

Google Message Discovery

Complete email security and archiving in one package



ABOUT GOOGLE SECURITY AND ARCHIVING, POWERED BY POSTINI

Google security and archiving products, powered by Postini, make email systems more secure, compliant and productive by blocking spam and other intrusions before they reach your network, and by providing encryption and archiving to help you meet compliance requirements. Google's hosted model leverages the "network effect" created by billions of daily email connections to detect and block threats in real time, without requiring on-site updates. Economies of scale in storage, along with simple deployment and maintenance-free service, drive a low total cost of ownership.

For more information, visit www.google.co.uk/postini

Make your email servers more secure, compliant, and productive. Block email threats before they reach your organisation. Create a secure and searchable email archive without making a significant infrastructure investment by storing messages in the cloud. Locate pertinent messages quickly and comprehensively even as your email volumes and compliance requirements grow. Leverage cloud services to reduce maintenance, protect bandwidth, and free up resources to work on strategic business initiatives.

Product Summary

Google Message Discovery, powered by Postini, is a secure, hosted service that provides enterprise-grade spam and virus protection as well as comprehensive email archiving for organisations looking for cost-effective email management and significant advantages over onsite server or media-based email archiving. Google Message Discovery lets you:

- create a centralised and searchable email repository for your organisation
- quickly search across the archive to find emails and save result sets
- secure your email from spam, viruses, phishing, and other email-borne threats
- set central email policies to manage content and compliance requirements

Google Message Discovery is hosted in the cloud and built on a Software as a Service (SaaS) model, so there's no need to forecast or plan for future storage needs. Google's secure and redundant data centres keep your messages fully protected and backed up, removing the risk of loss due to onsite server failure. Data ownership remains with your organisation so you retain the control over your information.

You can archive mail without worrying about disk space, and can eliminate storage quota headaches by giving users easy access to archived email. What's more, by removing aged mail from your servers, you can decrease both backup windows and recovery times.

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 organisation and ensure proprietary information that must remain confidential stays within your organisation.

Key Features

- **Secure and redundant** Ensure availability and redundancy by leveraging Google's network of secure, energy-efficient data centres. Minimise costly on-premise infrastructure and reduce IT maintenance
- **Scalable** Unlimited capacity without additional administration and contracts
- **Easy access and findability** Quickly pinpoint specific email without having to search multiple data sources
- **Export result sets** Quickly export messages or message sets into PST and MBOX formats
- **Manage retention policies** Reduce risks by implementing auditable email retention policies and preserve message sets beyond the retention period when required
- **End user archive access** Allow end users to access their own personal archive through a web-based interface or an MS Outlook toolbar, without IT assistance
- **Archive activity reports** View log reports of all archive activity including searches and exports from the archive for compliance needs

SYSTEM REQUIREMENTS

Google Message Discovery supports the following mail servers:

- Microsoft Exchange Server 2000 Standard or Enterprise Edition
- Microsoft Exchange Server 2003 Standard or Enterprise Edition
- Microsoft Small Business Server with Exchange Server 2000 or 2003 Standard Edition
- Microsoft Exchange Server 2007
- Lotus Domino 6.5–7x

To use the journaling option with Exchange Server Standard Edition, you need at least two of these servers on your network, with one server used exclusively for receiving journaled messages. The server cannot contain any user mailboxes.

- **Spam and virus protection** Provide market-leading email security including real-time spam and virus protection and content filtering for inbound and outbound email
- **Domain-to-domain encryption** Transmit secure messages with policy-based Transport Layer Security protocols
- **Intelligent routing** Easily route email traffic to de-centralised data centre locations

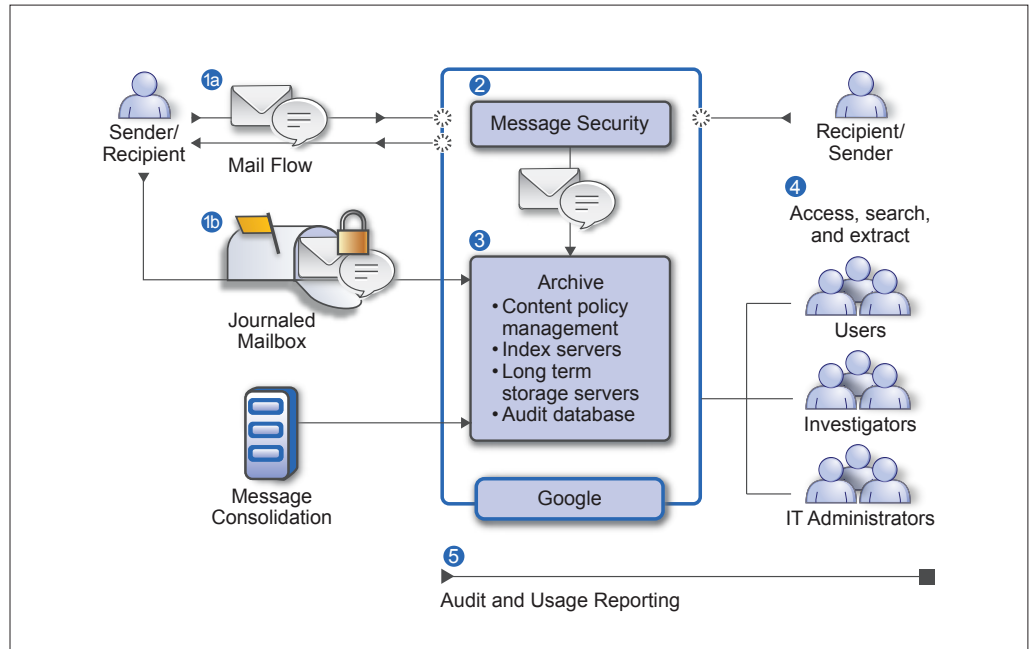


Figure 1: Message discovery flow

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 centres 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 organisation to meet internal and external retention requirements.
- 4. Search, discovery, extraction and reporting tools:** Permission-based access provides authorised 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.

