

Google Message Discovery



ABOUT GOOGLE APPS SECURITY AND COMPLIANCE

Google security and compliance products, powered by Postini, make your existing email system more secure and compliant. Built on a hosted service platform, these products block spam, phishing, malware and other intrusions before they reach your network, and provide content management and archiving to help you meet legal challenges. Google's hosted model offers several distinct advantages. Leveraging the "network effect" of tens of thousands of email networks, Google technology detects new threats in real time and blocks them across the entire Google security network – without requiring on-site updates. Similarly, economies of scale in storage, simple deployment and maintenance-free service drive a low total cost of ownership.

For more information, visit www.google.com/a/security

As email volumes grow in business environments, so do the legal implications of storing and managing archived email messages. In the event of litigation, the legal discovery process often requires you to locate and recover pertinent messages quickly and comprehensively. Sheer message volume can make meeting these requirements with traditional technology prohibitively expensive and time-consuming. IT leaders face the challenge of keeping large volumes of email safe and easily accessible without making a significant investment in new infrastructure.

Google Message Discovery, powered by Postini, is a secure, hosted email service that solves this problem for enterprises looking to cost-effectively protect and access archived email data. Google Message Delivery enables you to:

- Create a centralized and searchable email repository for your organization
- Quickly search across the archive to collect email for legal discovery
- Secure your email from spam, viruses, and other threats

Manage email retention without expensive investment in storage capacity

Google Message Discovery is delivered in an on-demand, Software as a Service (SaaS) model, so you don't have to worry about planning for current and future storage capacity needs – Google does it for you. By storing your messages in Google's secure and geographically redundant data centers, you can ensure that messages will not be lost in the event of an onsite server failure. You can archive all mail without worrying whether you have enough disk space and eliminate storage quota headaches by allowing users to access historical mail. In addition, by offloading excessive mail from your existing servers, you can decrease backup windows and reduce recovery times.

Collect email quickly and easily for legal discovery

When your company is involved in litigation or conducting an internal investigation, time is of the essence. Sifting through back-up tapes, email servers, and laptops in search of particular messages can create a costly strain on your team's productivity and budget. Delays in producing the right evidence can result in significant fines, lost revenue, or irreparable damage to your corporate reputation.

With Google Message Discovery, access to all your archived messages is always at your fingertips. What's more, legal, human resources, and compliance staff do not need to rely on IT personnel to conduct searches and inquiries. Google's easy-to-use web-based interface lets anyone – even end users – manage and search the message archive according to policy and depending on specific roles and authorizations. And because Google Message Discovery saves all messages based on your defined retention policies, indexes them, and stores them in a centralized repository, you can quickly and easily pinpoint relevant messages, place them on litigation hold to disable message deletion, and share as needed with legal counsel, law enforcement officers, or regulatory officials.

Deliver secure, spam-free email for your users

Google Message Discovery also includes a complete set of email security features, so you can provide the highest levels of security for your email systems – without installing expensive hardware or software. This lets you block spam, viruses, and other external threats before they reach your organization and ensure proprietary information that must remain confidential stays within your organization. You can also define which emails – within and beyond your network – are encrypted, providing an additional layer of security. Plus, because these security features are built into Google Message Discovery, you can manage all your messaging-related policies from a single, central console.

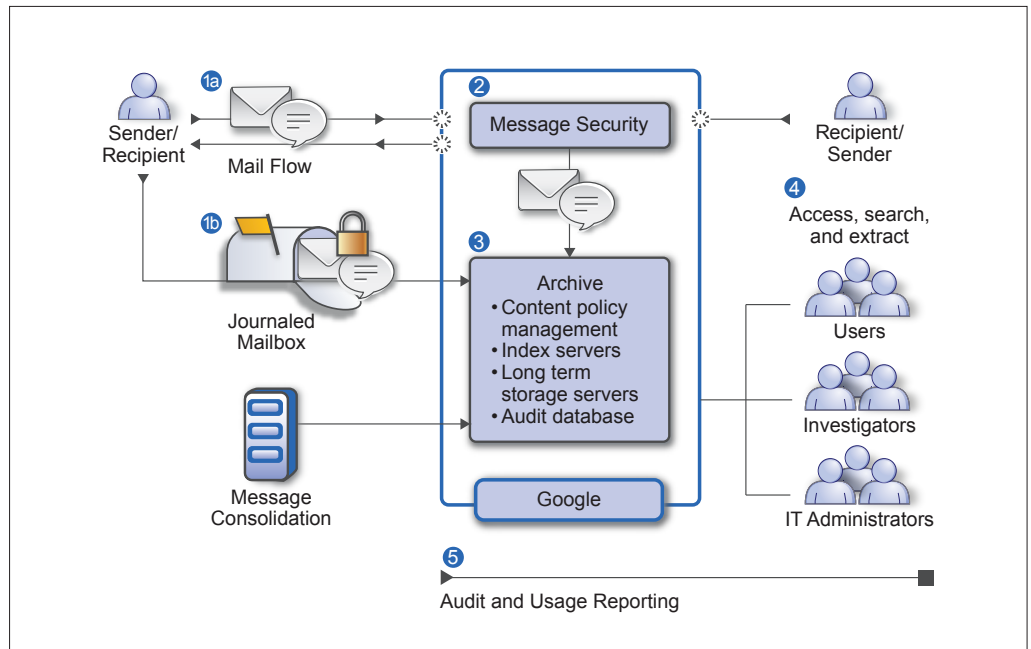


Figure 1: Message discovery flow

Google Message Discovery enables you to manage, protect, and access needed archival messages by providing:

- 1. Comprehensive message capture:** Messages are routed in real time to Google's secure data centers via the common envelope journaling capability on your email server. Alternatively, inbound and outbound email can be archived as part of the overall processing Google performs during our real-time threat analysis.
- 2. "Always on, always current" Message Security:** Routing messages through Google's market-leading Message Security functionality provides real-time threat protection, virus detection, content-based filtering, and policy-enforced TLS encryption.
- 3. Secure hosted archiving:** Messages and their attachments are stored and indexed in a central repository. Retention policy management enables IT to set policies at the user or organization to meet internal and external retention requirements.
- 4. Search, discovery, extraction and reporting tools:** Permission-based access provides authorized individuals with advanced tools to quickly and easily search, place litigation holds, and extract relevant email.
- 5. Extensive Reporting:** Usage and audit reporting provides the information necessary to monitor all activities that occur within the company archive.

SPECIFICATIONS

System Requirements

Use of the journaling option with Microsoft Exchange Server Standard Edition requires that at least two Standard Edition servers be on your network. One server must be reserved exclusively for receiving journaled messages and cannot contain any user mailboxes.

Feature	Benefits
Scalable, redundant storage in secure Google data centers	Avoid costly on-premise investment in infrastructure and maintenance and be confident email is secure and available
Administrative search interface and investigation management	Easily identify and collect email for legal discovery, internal investigations, and message recovery
Export messages in PST and MBOX formats	Quickly export individual messages or search results for recovery or for further review and analysis
Retention policy automation	Reduce risks and save time by implementing reliable and auditable email retention policies
Personal archive access	Allow end users to access their own email archive through a web-based interface or an Outlook™ toolbar
Litigation hold management	Preserve email in advance of or during litigation, eliminating manual processes and lowering risks
Audit reporting	Log all activity in the archive, including searches and exports
Spam, virus, and content filtering, powered by Postini	Deliver extremely effective spam filtering, low false positive rates, “zero-hour” virus protection, and 100% anti-virus SLA
Policy-based TLS encryption	Securely transmit messages within and beyond your organization
Email spooling	Receive messages without interruption in event of email server downtime

