

Removing the Complexity and Risk from Secure Message Delivery: Postini Encryption Manager

Whether your company is subject to regulations or requirements from business partners that mandate message encryption, or your legal staff is concerned about sensitive corporate information going unprotected over the Internet, convenient, secure messaging is finally within reach.

Postini Encryption Manager™ makes encrypting messages easy and affordable by overcoming the complexity, incompatibility, and costs associated with multiple encryption standards and technologies.

Managed Security Services Offer Message Encryption and Secure Connections

Postini Encryption Manager addresses broad, real-world, secure messaging needs with two encryption services:

Connection Security – Offers comprehensive session-level protection with industry-standard, server-to-server transport layer security (TLS). Postini integrates strong TLS encryption with policy-based management so IT staff has full command and control over which messages must be delivered via an encrypted connection.

Message Security – Offers content-level encryption to shield message content in cases where server-to-server security is not available or required. This “secure and post” encryption option relies on proven Secure Socket Layer (SSL) Web browser technology, and can be deployed at a policy level and individually by end-users.

Postini Creates Seamless Interoperability across Standards

As part of its Federated Encryption strategy, Postini will continue to build its encryption library, incorporating encryption technologies from well-known industry vendors and acting as an industry-first “universal translator” for encryption technologies. Companies will no longer be forced to purchase and maintain multiple non-compatible encryption products to comply with demands by regulatory agencies, business partners and clients.

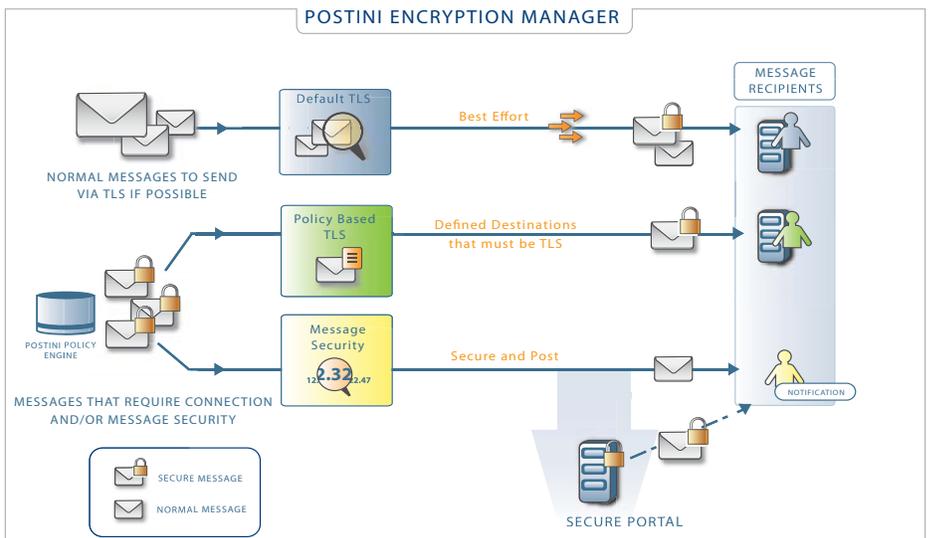
Advanced, Integrated Encryption Delivered Through a Managed Service

Postini Encryption Manager integrates seamlessly with Postini Perimeter Manager Enterprise Edition® because TLS protocol encryption is built into

Postini’s Integrated Message Management framework. Through Postini’s common policy framework and a common management platform, organizations can:

- Create private messaging networks with trusted partners
- Enforce mandatory domain-level TLS connections
- Restrict connections that cannot be encrypted
- Employ numerous content-level encryption solutions
- Receive alerts when TLS policies cannot be enforced
- Avoid the ongoing costs and complexities of multiple encryption product installations and key management

Figure 1: Postini ensures that emails are delivered via a secure connection over the Internet through its built-in TLS protocol support and message management capabilities.



How Postini Encryption Manager Works

Connection Security automatically enforces TLS rules with partners with established encryption requirements, preventing a sending or receiving server from converting a message to clear text if it encounters a non-compliant server. Email alerts automatically notify senders if encrypted messages cannot be delivered. Sensitive data is never sent over the Internet unless the path from gateway to gateway is encrypted.

Message Security requires no encryption technology between sender and recipient to communicate securely because the encryption is handled by Postini. Based on policy-based rules or initiated by an end user request, a message is sent securely to Postini Encryption Manager to be encrypted. Postini Encryption Manager posts the message to a secure Web portal, notifies the recipient of the encrypted message, and gives instructions on accessing the secured message. Once the secure Web portal authenticates the recipient, they are allowed to read and reply to the message.

IT staff can easily establish policies to encrypt all messages from a sender or a group of senders, or can encrypt all messages flagged confidential.

Why Choose a Postini Managed Service?

Mitigates business risks – Postini Encryption Manager offers complete policy-based encryption capabilities to comprehensively protect companies from the risks of non-compliance and employee negligence.

Eliminates complexity – Because Postini takes care of everything, there is no need to install multiple encryption systems and establish a database system to handle the retrieval and distribution of encryption keys, or maintain dedicated secure VPN channels to secure

Figure 2: Postini Encryption Manager Features & Benefits

FEATURES	BENEFITS
Flexible, secure email policies	Automatically identify and encrypt email by sender and/or recipient to satisfy internal policies or external regulations.
Automatic real-time protection	Ensures that intended recipients receive encoded messages and intelligently routes email based on real-time discovery of recipient capabilities.
Integrated message management	Enables IT staff to create policies at the organization, sub-organization or individual level.
Easy administration and use	Eliminates need for PKI certificate, keys, and password management and need for dedicated secure networks such as virtual private networks (VPNs). Also hides all complexity from end users.
Lower cost	Requires no additional hardware or software to install or maintain on desktops or email servers.
Convenient reports	Provides visibility into sender patterns and aids in policy enforcement.
Federated Encryption	Provides encryption platform freedom: leverages ZixCorp technology today; OpenPGP, S/MIME, and other market-standard encryption to be added in 2006.
Immediate deployment, flexible growth	Requires no infrastructure; the managed service can be activated in a matter of hours and scales easily and effectively across any size organization.

communications with employees and business partners.

Reduces operation costs – Postini replaces potentially escalating capital and capacity planning costs with a predictable monthly operation expense.

Puts your business back in control – Postini Encryption Manager removes the incompatibility and management headaches associated with multiple encryption standards and technologies. By federating disparate standards, Postini maximizes interoperability across technologies and

paves the way for platform-independent message encryption.

System Requirements

Email Server

- Lotus Domino 6/7
- Microsoft Exchange 2000 or 2003 Enterprise Edition
- Novell Groupwise 6/7
- Sendmail
- Postfix
- qmail
- Support for TLS protocol handshake

About Postini

Postini is the first and only enterprise-class managed service to provide Integrated Message Management. As the leader in Integrated Message Management, Postini provides security, compliance, availability and visibility solutions for corporate email and IM systems. Postini's messaging services are designed to protect businesses from a wide range of IM and email threats, address regulatory compliance requirements, and enable the management and enforcement of enterprise policies. Founded in 1999, Postini protects and manages electronic communications for more than 35,000 businesses worldwide, providing comprehensive, flexible and trusted managed services for message security and management.



Corporate Headquarters

San Carlos, California USA

Toll-free 1-866-767-8461

Email info@postini.com

Web Site www.postini.com

EMEA Headquarters

London, UK

Tel +44 (0)207 082 2000

Email info_emea@postini.com