



Echoworx Encryption Delivery Methods

Contents

Overview	4
TLS Encryption with Fallback	4
Encrypted PDF	6
Encrypted Attachment	7
Certificate Encryption	8
Web Portal Encryption.....	9

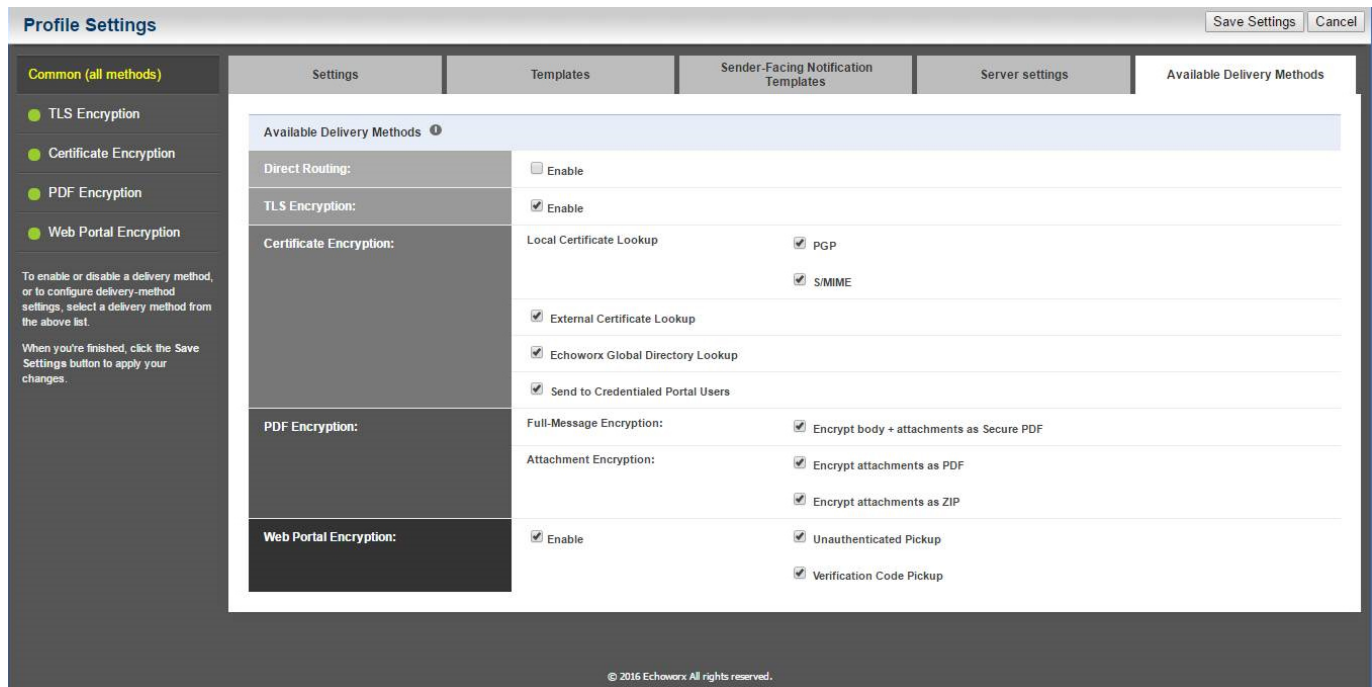
Overview

Do you need email encryption for secure communication with business partners? Do you need to provide a seamless user experience for sending and receiving encrypted messages?

Balancing message and document encryption with a customer-centric user experience is a common pain point among organizations and across industries. Providing a flexible email encryption solution can help crack this conundrum – enabling seamless secure communications.

Echoworx Email Encryption offers an extensive suite of secure delivery options – enabling organizations to meet a wide range of business use cases and branding requirements. Unique benefits to each encryption method ensure messages are protected in transit and accessible anywhere, on any device. And, with available customizable policy options, organizations can be rest assured correct delivery methods are applied on a case-by-case basis.

Echoworx offers **eight secure encryption delivery methods**: TLS Encryption with Fallback | Encrypted PDF | Encrypted Attachment (PDF, Office 365, ZIP) | Certificate Encryption (S/MIME and PGP) | Web Portal Encryption



TLS Encryption with Fallback

Seamless encryption of messages and attachments is provided in transport direct to the recipient – with no additional setup or password requirements.

- ✓ TLS connection is verified for validity on-the-fly.
- ✓ Configure an 'Allow List' - only send to - or 'Block List' - do not send - of TLS domains through a web-based administration console.

FEATURES

- Senders simply send messages, and our encryption platform takes care of the rest.
- No need for recipients to change behaviour – full transparent delivery.
- If TLS is not available, Echoworx automatically offers secure fallback delivery options, like Web Portal or Secure PDF – ensuring messages are not undeliverable or sent unprotected.
- Extensive message branding options for headers and footers.
- Support for 27 languages.
- Ideal for B2B environments where both parties use TLS.

LIMITATIONS

- Secure messages are not encrypted at-rest, after they are received.
- TLS must be available to enable secure replies.

Encrypted PDF

Encrypt both body and attachments contained within an outgoing email using standard Secure PDF, Office 365, and ZIP technologies.

- ✓ Self-Registration: Recipient receives a one-time prompt to set their own password.
- ✓ Registration process can also include an out-of-band confirmation.
- ✓ Authentication can be through existing customer portals without the need for additional URLs. The customer logs into an existing portal and is auto logged into a PDF password management portal via webservice calls.
- ✓ Sender-Set Password: Recipient provides the password set by the sender at time of sending through a plugin or subject line trigger.

FEATURES

- Enables more flexible delivery – anywhere on any device.
- Extensive branding features for all customer-facing webpages, encrypted messages, and message notifications.
- Support for 27 languages.
- Deliver encrypted PDFs direct to an inbox.
- Secure messages remain encrypted at-rest.
- Offline message access.
- Options for sender or recipient set passwords.
- Secure reply functionality with the option to have a secure copy for recipient.
- Access via any standard PDF viewer on any device.

LIMITATIONS

- Limited message audit and tracking options.

Encrypted Attachment

Deliver sensitive documents via regular email as encrypted attachments. This option is useful for generating and processing bulk electronic statements, for example.

- ✓ Encrypted PDF attachments remain unchanged from native formats.
- ✓ Support for Office Document Encryption.
- ✓ Support for ZIP File Encryption.
- ✓ Support to wrap files into Encrypted PDF or ZIP.
- ✓ Self-Registration (same as Encrypted PDF).
- ✓ Sender Set Passwords (same as Encrypted PDF).
- ✓ Branded header and/or footers added to the message body with an account management link or Shared Secret Hint.

FEATURES

- Read secure messages anywhere – on any device.
- Message body remains clear-text – only the attachments are encrypted.
- Message support for multiple encrypted attachments in their original native formats.
- Extensive branding features for all customer-facing webpages, encrypted messages, and message notifications.
- Support for 27 languages.
- Deliver encrypted PDFs and Office documents direct to an inbox.
- Message remains encrypted at-rest.
- Options for sender or recipient set passwords.
- Offline message access.

LIMITATIONS

- For Secure ZIP, recipient must have ZIP software installed capable of opening AES 256-bit files (such as WinZip, Secure ZIP, WinRAR, 7-ZIP).
- Limited message audit and tracking options.
- No read receipt options for sender.

Certificate Encryption

Beneficial when recipients already have a third-party S/MIME or PGP.

- ✓ Certificate Encryption is based on a user-uploaded public certificate.
- ✓ External lookup in LDAP for public recipient certificate.
- ✓ Full PGP key creation / management for senders to external PGP users. External users will get a PGP encrypted email that is a digitally signed with a public key attached for the sender.
- ✓ Full support for PGP migration to the cloud, consolidating all PGP activity under one secure communication platform.

FEATURES

- Upload existing keys to the Echoworx Email Encryption platform.
- Auto generate new keys as needed, maintaining current and future identities.
- No need for recipients to change behavior.
- Secure delivery can be made to any email address in the world (assuming key exists).

LIMITATIONS

- Configuration of inbound email flow is required to detect encrypted reply messages.

Web Portal Encryption

Enables secure delivery of encrypted messages via a secure website, like an existing customer portal. Secure messages are not delivered direct to the recipient, they receive a notification that they have a message waiting for Web Portal pickup.

- ✓ Self-Registration: Recipient gets one-time registration message and registers and set their own password.
- ✓ Support for 27 languages.
- ✓ Registration optionally supports out-of-band confirmation (on registration).
- ✓ Supports full OAuth access: Office 365, Gmail, Hotmail, Facebook, LinkedIn, and Salesforce
- ✓ Web services integration enables auto-login via an existing customer portal.
- ✓ No-Authentication: Recipient gets a URL that directly opens the message (no registration).
- ✓ Sender Set Password: Recipient enters a password the sender set at time of sending through the plugin or through subject line trigger.
- ✓ Out of Band Password: System generates a per message password and emails it back to a sender. The recipient must obtain this system password out-of-band from the sender to gain access to the message.

FEATURES

- Enables more flexible delivery – anywhere on any device.
- Extensive branding features for all customer-facing webpages, encrypted messages, and message notifications.
- Message remains encrypted at-rest.
- Ability to save messages locally in several formats from Outlook to Encrypted PDF.
- Ability for secure passwords to be set by the sender or by the recipient.
- Secure reply functionality and read receipts.
- Full message audit and recall for both sender and Administrator.

LIMITATIONS

- Retention period (30, 60, 90 days) then deleted.
- Recipient must leave their local mailbox to retrieve messages online.
- Limited message tracking. No read receipt option for sender.

ECHOWORX™

IT PAYS TO BE SECURE

Echoworx protects the privacy of people and businesses throughout the world by making email data protection easier. Our customizable email encryption platform helps organizations easily share protected email, statements, and documents from anywhere and from any device. Our passionate encryption experts transform communication chaos into order for world leading organizations who understand — it pays to be secure.

Encryption is an investment in brand, maximizing competitive advantage.

Clients in 30 countries use Echoworx and more than 5,000 business, public sector, and institutional deployments are serviced through our data centers in the U.S., Canada, Germany, Ireland, and the U.K.

For more information www.echoworx.com

✉ info@echoworx.com

☎ North America 1 800.735.8916 | UK 44 0.800.024.6657

🐦 @Echoworx