain for organizations that communicate sensitive or regulated information — both inside and outside their organization — via email.

Automatic Encryption

To transparently manage security functions and help enforce corporate email policies, the Entrust Entelligence Messaging Server can automate encryption for some or all email messages leaving a specific network. The solution works with popular email environments such as Microsoft® Outlook® and Lotus Notes®, and even Yahoo, Microsoft® Hotmail®, Gmail and virtually any Web-based email service.

To suit the encryption requirements and preferences of an organization, Messaging Server can be deployed standalone or with a variety of complementary solutions such as desktop encryption, content-monitoring, strong authentication, email-archiving, storage area networks and off-board public key infrastructure (PKI) integration with Microsoft Certification Authority or Entrust Authority.

Secure eStatements

The convenience of electronic statements can help reduce printing and mailing costs, increase efficiency, eliminate paper waste and improve the overall customer experience. It's important to deliver electronic statements in a manner that respects the privacy of sensitive information and ensures that only the recipient can access the content.

Entrust's solution enables customers to use their existing statement-generator applications to have all statements generated in industry-standard PDF format and forwarded via email to the Entrust Entelligence Messaging Server. Statements are automatically encrypted and sent to customer email inboxes. Statements are decrypted with simple, but secure, password protection.

Content Control

For protection against inadvertent compliance violations and intellectual property theft, Messaging Server supports native content-filtering of outgoing messages based on customer-definable policies. The solution also seamlessly integrates with third-party content scanners that customers may already have deployed.

Product Features

- **Encrypt eStatements** – securely reduce printing and mailing costs, increase efficiency, eliminate paper waste and improve the overall customer experience
- **Regulatory compliance through encryption** – automatically encrypt messages leaving an organization to help protect the confidentiality of information
- **Content control through e-mail security** – automatically scan outgoing messages for a range of customer-definable policies and encrypt when sensitive information is detected
- **Email security that works for partners and customers** – offers a range of delivery methods to meet varied recipient needs including Adobe PDF, Web-based secure email, S/MIME and OpenPGP; S/MIME certificates can be generated for external users providing a seamless encryption experience within email applications such as Microsoft® Outlook®
- **Boundary-based email security** – automatically encrypt emails at the network boundary before it is delivered to recipients, without requiring end-user action
- **Versatile support** – includes hardware or VMware platforms, as well as a hardened operating system, which support email encryption modules and online updates

Messaging Server will automatically encrypt sensitive emails containing customer account information, personal employee data, client lists, merger and acquisition information, financials, source code and other valuable informational assets that have been flagged by content scanners before they are routed outside an organization's boundary.

Key Features

- Embedded standards-based certification authority (CA) – transparently manages harvesting of existing S/MIME, OpenPGP external-user certificates; generates new S/MIME proxy certificates for both internal and external users; integrates with existing Microsoft and Entrust PKIs as required
- Flexible encryption options including automatic encryption based on message header information (e.g., sender, recipient, recipient domain); message body content, including keywords and Regular Expressions (REGEX); as well as Microsoft Active Directory group membership
- User-initiated boundary encryption through client-based email plug-ins for Microsoft Outlook and Lotus Notes
- Flexible delivery allows external recipients to communicate securely using the encryption standard of their choice, including S/MIME, Open PGP, SecurePDF, WebMail Pull and WebMail Push
- Highly customizable deployment through integration with optional solution components such as portal authentication systems, content-control, email archiving, storage area networks, anti-spam/anti-virus, SNMP monitoring and strong authentication
- Support for mobile email clients such as RIM BlackBerry, Apple iOS, Android and Java-based platforms, as well as WAP-compatible browser-based cell phones
- Automatic eStatement encryption for securing machine-generated statements that may contain customer sensitive information such as bank statements, confirmations, payroll statements, medical claims or utility statements

Technical Features

- Customizable deployment of appliances for clustering, distributed physical deployment and segregations of application processes such as webmail on separate nodes
- Comprehensive Web administration interface and simplified deployment
- Server-side expansion of distribution lists for secure delivery
- Fully automated certificate retrieval and management
- Highly configurable system-level options for external message delivery formats, user and system administration, and integration of third-party solutions
- Hardware- and application-level SNMP support
- Security-hardened appliance built on FIPS-validated Entrust Security toolkit
- DKIM (DomainKeys Indentified Mail) signing of outgoing messages
- Customizable roles-based access for system configuration and administration
- Dashboard-level system monitoring with drill-down access to individual application processes and clustered servers
- Detailed standard and customizable reporting capabilities

Cryptographic Algorithms Supported

- AES-256, RC2-128, Triple-DES, CAST128, IDEA, Twofish-256, Blowfish-128
- RSA 1024, 2048, 4096, DSA 1024
- MD5, SHA-1, SHA-256

Optional Hardware Provided

- High-end, dual-CPU server includes redundant power supplies, RAID hard disk array and separate hardware monitoring backplane

Platforms Supported

- Microsoft Exchange
- Lotus Domino
- Any SMTP-compliant email server

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

22123/3-11