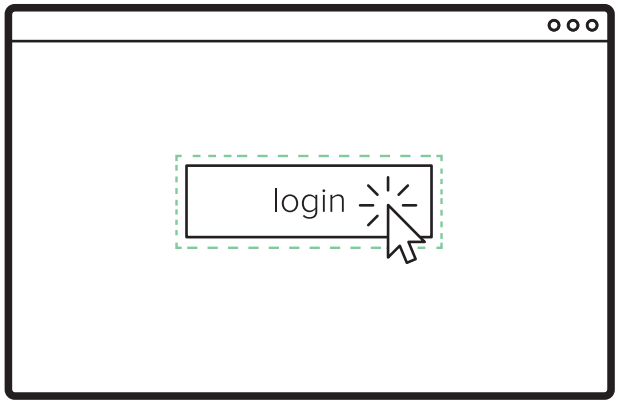
Secure Messaging **Single Sign-On**

Secure Messaging seamlessly integrates into your enterprise SSO to give your users total email security and an extra set of robust communications tools.



Secure Messaging **Single Sign-On**

Single sign-on (SSO) systems create a single user authentication environment across multiple systems, organizations, and/or websites. They reduce the need for users to remember multiple profiles and enhance the security of an organization or entity by streamlining user access and data security.

Seamless SSO Integration

Common SSO environments include SAML 2.0, an XML-based open standard data format for exchanging authentication and authorization data between parties (in particular, between an identity provider and a service provider), and OAuth 2.0, which allows secure authorization in a simple and standard method from web, mobile and desktop applications.

Secure Messaging seamlessly integrates with such SSO deployments (whether SAML 2.0 or OAuth 2.0) without requiring new identities for users. As well, Secure Messaging quickly and seamlessly integrates into existing email environments, including Outlook, Office 365, and Gmail, along with DLP engines and archiving systems. Because integration into your existing environment is seamless and the learning curve is minimal, new users can be up and running with Secure Messaging in minutes.

Secure Messaging makes it simple for your enterprise users to securely send, receive, track, and control email messages and attachments internally and externally on any device.

Because Secure Messaging comes branded to your organization and integrates right into your environment, there's very little disruption to your users. Not only does this make the transition to a secure communications workspace simple, but it also increases the likelihood of user uptake since they won't be frustrated by having to learn a new system. Not only do you benefit from infrastructure cost savings, you can streamline enforcement of security policies without disrupting core business processes.

As well, fully functional apps for iOS, Android, and other platforms are free and easy to install and use. This means that in a BYOD world you can ensure that your users are authenticated and their communications are secure even when they're on the go. This is especially critical if they are conducting company business over open (and often remarkably unsecure) WiFi networks.

Secure Messaging **Single Sign-On**

Features & Benefits

- Simple set up
  Secure Messaging has no hardware to install, deploys in minutes, and requires no outside IT expertise to set up.

- Unlimited scaling
  Because it's a cloud solution, Secure Messaging scales to match your needs with no limits on the number of professional users you can license or guest users you can invite.

- Users keep their existing profile
  Because users are authenticated using existing email addresses, they don't need to create (or have to remember) an additional profile.

- Fully integrated with Outlook & Office 365
  Secure messages can be received, opened, replied to, saved and indexed directly from within Outlook and Office 365.

- E-signatures built in
  Users can easily and securely request and provide e-signatures on sensitive documents (such as contracts, financial details, personal health information, etc.). The process is simple and takes seconds at either end of the exchange without requiring additional complex workflows. It supports common document formats (PDF, DOC, PPT, etc.) as well as most image formats (JPG, GIF, PNG, etc.).

- Share large files securely
  Users can easily and securely share large files (up to 5 GBs) without taxing the network or the mail server, thereby saving network bandwidth, improving productivity (since the user can do everything right from within email), and reducing the costs of needing additional file-sharing products or couriers.

- Real-time notifications
  With detailed real-time notifications for all activity, you can know exactly who, when, and where protected information is accessed, giving you the peace of mind that your data is being handled by authorized recipients.

- Every exchange is non-repudiable
  Because all exchanges are verified and time-stamped, all messages sent, files shared, and e-signatures provided are non-repudiable.

- Advanced message controls
  Along with real-time notifications of activity, Secure Messaging lets your users easily control whether messages can be replied to or forwarded. Messages can be set to expire at a later date, and even completely recalled if sent in error—even after they've been delivered.

Secure Messaging **Single Sign-On**

- Additional security options
  For especially sensitive information, your users can use the Confidential and FYEO ("For your eyes only") features to apply additional password protection to individual messages. With Confidential, to unlock the message, the recipient must enter their authentication credentials. With FYEO, the recipient unlocks the message using a password that you provide them with (outside of email, such as over SMS).

- Works on any device
  Fully functional mobile apps for iOS, Android, and other platforms ensure the security of company communications beyond the enterprise security perimeter.

- Add your own authentication layer
  Using your own federation service for authentication adds additional reputation to verifying the authenticity of every user.

- Only the highest security standards
  Secure Messaging encrypts all data using the highest security standard (AES-256 encryption) using the most advanced cloud-based architecture.

- Support for third-party archiving systems through our API
  Secure Messaging supports all standard third-party compliance archiving systems and document management systems through a powerful rest-based API, and ensures that every message is secure, tracked, and auditable.

- Enhanced e-discovery features
  Secure Messaging supports the full spectrum of information privacy and security regulations. For e-discovery purposes, it ensures messages are verified and intact, and provides real-time knowledge about whether messages were received and read, using date and time stamps.

- Compliant with major laws and regulations
  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 and secure cloud environment
  Secure Messaging gives you a dedicated "slice" of the secure cloud that is fully customizable to match your security policies. The portal is branded and encrypted to your needs, simplifying and securing account admin.

- Choose where to host your data
  With servers located globally, you can choose where your enterprise data is hosted to comply with data jurisdiction requirements.

Secure Messaging **Single Sign-On**

- Easy to integrate
  Secure Messaging's technology architecture allows it to easily integrate with other IT systems, meaning that each secure message is not "held hostage" by a single encryption key, which for an average organization can add up to millions of encryption keys (a nightmare for content management should these messages need to be decrypted by anyone but the receiver).

- Email masking options
  Secure Messaging lets users mask sender email addresses and subject lines to ensure maximum privacy and data security.

- Complete admin control
  Secure Messaging gives you complete control over portal user groups, daily email-send restrictions (spam throttling), access permissions, and the ability to enable/disable Outlook and mobile apps. You can also:
  - Leverage two/three-factor authentication for user registration;
  - Customize your own SMTP relay for secure notification delivery (support for Sender Policy Framework [SPF] and Domain Message Authentication Reporting & Conformance [DMARC] records for anti-spoofing);
  - Customize your own URL for branding purposes;
  - Leverage your own SSL certificate to control the level of encryption in transit.