
OpenText™
OpenText™ Secure Mail
Secure email — simplified and integrated
OpenText Secure Mail is a cloud-based email solution that successfully tracks, controls and secures the transmission of confidential email messages and attachments.

OpenText™ Secure Mail

Do you know who's reading your emails? After sending one, did you ever wonder if the recipient actually opened it? What if you send something to the wrong email address by accident? Can you recall the message and verify whether it was read or not? For a typical enterprise these are serious questions. The news is filled with stories of data breaches, data theft and leaked proprietary information, yet the need to share confidential data via email remains critical. Today email communication is so risky that you can't afford to leave anything to chance regarding who is accessing your messages.

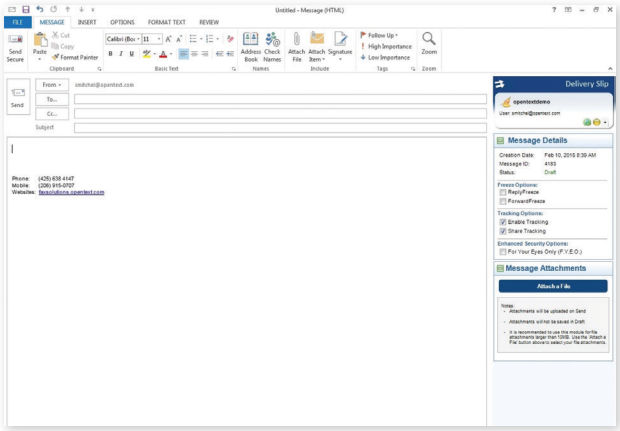
OpenText Secure Mail lets you easily exchange secure messages and attachments with each colleague, customer and partner. Secure Mail integrates with email systems to intuitively track, control and secure transmitted messages and files for users.

I might use…	But I can't because…
Email	It is easily intercepted and I can't track it after messages are sent
Encryption Add-ons for Email	They are complex, cumbersome and often require technical expertise to use
An Encryption Gateway	An encryption appliance tends to be expensive, and it's just another piece of hardware to manage.

REQUIREMENT	SECURE MAIL DELIVERS
TRANSMISSION SECURITY	State-of-the-art encryption for data in transmission and at rest in the cloud
PASSWORD PROTECTION	An added layer of security for any transmitted message
TRACKING	A patented Delivery Slip that tracks actions taken on messages by every recipient
DATA LOSS PREVENTION	Policy-based content filtration using keywords and/or regular expressions
MESSAGE RECALL	Quick elimination of messages transmitted in error
USABILITY	Multiple user interfaces make email communication simple and familiar - including Microsoft Outlook plug-in, Google Chrome plug-in as well as common web and mobile clients
BI-DIRECTIONAL MESSAGING OUTSIDE THE NETWORK	A web portal that enables secure messaging to any recipient with an email address
EASE OF MANAGEMENT	User self-provisioning and cloud architecture that lessens the management burden
ABILITY TO SEND LARGE FILES OR FILES OF SPECIAL TYPE	Quickly and securely share large file attachments of up to 5GB in size
MOBILE	Compatibility with iOS, Android, Windows® Phone and Blackberry through native applications
APPLICATION INTEGRATIONS	REST-based API's that drive robust integrations and added production capability
CONFIGURABILITY	Corporate branding, message expiration and archive capabilities

Simplify the Protection of Email Exchanges

Implementation of email security often fails for one reason – it is complex, cumbersome and requires a lot of work for typical users. Ever try to use Microsoft® Exchange Information Rights Management (IRM) feature? It's not pretty. Secure Mail, however, is designed for simple use throughout to make sending secure emails simple and familiar. Secure Mail accomplishes this by easily integrating with Microsoft Outlook® and by being accessible via multiple cloud email systems and on a variety of mobile platforms.

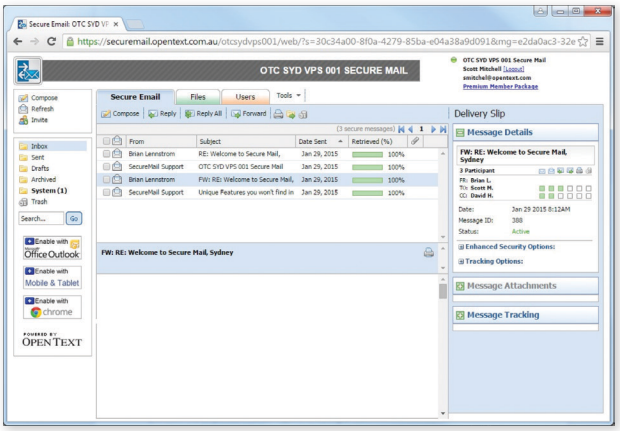


Manage secure messages in the world's most widely used enterprise email program, Microsoft Outlook.

Microsoft Outlook Plugin

The Secure Mail Microsoft Outlook Toolbar allows internal and external users to manage their secure messages alongside their basic email messages seamlessly in the world's most widely used enterprise email program. Once installed, any authorized user can use Outlook to create, read and respond to secure messages. Secure messages can make use of all existing Outlook features and corporate global policies.

The Secure Mail Outlook Toolbar conforms to the way users work within their email program. It seamlessly integrates with Outlook regardless of the mail system the Outlook client is accessing: Exchange (on-premises or hosted), Office 365, or Outlook.com.



The Secure Mail web portal offers secure access from any browser

Secure Mail Web Portal

The Secure Mail web portal is a full-featured web, mobile, tablet and visually impaired-enabled email program that gives users access to all their secure messages. The Secure Mail web portal looks and feels like a traditional email client with its inbox and outbox displays, email tools, preferences and account settings. It also allows users to download and enable the Outlook Toolbar and Desktop Agents.

Google Chrome Extension

The Chrome Extension installs in seconds and allows Gmail, Office 365 or Outlook Web Access (OWA) users to read, reply to and even search secure messages in Chrome without having to navigate the Secure Mail portal. The program allows for this all while keeping the content private from email hosting providers. The simple user interface requires no training to learn.

Secure Mail Apps for Mobile Devices

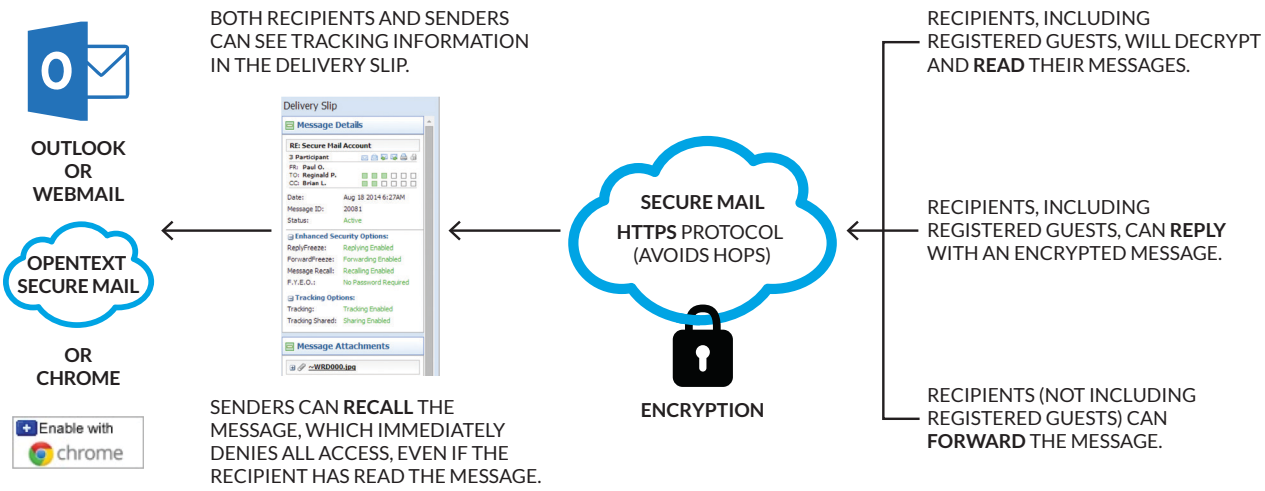
Mobile Clients

Secure Mail supports multiple mobile devices and clients to enable secure communication – even when not using a corporate device. Struggling with securing data in the age of BYOD? If users decide to bring their own non-company IT into your organization, the Secure Mail network policies will create an environment of full security. In fact no Secure Mail messages or attachments are stored on mobile devices. If you lose your phone, or if it's stolen, your confidential data will remain secure.

The Secure Mail App is a powerful and flexible enterprise email encryption solution for mobile users. It provides email encryption, real-time tracking and all other features available with Secure Mail. Secure Mail for iOS, Android Windows Phone or Blackberry requires no enterprise-level installation.

Create, read and reply to secure messages on any iPhone, iPad, Windows or Blackberry device through the use of native mobile apps. The Secure Mail mobile application is free for all users and available on the Apple iTunes App Store, Google Play App Store, Windows Phone Store or Blackberry World.

Easily Track, Secure and Control

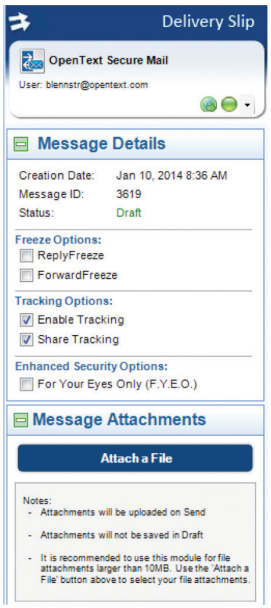


Track

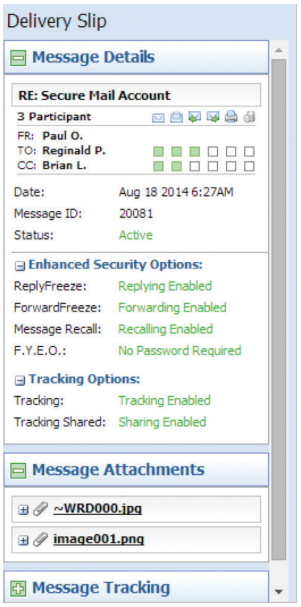
For both sender and recipients, the Delivery Slip tracking feature displays a list of message participants, and whether or not each participant has:

- retrieved the secure message (if the recipient has set their preferences not to automatically retrieve Secure Mail messages)
- read the secure message
- replied to the secure message, and when
- forwarded the secure message and when and to whom
- printed the secure message though the Secure Webmail portal
- deleted the secure message though the Secure Webmail portal

Every action is recorded with a date stamp and IP address. As a sender, you can share this information with other participants, keep it private to the sender, or disable either on a per message basis or across the entire organization.



Microsoft Outlook Plug-in



Secure Webmail Portal

Secure

Secure Mail protects your data wherever it is – even when you access it using your phone. Data is secured in transit with a minimum of 128-bit SSL connectivity and at rest with AES256-bit encryption. No secure message content is ever delivered via the standard unencrypted Simple Mail Transport Protocol (SMTP) used by ordinary email systems. Instead, communications between customer email servers and Secure Mail are secured by HTTPS – the same level of security used for making online banking transactions. Secure Mail only uses state-of-the-art, Tier-1 data centers located around the world and across selected "data zones".

Administrative settings include:

- Blacklist registrations by domain, if desired
- Requirement for new users to validate themselves based on a specific set of criteria
- Security settings defined by user (e.g. automatic use of Secure Mail for all messages and/or users, if desired)
- Message expiration settings so messages are deleted from the OpenText cloud after a set number of days
- Ability to print secure messages through the Secure Webmail portal
- Archiving enabled so that sent and received secure messages are housed in your Exchange store in an unencrypted state, for e-Discovery and other purposes.

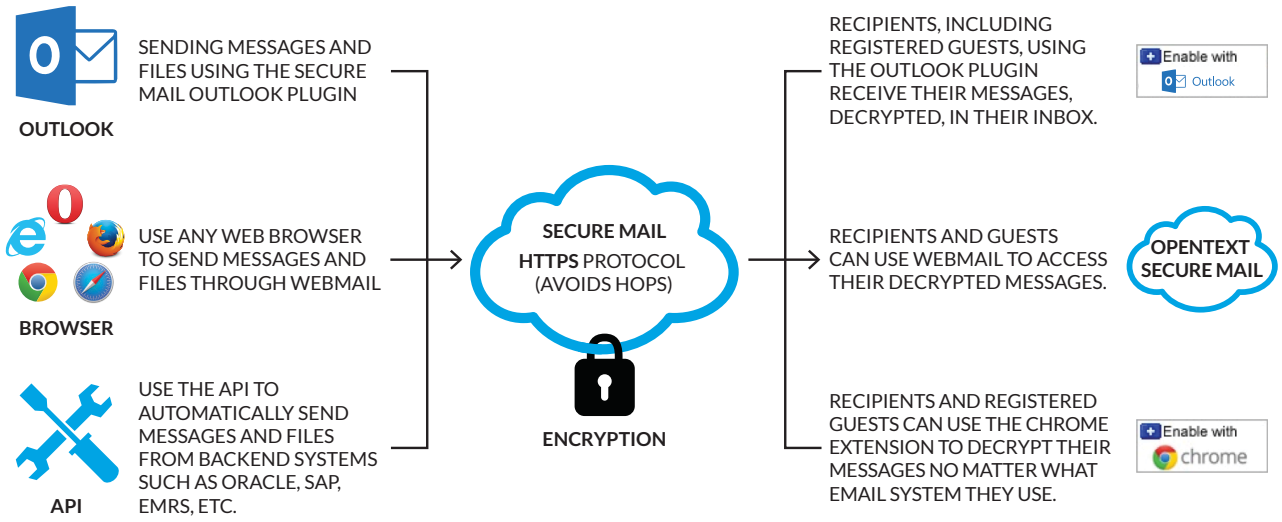
Control

Data Loss Prevention

Pre-emptive Data Loss Prevention allows keyword inspecting of all messages (secure and non-secure), black listing of message content, and enforces or recommends using Secure Mail based on policies before messages are actually sent (as centrally set by the group administrator). Policy control takes place dynamically – on 'SEND' - before the message is transferred to the server. This is significantly different (and more effective) than solutions which rely on ad-hoc parsing or outgoing message filters. You can create enforcement rules based on:

- **A regular expression** – allowing control over email that contains specific patterns like social security and credit card numbers
- **A keyword** – such as "confidential" or "financial results"
- **An email address or email domain**

Messages that do not meet the organization's enforcement rules can be blocked or sent securely using the unique 'Enforce Secure' feature. Secure Mail can also suggest that messages be sent encrypted, while still allowing the option for them to be sent in an unencrypted format.



Sending Messaging with Secure Mail

There are 3 main ways to send secure messages using Secure Mail: the Outlook Plug-in, a web browser using Webmail, and the API.

When sending messages using the Outlook plug-in, once the "Send" button is pressed, the toolbar intercepts the command and re-routes the email message via SSL instead of sending the message via SMTP. At rest in the cloud, the message content and file attachments are encrypted.

- If using the Outlook Plug-in, recipients, including registered guests, will receive their messages, decrypted, in their Outlook inbox.
- If not using the Outlook Plug-in, recipients can use Webmail or the Chrome extension to access their decrypted messages.

Senders can recall the message even after the recipient reads it, reducing the problem of an accidental send. Also, registered guests have their messages decrypted, can read the message, and reply back with an encrypted message (although they cannot forward it).

Simple Cloud Deployment

OpenText Secure Mail is a cloud-based service. It does not replace existing email servers or current email addresses, it complements them. Unregistered email recipients outside your organization are automatically invited to join the customer-branded Secure Portal as a 'Guest User.' From that point, they have limited use of the service, free of charge.

Keep Confidential Emails Secure and Private

Secure Mail protects your outbound messages in a way that reduces exposure to risk. For example, you have to send emails containing confidential or proprietary information, but cannot use regular email because it "is full of holes" from a security standpoint. In that case, Secure Mail offers a solution that works right in email, but provides the security, control and tracking you need over confidential material. This is essential for industries with regulations requiring email solutions that protect your confidential information and facilitate security compliance. Secure Mail has the type of risk mitigation built in that helps you comply with government and market-driven regulations for transacting business electronically.

E-Discovery

In the event you need to archive email messages for e-discovery purposes, Secure Mail provides secure, long-term storage that drives litigation preparedness.

Data Sovereignty

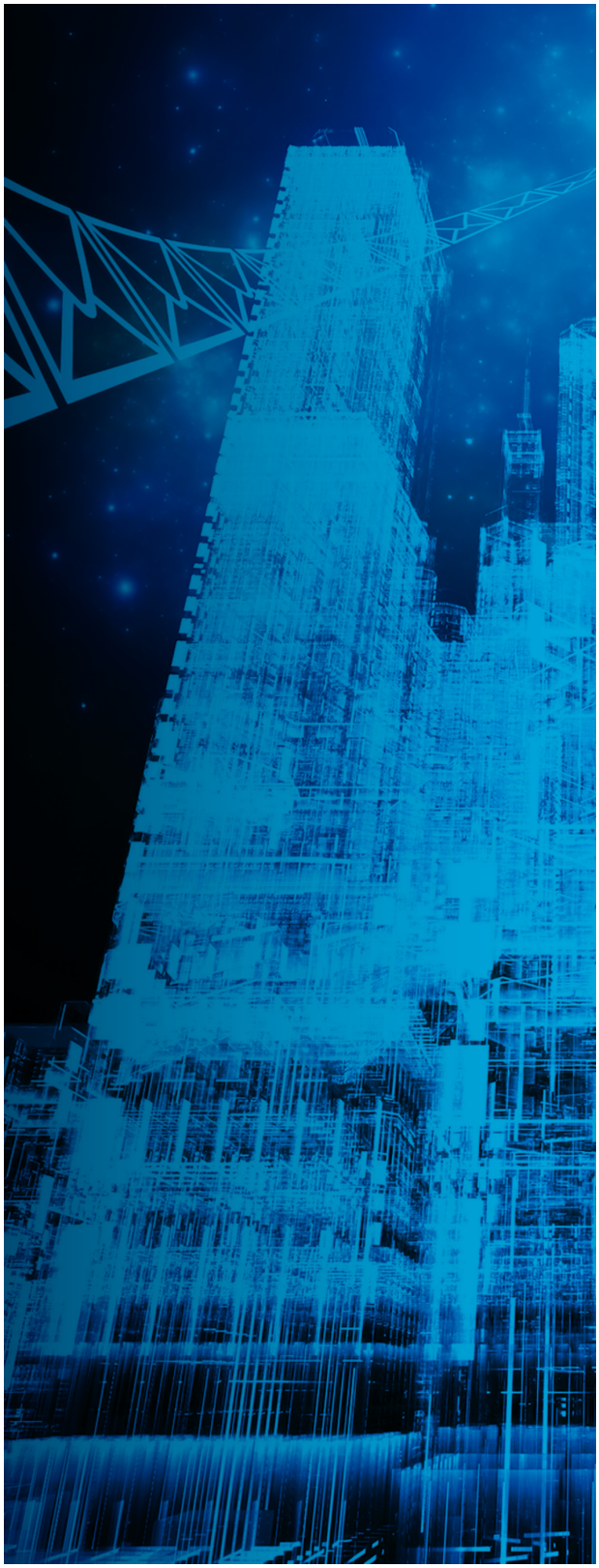
Secure Mail addresses data sovereignty, privacy and compliance concerns with in-region processing and dedicated infrastructure.

OpenText has the ability to store and process customers' email sent via Secure Mail strictly within "data zones" by operating data centers in Ashburn, VA USA; Frankfurt, Germany; or Sydney, Australia. This in-region processing capability was designed to help address privacy and data sovereignty concerns for customers who have requested in-region processing. Thus, all emails sent via Secure Mail will be stored exclusively at the regional data center, and all metadata processing, user authentication, and auditing information recording will handled exclusively at the same regional data center.

Solve Email Security Problems

Common Use Cases

- **Missing Children Alerts**: Agencies that track information about missing children are required to encrypt any transmitted information announcing a missing child.
- **High School Grade Reports**: High schools that forward grades, reference letters, etc., to colleges as part of the application process require messaging tools that are both highly secure and easy to use.
- **Financial Services**: Financial institutions have very tight policies around how confidential information is sent; for example, any tools used to send messages must fully support data leak protection.
- **Email Confirmation Messages**: In many cases, a business may like to gauge interest in the information it sends to recipients. More specifically, it wants to know if the emails were received, read, forwarded, or deleted/printed.
- **SMTP Alternative**: Hackers, agencies or individuals take copies of your email from one of the "hops" that SMTP email usually takes in their transmission journey. These instances require a solution that protects information from sender to receiver against this type of threat.
- **Legal Correspondence**: Many companies want to reduce the risk of forwarding sensitive legal documentation that should not go through ordinary email channels.
- **Human Resources**: Organizations need to communicate human resources information to both current and former employees. Much of this information is highly confidential, and these companies need a secure messaging solution to forward it to ensure the proper individuals receive it.



OpenText Secure Mail Quick Facts

- Fully integrates with all email applications
- Optional ability to send a copy of all sent and received messages to a central mailbox for archival purposes
- Supports mobile and tablet devices through native apps
- Offers data leakage protection without requiring an expensive gateway deployment at the perimeter, mitigating the risk of breach of confidential data
- Rapid deployment in the cloud, and easy user self-registration eliminates expensive encryption project and deployment costs
- Documented REST-based APIs enable integration into applications and workflows
- Allows archiving of secure messages decrypted to any third party cloud archive solution (on-premises or hosted)
- Total Message Recall – even received messages can be recalled to prevent further reading
- Comprehensive message tracking – see status of each message for each recipient
- Configurable user permissions, white labeling, message expirations
- Exchange large file attachments without taxing your network or the mail server

www.opentext.com/securemail

NORTH AMERICA +1 800 304 2727 • EUROPE, AFRICA +31 (0)23 565 2333 • MIDDLE EAST +971 4 390 0281
JAPAN +81-3-4560-7810 • SINGAPORE +65 6594 2388 • HONG KONG +852 2884 6088 • AUSTRALIA +61 2 9026 3400