

# Google Message Encryption



---

## ABOUT GOOGLE APPS

---

Google Apps is a suite of applications that includes Gmail, Google Calendar (shared calendaring), Google Talk (instant messaging and voice over IP), Google Docs & Spreadsheets (online document hosting and collaboration), Google Page Creator (web page creation and publishing), Start Page (a single, customizable access point for all applications) and Google Security & Compliance. Google Apps offers editions tailored to specific customer needs, including the Standard Edition (ideal for family domains), Education Edition (K-12 schools, colleges and universities) and Premier Edition (businesses of all sizes).

For more information, visit [www.google.com/a/security](http://www.google.com/a/security)

---

## Automatic Encryption for Sensitive Email Communications

Business requirements, industry regulations, and government mandates increasingly dictate that your organization must secure electronic communications. Whether it is financial data, medical records, or proprietary corporate information, you simply must secure the delivery of sensitive content to its destination. Encrypting email communications is a cost effective solution that helps your organization prevent financial penalties and potential brand equity damage when sending unprotected proprietary or regulated data via email.

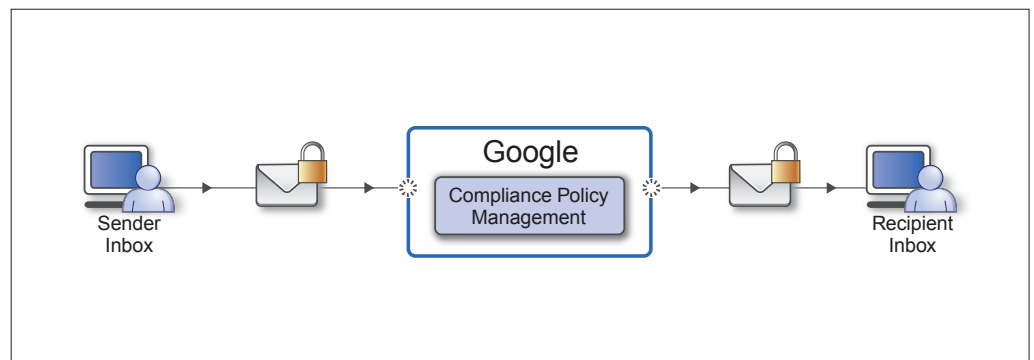
## What Google Message Encryption Service Does

Google Message Encryption service, powered by Postini, provides on-demand message encryption for your organization to securely communicate with business partners and customers according to security policy or on an “as needed” basis.

Without the complexity and costs associated with legacy on-premises encryption technologies, Google Message Encryption service makes encrypting email messages easy and affordable. The policy-based solution enables your organization to send encrypted email to any recipient.

## The Google Message Encryption service enables:

- Secure messaging between business partners, customers, or individuals without any additional software, hardware, or technical training
- Automatic enforcement of organizational email encryption policies based on individuals, groups, or specific message content
- User-initiated encryption for confidential messages to any email recipient
- Auditable protection of emails containing regulated or company proprietary information
- Centrally-managed security policies and reporting



**Figure 1:** Inbox delivery provides encrypted messages directly to the recipient's inbox.

## How Google Message Encryption Service Works

Google Message Encryption service secures outgoing email to the Postini data center using a secure SSL/TLS encrypted connection. At the data center, messages are scanned for viruses and messaging policy compliance.

Based on centrally managed policies, messages are encrypted for each intended recipient. Encrypted messages are either delivered directly to the recipients' inbox or stored on a web-based portal for secure pickup.

### Inbox delivery

The inbox delivery method delivers email directly to the recipients' email application as an encrypted attachment. Recipients can view their messages by opening the attachment and providing their password. If the recipient does not have an existing password, the recipient is stepped through a simple, one-time registration. No additional software is required.

### Portal delivery

Using the secure portal delivery, email notifications are sent to intended recipients letting them know a message is waiting for them. The notification message includes a link to the portal and instructions on how to view the encrypted message using their web browser.

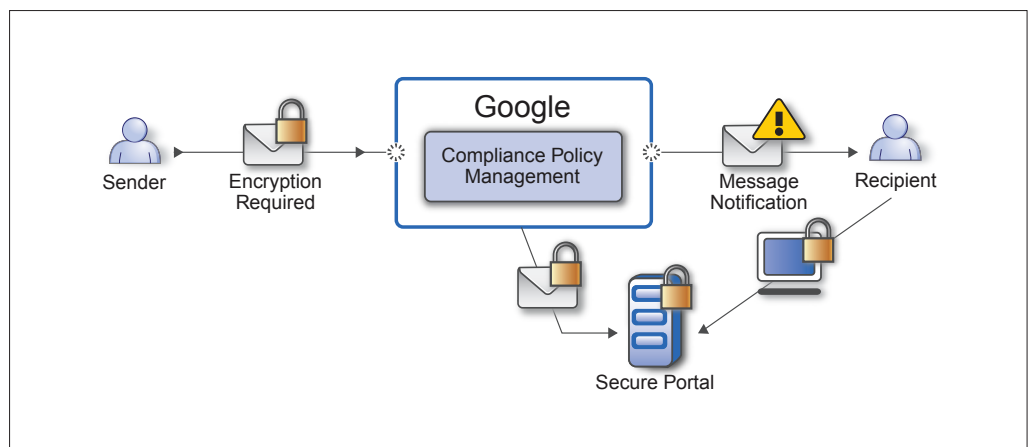
Clicking on the link directs recipients to the secure portal. Using the full-featured messaging console, recipients can view, reply to, and compose new messages securely.

### Customized branding

The portal can be branded to match the look and feel of your organization's existing website or portals, providing your customers with a consistent online experience and strengthening your brand equity.

### Content-based encryption

Administrators can centrally define and enforce email encryption policies based on specific email content. This enables your organization to automatically encrypt sensitive email based on established policies for email and data security.



**Figure 2:** Secure portal enables delivery of protected email through a secure, web-based portal.

### User initiated encryption

Administrators can create rules that enable individual users to initiate secure delivery for designated messages. For example, a user can simply mark a message as “confidential” in their email client to trigger the automatic encryption.

### Delivery failure notification

Google’s Message Encryption service automatically notifies the sender if the recipients do not view the encrypted messages. This provides the sender with confidence that the message delivery was successful.

### Integrated service component

Google Message Encryption is tightly integrated into patented, on-demand architecture that also provides additional security and compliance solutions, including spam protection, anti-virus, and email archiving.

### Conclusion

Google Message Encryption service enables your organization to securely exchange sensitive information with business partners and customers using encrypted email. The automatic, policy-based encryption is easy to implement and provides a more cost-effective solution than legacy on-premise email encryption infrastructures. As with all the Google on-demand solutions, Google Message Encryption service requires no additional hardware, software, updates, or maintenance.

Features	Benefits
Secure, encrypted, auditable communications	Comply with regulatory, business partner, and internal policies for protection of sensitive data. Detailed reporting on rule enforcement enables policy refinement and simplified auditing.
Content-based policy enforcement	Enables consistently enforced policies based on an organization’s specific encryption requirements.
Web portal or inbox delivery options	True ad-hoc email encryption capabilities to meet sender and recipient requirements.
Always on, always current	Provides always-on service and scalability to ensure uninterrupted business operations.
Rapid implementation	Everything is included for sending and receiving encrypted email, no additional components are required.

