ECHOWORX ONEWORLD ENCRYPTION

DELIVERY METHODS

ECHOWORX

IT PAYS TO BE SECURE

Echoworx - OneWorld Encryption Delivery Methods

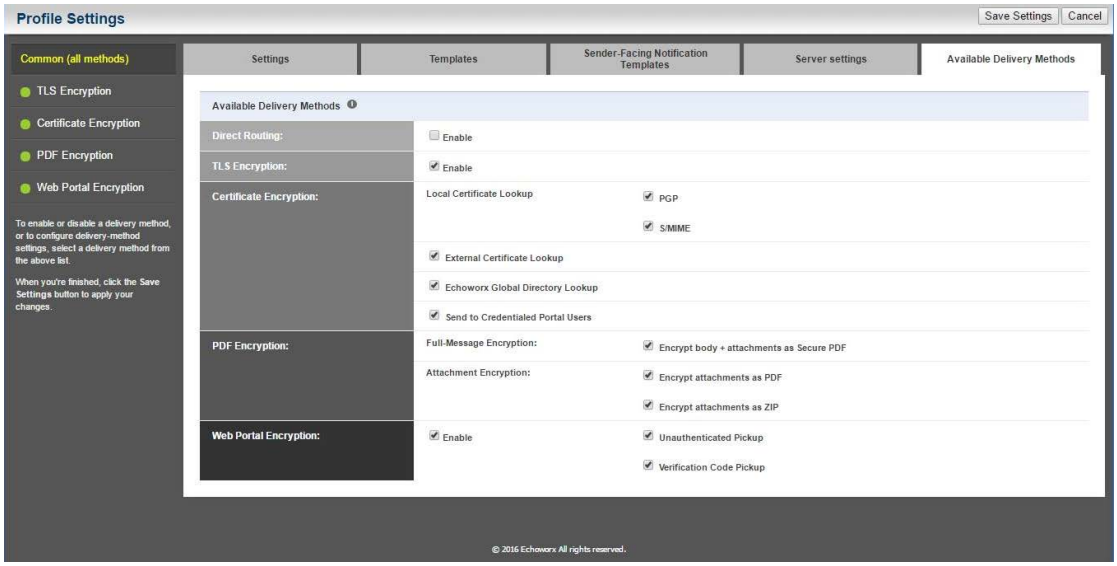
Do you want secure communication with business partners? Do you want a seamless user experience for sending and receiving encrypted messages?

If you are like most organizations today, encryption services are requirements for external communications: customers, prospects and business partners.. This gets problematic when it comes to effectively serving your customers – with balancing strong encryption with a customer-centric user experience a common encryption barrier. As a security administrator, it is your responsibility to crack this conundrum with a flexible encryption solution which offers multiple delivery methods.

That's why Echoworx's OneWorld Encryption Platform offers extensive encryption delivery flexibility – allowing organizations to meet a wide range of business use cases and branding requirements. And any or all of OneWorld's secure delivery methods can be used at the same time with customizable encryption policy options. Unique benefits to each encryption method ensure your messages are protected in transit regardless of what is around the corner.

Echoworx OneWorld offers **eight secure encryption delivery methods:**

TLS Encryption | Encrypted PDF | Encrypted Attachment
Certificate Encryption | Web Portal Encryption



TLS ENCRYPTION DELIVERY

Encryption of messages and attachments in transport directly to the recipient. No setup or password requirements to provide the most seamless method.

NOTEWORTHY FEATURES:

- TLS connection is verified for validity on-the-fly.
- Configure a White List (only send to) or Black List (do not send) of TLS domains through a web-based administration console.

FEATURES:

- Senders simply send messages and our OneWorld encryption platform takes care of the rest.
- No need for recipients to change behavior – customer-centric at every step.
- If TLS is not available, OneWorld automatically offers alternative secure encryption delivery options, like Web Portal or Secure PDF – ensuring the messages is not sent unprotected.
- Can be branded (footer or header)
- Ideal for B2B when whitelist employed to ensure recipient is using TLS for replies

LIMITATIONS:

- If you want secure messages to stay encrypted at rest post-transit, TLS should not be used.
- Message not secured at rest
- Secure replies are not provided unless customer uses TLS

ENCRYPTED PDF

Encrypt both body and attachments contained in outgoing email using standard PDF, Office and ZIP technologies.

NOTEWORTHY FEATURES:

- Self-Registration: Recipient gets one-time registration message to set their own password.
- Registration process can also include an out-of-band confirmation.
- Authentication can be through existing bank 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:

- Excellent mobile experience.
- Complete branded experience for recipient including all customer-facing webpages, encrypted messages and email notifications.
- Deliver encrypted PDFs direct to an inbox.
- Secure messages are encrypted at rest post-delivery.
- Messages are available locally for offline viewing. offline.
- Ability for secure passwords to be set by either sender or recipient.
- Secure reply functionality with the option to have a secure copy for recipient.
- Any standard PDF viewer on any device may be used to open an encrypted PDF.

LIMITATIONS:

- Limited message tracking.
- No read receipt option for sender.

ENCRYPTED ATTACHMENT

Deliver sensitive documents in messages as encrypted any attachments – without appearing in body of email. This option is useful for generating and processing bulk electronic statements.

NOTEWORTHY FEATURES:

- Encrypted PDF attachments remain unchanged from their original 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:

- Message body remains clear-text – only the attachments are encrypted.
- Excellent mobile experience.
- Messages can be sent with multiple encrypted attachments in their original native format
- Complete branded experience for recipient including all customer facing webpages, encrypted messages and email notifications.
- Deliver encrypted PDFs and Office documents direct to an inbox.
- Message remains encrypted at rest post-delivery.
- Ability to save messages locally or offline.
- Ability for secure passwords to be set by either sender or recipient.
- Offline reading of attachments

LIMITATIONS:

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

CERTIFICATE ENCRYPTION

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

NOTEWORTHY FEATURES:

- 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. Eliminates need for PGP desktop software under PGP communication.

FEATURES:

- Upload existing keys to our OneWorld 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. The email is not delivered to the recipient, but instead users are notified in their regular Inbox that an encrypted message is waiting for them.

NOTEWORTHY FEATURES:

- Self-Registration: Recipient gets one-time registration message and registers and set their own password
- Registration optionally support out-of-band confirmation (on registration).
- Authentication can also be through OAuth connectors.
- Authentication can be through existing portals (no URLs in notifications).
- 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:

- Excellent mobile experience.
- Complete branded experience for recipient including all customer facing webpages, encrypted messages and email notifications.
- Message remains encrypted at rest post-delivery.
- 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.
- Read receipts.
- Full message audit for both sender and Administrator.
- Message 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.

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 encryption platform, OneWorld, 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.

The Echoworx Advantage
8 different ways to deliver secure emails and support for 26 languages.
Enterprise Focused. 100% email encryption focused.
Product Company. SaaS Business Model.

Agile. Responsive. Passionate.
Private Canadian Company. Global Reach.
Data centers in the US, UK, Germany, Ireland, and Canada.

Trusted Root Certificate Authority
AICPA/CICA WebTrust Certification, SOC2 Audit, PCI DSS Level 1 Certification, FSQS and Microsoft and Apple Root Member Certifications.
Yearly renewal rate of 97%.

Visit us at www.echoworx.com

For more information www.echoworx.com

✉ info@echoworx.com
North America 1 800.735.8916 | UK 44 0.800.024.6657
@Echoworx