

Proofpoint Secure Messaging Module

Powered by Voltage IBE™

The Proofpoint Secure Messaging™ module, a component of the Proofpoint Protection Server® and the Proofpoint Messaging Security Gateway™, makes ad hoc, secure communication just as easy as traditional, non-encrypted messaging. Proofpoint's powerful, policy-driven encryption features mitigate the risks associated with regulatory violations, data loss and corporate policy violations, without adversely impacting business operations. Proofpoint Secure Messaging is ideal for organizations in the healthcare, financial services, government and other sectors that need to protect sensitive data, while still making it readily available to appropriate affiliates, business partners and end users.

overview

As email has become the preferred medium for business communications, organizations have become increasingly concerned about ensuring the security of individual messages. Email is commonly used to transmit sensitive or confidential information—including operational data, trade secrets, legal documents, financial information, and personal healthcare and identity information—both inside and outside the enterprise.

The need to secure this confidential information—and comply with a growing body of regulations that govern the transmission of private data—have made policy-based email encryption a “must have” feature of a complete messaging security solution. The Proofpoint Secure Messaging module meets these requirements with the industry's most powerful and flexible solution for policy-driven secure messaging.

features

Policy-driven secure messaging

Training end users in the proper use of encryption systems can be a significant barrier to successful deployment of traditional secure messaging solutions. But Proofpoint Secure Messaging is much easier to use and manage. Proofpoint's secure messaging solution automatically and dynamically applies encryption or decryption based on your organization's policies, right at the gateway. As a result, end users don't need to take any special actions to take advantage of encryption features and your compliance and content security policies are consistently and accurately applied on an as-needed basis.

Easy to administer

Unlike alternative approaches to encryption, Proofpoint's identity based encryption features provide effective protection for sensitive information without the administrative burdens and infrastructure costs typically associated with secure messaging.

- **Easy policy management:** All encryption policies—whether they are driven by regulatory compliance, data security or internal corporate concerns—are centrally managed and enforced at the gateway. The Proofpoint Messaging Security Console™ provides a convenient graphical interface for defining encryption policies, which can be triggered based on message content identified by the Proofpoint Regulatory Compliance™, Proofpoint Content Compliance™ or Proofpoint Digital Asset Security™ modules.
- **Simplified key and certificate management:** Using Voltage Security's IBE (Identity-Based Encryption) technology, public keys are generated on-demand, eliminating the daunting certificate lifecycle and key management requirements of other encryption solutions. Ongoing maintenance of certificates and Certificate Revocation Lists (CRLs) is not required.
- **Minimal data storage and archive requirements:** Proofpoint Secure Messaging also simplifies the storage, backup and recovery overhead usually associated with message encryption. Using IBE, messages and keys do not need to be backed up or stored for extended periods of time.



What is Identity Based Encryption?

The Proofpoint Secure Messaging module is powered by Identity-Based Encryption (IBE) technology from Voltage Security.

Voltage IBE is a public key cryptography system that uses common identities—such as an email address—as public keys, eliminating the need for certificates, Certificate Revocation Lists and other costly infrastructure. The result is a powerful encryption solution that is easy to implement and easy to manage, without the overhead and cost inherent in traditional security solutions.

How does IBE work?

Any user can communicate securely with any other user by using the recipient's email address as the encryption (or public) key. Decryption (or private) keys are generated by the Proofpoint Secure Messaging module on an as-needed basis. These keys can be recreated at any time, eliminating the need to archive or store decryption keys.

These basic properties allow for a secure messaging environment where certificates are never required and users need to know nothing other than their email addresses.



Proofpoint Secure Messaging Module

Powered by Voltage IBE™

features (continued)

Easy to use

Proofpoint Secure Messaging operates transparently to end users without requiring software downloads or the installation and maintenance of desktop encryption clients. Proofpoint's encryption solution automatically encrypts and decrypts sensitive content as required, without end users having to use and manage complicated digital certificates or encryption keys.

Low total cost-of-ownership

The Proofpoint Secure Messaging module seamlessly interfaces with other Proofpoint modules including Proofpoint Regulatory Compliance and Proofpoint Digital Asset Security. Easy deployment and minimal ongoing management requirements greatly reduce the ongoing costs associated with managing your secure messaging solution. And Proofpoint's unparalleled ease-of-use for end users minimizes support, training and helpdesk costs.

powerful, secure messaging policy enforcement

Extremely granular control of encryption policies

As in Proofpoint's anti-spam, anti-virus and content security modules, secure messaging policies are managed and enforced on an enterprise level from a single location, using the Proofpoint Messaging Security Console. Once defined, enterprise encryption policies are applied automatically at the gateway, eliminating the risk of user error.

Message encryption policies can be extremely granular—encryption can be triggered by any combination of:

- **Structured data matches:** Such as the presence of protected healthcare or financial information such as HIPAA codes, ABA routing numbers, credit card numbers and social security numbers as detected by the Proofpoint Regulatory Compliance module.
- **Unstructured data matches:** Such as the presence of confidential information as detected by the Proofpoint Digital Asset Security module.
- **Keywords and regular expressions** found in the subject line or content of messages as defined in the Proofpoint Content Compliance module.
- **Message origin or destination:** Encrypt messages based on destination (e.g., a specific business partner or supplier) or sender. Messages can also be encrypted based on other message attributes such as attachment type.

Apply inbound policies to encrypted messages

Email can also be decrypted at the gateway, allowing Proofpoint's anti-spam, anti-virus and content compliance policies to be applied to encrypted email before it is delivered to end users, ensuring that encrypted spam, malware and non-compliant messages are properly handled.

The Simplicity of IBE

Proofpoint's use of IBE ensures the security of encrypted email communications while minimizing the burden on end users.

Consider the case of a doctor who needs to send a message—containing confidential healthcare information—to a patient. The transaction works as follows:

- Doctor A writes and sends an email to Patient B using their regular email client. The Proofpoint software or appliance analyzes the message and detects the presence of confidential healthcare info and classifies message, triggering an encryption policy.
- Patient B receives the encrypted email and clicks the attachment to authenticate himself to the Proofpoint Secure Messaging module via SSL.
- Proofpoint Secure Messaging decrypts the message and hosts it in server memory for Patient B to review. After Patient B accesses the message, it is removed from memory.
- Using the Proofpoint Secure Messaging module's webmail functionality, Patient B can securely reply to Doctor A.

Additional Encryption Options

In addition to providing the Proofpoint Messaging Security module, Proofpoint easily integrates with a variety of popular third-party encryption solutions. Contact Proofpoint for up-to-date information about supported encryption solutions.

Learn More about Proofpoint Secure Messaging

For more information about Proofpoint's identity-based encryption features, download our free whitepaper, *Encryption Made Easy*, by visiting:

<http://www.proofpoint.com/encryptionwp>

©2007 Proofpoint, Inc. Proofpoint Protection Server is a registered trademark of Proofpoint, Inc. in the United States and other countries. Proofpoint, Proofpoint Messaging Security Gateway, Proofpoint Content Compliance, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, Proofpoint Secure Messaging and Proofpoint MLX are trademarks of Proofpoint, Inc. in the United States and other countries. Voltage and Voltage IBE are trademarks or registered trademarks of Voltage Security in the United States and other countries. All other trademarks contained herein are the property of their respective owners. 10/07