OpenText Secure Mail

Secure Email Simplified and Integrated

OpenText Secure Mail (Secure Mail) is a cloud-based secure messaging solution for encrypting, tracking, and preventing the leak and interception of confidential information. It enables internal and external users as well as applications to easily exchange secure messages and attachments. Users can send, receive, and track from any device and any location.

Secure Mail is cloud-based secure messaging designed to integrate into and enhance your existing email infrastructure. Secure Mail's unique, deep integration with email systems makes exchanging and tracking encrypted messages and files remarkably intuitive and transparent for users. Its ability to integrate with your organization's applications and workflows creates productivity gains. By improving secure communication and reducing data leakage, Secure Mail gives enterprises the control they need over email.

Key differentiators include:

- Tight integration with existing email infrastructure that delivers a superior user experience
- Enables integration into applications and workflows for all user and application-initiated sending use cases
- Simple cloud deployment without hardware installations
- Easy-to-implement policy-based data leakage prevention
- Message tracking, "for your eyes only," and policy control features easily managed from the message window

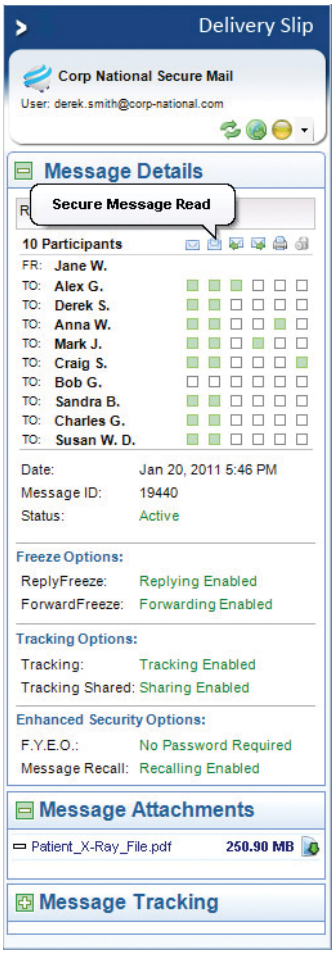
In the Cloud

OpenText Secure Mail is offered as a cloud-based service. It does not replace existing email servers or current email addresses, it complements them. New 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.

OPENTEXT SECURE MAIL QUICK FACTS

- Fully integrates with Microsoft® Outlook for both internal and external users ensuring all participants have the decrypted messages in their email server and are not forced to use a separate mail store / web browser
- 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-premise or Hosted)
- Total Message Recall – even received messages can be recalled to prevent 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

iOS and Android Secure Mail Apps



The patented 'Delivery Slip' is a window to the secure message.

Microsoft Outlook Plugin

The Secure Mail Outlook Toolbar allows users to seamlessly and transparently manage their secure messages alongside their basic email messages in MS Outlook®. Once installed, users never have to leave Outlook® to create, read, respond, forward and track secure messages. Corporate DLP policies are applied through Outlook as well.

The Outlook Toolbar integrates with Microsoft Exchange® (on-premises or hosted), Microsoft Office 365®, Google® Mail, as well as external or guest user's individual personal email such as Gmail® or Yahoo Mail®.

Secure Mail Web Portal

The Secure Mail Web Portal is a full featured web service that gives users access to all of their secure messages and file attachments from any web browser, from any device. It looks and feels like a traditional email client with its inbox and outbox displays, email tools, and account settings, which makes it intuitive to use.

Secure Mail Delivery Slip

Secure Mail's patented Delivery Slip is a unique window in every message used to set security options and track details on a per message basis. Its deep integration with Outlook enables users to easily track key information about each secure message sent, the sender and recipients, and what actions have been performed on the secure message.

With just a few clicks, users can quickly and easily set the following options directly from the Delivery Slip.

Security Options

- Prevent message replies
- Prevent message forwards
- Password protect attachments
- Recall message

Tracking Options

- Reviewed the Delivery Slip but not read the secure message.
- Decrypted and read the secure message.
- Downloaded any file attachments.
- Replied to the secure message and to whom.
- Forwarded the secure message, and to whom.
- Printed or deleted the secure message.

Data Leakage Prevention

Secure Mail offers easy-to-implement policy-based data leakage prevention to help organizations gain greater control over their email, prevent a breach and protect their brands. It enables keyword and regular expressions filtering of messages and enforces secure delivery based on policies set by the group administrator.

Production Secure Messaging

High-volume, production secure messaging has tremendous appeal because of its efficiency; however, realizing it has been difficult…until now. Secure Mail offers fully documented REST-based API's that facilitate the integration into back-end applications such as ERP and billing systems. Integration with back-end applications that overcomes the hurdle of external user decryption and delivers new efficiencies with application generated secure messaging.

OpenText Secure Mail Mobile Apps

The Secure Mail App is a powerful and flexible enterprise email encryption solution for mobile users of the Secure Mail. It provides email encryption, real time tracking, compliance services and all other features available with Secure Mail. Unlike other solutions, Secure Mail for iOS® or Android® requires no enterprise level installation. Administrators can globally manage compliance policies on any device, and mobile data is secured in the cloud against loss.

REQUIREMENT	SECURE MAIL DELIVERS	
SECURITY	State-of-the-art encryption for data in transmission and at rest	■
USABILITY	Delivers a familiar user interface by leveraging existing customer email infrastructure – no training required	■
BI-DIRECTIONAL MESSAGING OUTSIDE THE NETWORK	Web portal enables secure messaging to any approved receiver with an email address	■
TRACKING	In the Delivery Slip, track actions taken on messages by every recipient	■
APPLICATION INTEGRATIONS	REST-based API's that enable integrations and production capability	■
EASE OF MANAGEMENT	User self-provisioning and cloud architecture lessen management burden	■
DATA LEAKAGE PREVENTION	Policy-based encryption based on keywords and/or regular expressions	■
MOBILE	iOS and Android Apps	■
CONFIGURABILITY	White labeling, user permissions, message expirations, local store	■

Create, read and reply to secure messages on any iPhone®, iPad® or Android device through the use of native mobile apps, or any other mobile or tablet device through the use of the mobile-enabled thin client Webmail Portal.

The Secure Mail mobile application is free for all licensed users and is available on the Apple iTunes App Store and Google Play App Store.

OpenText Secure Mail System Requirements

- Web browser connected to the Internet.
- Optional Outlook Toolbar (2003, 2007, 2010, 2013) all Editions.
- Optional Desktop Agents for Windows and Mac.
- Optional Native Apps for iPad, iPhone and Android.
- Does not conflict with other email applications, including PKI & TLS-based encryption applications.
- Works with any and all mail servers – no exceptions: Exchange (on-premises or hosted), Lotus® Domino, Zimbra®, Google Mail. ■