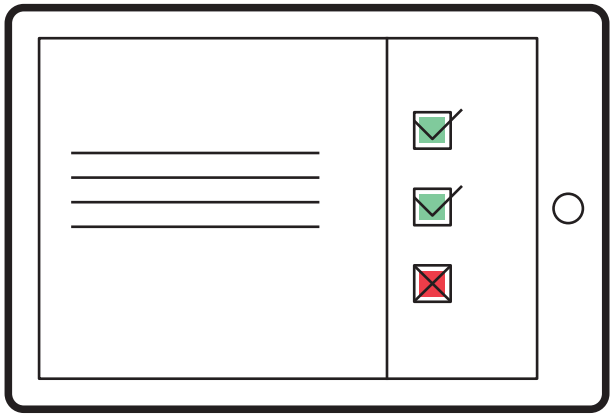
Secure Messaging

Secure communications simplified

Secure Messaging is a powerful, secure, cloud-based communications and information management solution that enables regulated and non-regulated organizations to effectively protect, control, and manage communications.



Secure Messaging
Overview

Secure Messaging makes it simple to send and receive secure messages, request or provide legally valid e-signatures, and share large files directly from your existing email address. It provides real-time message tracking and control, along with enhanced regulatory compliance and archiving capabilities. There's no complex installation required, it takes minutes to set up, and is fully functional on mobile devices.

Secure

Secure Messaging transforms a normal, unprotected email environment into a secure communications workspace. All messages, attachments, and e-signed files are cryptographically hashed and delivered via secure cloud rather than over basic unsecured email without requiring any additional hardware or additional software beyond the easy-to-install app that integrates right into your email environment.

All messages and their contents are stored "at rest" using AES256bit encryption in your dedicated cloud portal (and can be delivered to your archive) for easy retrieval at any time. Enterprise deployments can also opt for custom encryption salt and hashing of data.

Simple

Secure Messaging seamlessly integrates into existing email environments such as Outlook, Office 365 and Gmail, and getting up and running is as simple as your users accepting an email invitation.

Because users are authenticated using existing addresses without having to create an additional profile, Secure Messaging can integrate right into your SSO environment and works with your DLP deployments and archiving systems. This means there is very little disruption to your users' workflow or to your enterprise.

All of Secure Messaging's robust features are readily available in the Delivery Slip control panel that accompanies every secure message. This includes secure e-signatures, large file sharing, and managing real-time tracking options.

The fully functional mobile and web apps ensure that your sensitive data will be secure even when your users are on the go (and using potentially dangerous unsecured Wi-Fi).

Secure Messaging
Delivery Slip

The Delivery Slip is an advanced control panel that appears next to every secure message for managing features such as sharing large files, requesting or providing e-signatures, and managing your tracking and control options.

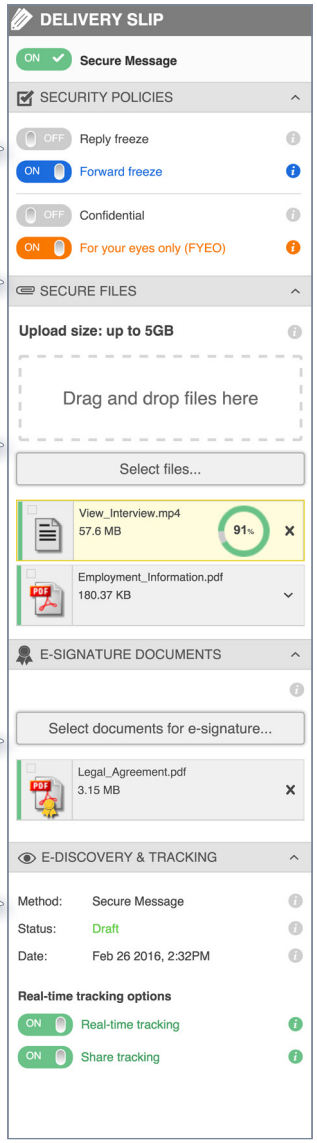
Prevent unauthorized use with unique message controls.

Password-protect messages and their attachments for added security.

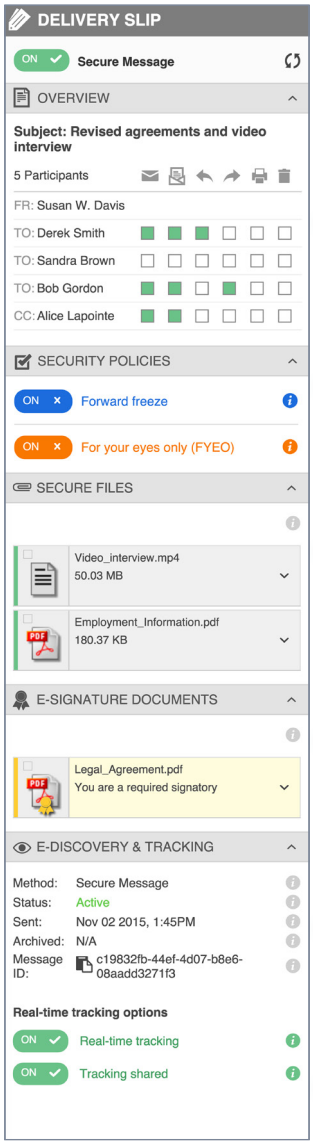
Share files up to 5GB securely from any device, regardless of other limits in place.

Securely request legally binding e-signatures on documents and images.

Monitor messages in real-time and receive (and share) provable notification of delivery and open times.



Compose view



Receive view

View real-time message notifications and granular message tracking, including who opened the message, if it has been responded to or forwarded, and more.

Review detailed message information, including which security policies the sender enabled.

Securely download large files regardless of any restrictions imposed by your email provider.

Provide a legal e-signature on documents right from the Delivery Slip in seconds simply by opening the file and typing your name.

Enable and simplify e-discovery and archiving (and retrieval) with a unique message ID on every message.

Be notified of whether the message is being monitored and if you have access to the details.

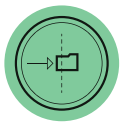
Secure Messaging
Features & Benefits

“Click to Acknowledge” Secure E-Signatures

Secure Messaging makes it easy for you to securely request and provide e-signatures on documents and image files directly within a secure message. The process takes seconds at either end and is fully secure from start to finish, ensuring data integrity, regulatory compliance, and non-repudiation.

It requires no additional workflow (i.e., no extra software or app) and, because the actual master document is stored in the cloud, users can sign it at any time without having to wait for it to be transferred between signatories. Plus, with the real-time tracking options available in Secure Messaging, you always know the exact status of the document and who has (or has not yet) signed it.

Because the process is secure throughout and accompanied with time and date information, all e-signatures are legal, non-repudiable, and satisfy legislative requirements where they exist (such as E-SIGN, GLBA, HIPAA in the U.S.; PIPEDA in Canada; and the Electronic Transactions Act in Australia).



Secure Large File Sharing

Secure Messaging lets you easily and securely share large files of up to 5 GBs. Files sent through Secure Messaging are unaffected by email bandwidth limitations and will not clog company email systems because they are uploaded and downloaded via the cloud.

Scales to Match Your Needs

Because Secure Messaging is a simple add-on to existing email environments, there is no limit to how many users you can have and no need to set up elaborate hardware/software environments. You can license as many professional users (e.g., your employees or clients) as you need, while all guest users are free, thus enabling you to secure your organization’s communications across the enterprise as well as externally with customers, partners, suppliers, and more.

Branded to You

Secure Messaging integrates into your branded environment to ensure the integrity of your organization is maintained and so that at no point during the exchange will anyone think they are dealing with anyone but you. The absence of documents having to go through 3rd-party solution providers will not only allay users’ fears that the process is not secure, but it will bolster your brand and authority as an organization that knows how to effectively and securely conduct business in a digital economy.

Secure Messaging
Features & Benefits

Advanced Message Control and Notifications

Secure Messaging's Delivery Slip notifies you in real time when an email is received and read and lets you easily control whether messages can be replied to or forwarded. You can apply additional password protection to individual messages for sensitive information, and can also set messages to expire at a later date and even recall messages sent in error, even after they've been delivered. You can be notified when files are downloaded and when requested e-signatures have been provided.

Full Mobile Functionality

Secure Messaging and all its features are fully enabled on mobile devices, including iOS, Android, Windows Mobile, and Blackberry 10. This means, for example, that a required signatory on a time-critical file can e-sign right from their device, wherever they are, without having to return to a desktop or use additional programs or apps. As well, for even greater protection, Secure Messaging supports fingerprint authentication on iOS devices.

Supports Regulatory Compliance and E-Discovery

For most regulated industries or any organization that needs to archive electronic communications, managing the storage and retrieval of communications is onerous and often costly given that it often requires third-party archival services. Plus, PKI-encrypted messages may become difficult or impossible to retrieve if the encryption key is lost.

With Secure Messaging, all data is MD5-hashed for later comparison and validation of the original information (which always includes verifiable records of whether messages were received and when they were read). Hashed documents are stored indefinitely on the Secure Messaging portal (and can be stored decrypted into your existing third-party archive) regardless of the data retention policies set in place for your portal, ensuring auditability at any time.

Secure Messaging enhances compliance with major privacy and security laws and regulations (including major legislation such as E-SIGN, GLBA, and HIPAA in the U.S.; PIPEDA in Canada; and the Electronic Transactions Act in Australia).

Dedicated, Customizable, Secure Cloud Environment

Secure Messaging provides businesses with dedicated space on its secure cloud servers and is fully customizable to security policies. As well, every Secure Messaging portal is custom-branded and encrypted for a seamless user experience.

Secure Messaging
Features & Benefits

Complies with Data Jurisdiction Requirements

Your organization gets a secure, dedicated area in the Secure Messaging Cloud Command Center in your region (there are dedicated servers strategically located worldwide). You choose where your data is hosted to help ensure data jurisdiction compliance.

Prevents Data Loss

Secure Messaging works with any existing data leak prevention (DLP) engine to help prevent unauthorized or mistaken sharing of sensitive or prohibited content and offers “intelligent content scanning” based on security policies.

Integrates with SSO Environments

Secure Messaging seamlessly integrates with existing SSO deployments (whether SAML2.0 or OAuth2.0). Plus, using your own federation service for authentication adds additional reputation to verifying the authenticity of every user action without requiring the use of complex keys. (Available with the Enterprise Dedicated Cloud service.)

Provides Unlimited Secondary Domains

For enterprise-level clients, in addition to a dedicated URL, unlimited secondary domains can be configured to enable enterprise-wide secure messaging for all of your email addresses, from .com to .org and beyond.

Integrates into Other Apps

The Secure Messaging API is available as a rest-like API for developers who want to embed secure messaging features such as secure e-signature into other business solutions such as CRMs, EMRs (electronic medical records) or any third-party application with Web API capabilities

Provides Dedicated Cloud Control

Secure Messaging give you complete control over portal user groups, daily email-send restrictions (SPAM throttling), access permissions, and the ability to enable and disable Outlook and mobile apps. You can also:

- Leverage two/three-factor authentication for user registration;
- Customize SMTP relays for secure notification delivery (support for Sender Policy Framework [SPF] and Domain Message Authentication Reporting & Conformance [DMARC] records for anti-spoofing);
- Customize URLs for branding purposes;
- Leverage SSL certificates to control the level of encryption in transit.