

One Platform. Every Recipient. Secure Every Time.

Your guide to Echoworx delivery options — and the smarter way to protect every message that leaves your enterprise

Every day, your organization sends sensitive information to clients, partners, regulators, and colleagues who each work differently and expect a different experience. Echoworx sits at the boundary of your environment, weighs every outbound message against your policy, and routes it through the right delivery method automatically. The pages ahead walk you through each option in turn, so you can match the right method to the right recipient with confidence.

Encryption Options Delivered in 28 Languages

Pull

Portal User
(default)

Portal Message
Level

Push

Full Message

Attachment
(PDF, Office, ZIP)

Direct

TLS

PGP
(with certificate
harvesting)

S/MIME
(with certificate
harvesting)

DigiCert
API

SwissSign
API

AWS
API

Authentication Options

OAuth

OpenID

SSO

2FA
(TOTP & Phone)

PassKey

Sender
Set

Out Of
Band

No Auth

Text & Call

Sender
Set

User
Managed

Sender
Set

User
Managed

Web Portal

When sensitive information needs a controlled, trackable home, the Secure Web Portal delivers it without the password fatigue that frustrates recipients and floods IT with reset tickets. Recipients authenticate using credentials they already trust, senders and administrators keep full visibility over every message, and governance travels with each communication from first delivery through to reply and recall.

Key Features

- **Federated sign-in and OAuth 2.0:** Full OAuth 2.0 support for Microsoft 365, Gmail, Hotmail, Facebook, LinkedIn, Salesforce, and additional providers. Recipients sign in with credentials they already have — no new accounts, no new passwords.
- **OpenID Connect:** Organizations supporting OpenID for authentication allow recipients to sign in with current credentials, bypassing new account creation entirely.
- **SSO integration:** Web services integration enables auto-login through an existing business portal, embedding secure message access seamlessly into the recipient's familiar environment.
- **No-Authentication mode:** For low-risk communications, recipients access messages via a direct link with no login required, while message activity and secure inbound reply tracking remain active.
- **Sender-Set Password:** Senders define a shared passphrase with an optional hint through the M365 Outlook Add-On, communicated to the recipient through a separate channel. Recipients access the message without registering.
- **Text Message verification:** Senders enter a recipient phone number through the M365 Outlook Add-On and a one-time code is delivered to the recipient's device for portal authentication.
- **Voice Call Verification for 2-Step Verification:** For recipients who cannot receive a Text Message — whether due to location, connectivity, or accessibility needs — voice call delivery provides a dependable alternative, keeping access moving without delays or complaints.
- **Passkeys (Passwordless Access):** Biometric authentication via fingerprint scanner or device biometrics enables secure, single-step portal access using a PIN or biometric autofill.
- **Reply-All Controls:** Limits portal Reply-All to internal subscribers and automatically removes unrecognized domains from drafts, closing a common path to accidental data exposure and reinforcing your DLP policy.
- **Secure Message Forwarding:** Restricts registered recipients to forwarding messages only within permitted domains, keeping collaboration inside a secure, fully auditable channel.
- **Adding Portal Recipients:** Permits registered recipients to add participants during reply or forward actions, within the same policy-governed environment, so real teamwork never leaves your defined boundaries.
- **Per-Recipient Notification Controls:** Allows recipients to opt out of reminder and final notifications, reducing inbox friction without compromising exchange integrity.
- **Accessibility:** Expanded WCAG conformance across the recipient portal meets the accessibility bar now standard in enterprise RFPs and compliance audits.

Additional Features

- Device-agnostic delivery across all major platforms and form factors, wherever your recipients work.
- Extensive branding controls for customer-facing pages, encrypted messages, and notifications, so recipients always recognize the source.
- Localization support across 28 languages.
- All messages stored encrypted at rest within the Echoworx cloud, with standard retention periods of 30, 60, or 90 days and extended terms available upon request.
- Local message export in Outlook and Encrypted PDF formats for long-term recipient retention. Password management available to both senders and recipients.
- Secure reply and read receipt functionality for ongoing, auditable exchanges.
- Full message audit and recall capabilities for senders and administrators.
- **Accessibility:** Expanded WCAG conformance across the recipient portal meets the accessibility bar now standard in enterprise RFPs and compliance audits.

Tech Note

Messages are accessed online through the portal and are not permanently stored on the recipient's local device. Recipients who need to keep a copy long term should save or export messages upon receipt.

What this means for you: Your recipients sign in with credentials they already trust and reach their messages in seconds — on any device, in any language, with no new accounts to create. Your senders keep full control over who reads, replies to, and forwards every message. And your organization meets the governance, accessibility, and compliance standards that regulators and procurement teams now expect as standard.

Encrypted PDF

Sometimes the fastest way to protect sensitive information is to send it as a locked document, not a portal link. Encrypted PDF delivery secures both the message body and its attachments using trusted Secure PDF, Office 365, and ZIP technologies. Recipients receive a familiar file they can open, save, and keep, while your organization keeps the content protected from the moment it leaves your gateway.

Key Features

- **Verification Code Access:** Picture sending a secure document to a non-technical recipient on a tight deadline. Registration becomes a bottleneck. This document-encryption method removes it entirely. The sender shares an on-the-fly code through a separate channel, such as a quick phone call, and the recipient uses it to open the encrypted PDF or attachments right away. No registration, no passwords, no delays — just security that moves at the pace of the conversation.
- **Self-Registration:** Recipients set their own password through a single one-time prompt, so first-time access stays simple.
- **Password Management:** Recipients recover or update their password through a self-service link, without a call to your helpdesk.
- **Sender-Set Passwords:** Senders create a shared passphrase and pass it to the recipient out-of-band, giving both sides control over access.
- **Seamless Viewing:** Encrypted PDFs and Office documents open directly in Gmail or Outlook for Web, with nothing new to download or install.

Additional Features

- Flexible delivery to any device, wherever your recipients work.
- Customizable branding for messages and notifications, so recipients always recognize the source.
- Support for 28 languages.
- Offline access with at-rest encryption, letting recipients keep secure copies for as long as they need them.
- Secure replies with recipient copies, keeping the conversation protected in both directions.

Tech Note

Push encryption delivers each message straight to the recipient for immediate access. Because the document lands directly in their inbox, messages sent this way cannot be recalled.

What this means for you: Your recipients get a simple, familiar document they can open on any device, your team can reach even non-technical contacts in seconds with verification codes, and your sensitive content stays protected from send to open.

Encrypted Attachment

When sensitive information needs to travel fast, sometimes the safest path is the simplest one: a locked attachment that lands right in the recipient's inbox. Encrypted Attachment delivery protects your documents while leaving the message body in clear text, so recipients see a familiar email with a secure file they can open, save, and keep. It is ideal for high-volume, document-driven work like processing bulk electronic statements, where speed and security have to move together.

Key Features

- **Verification Code Access:** Picture sending a secure document to a non-technical recipient on a tight deadline. The traditional registration step becomes a bottleneck. This verification code method removes it entirely. The sender shares an on-the-fly code through a separate channel, such as a quick phone call, and the recipient uses it to open the encrypted attachment right away. No registration, no passwords, no delays. Security that keeps pace with a conversation, not a paperwork queue.
- **Voice Call Verification for 2-Step Verification:** When a recipient cannot receive a Text Message — because of where they live, an accessibility need, or simply a signal gap — Voice Call Verification for 2-Step Verification gives them a dependable alternative. Access stays open, authentication delays drop.
- **Native Encryption for PDF, Microsoft Office, and ZIP:** Attachments are encrypted natively, preserving each file's original name and properties so recipients recognize exactly what they are opening.
- **Seamless Viewing:** Encrypted PDFs and Office documents open directly in Outlook for Web and the Gmail client, with nothing new to download or install.
- **Broad File Support:** Other attachment types are bundled into an Encrypted PDF or ZIP format, so no document is left unprotected.
- **Self-Registration:** Recipients set their own password through a single one-time prompt, keeping first-time access simple.
- **Sender-Set Shared Passphrase:** Senders create a shared passphrase and share it with the recipient out-of-band, giving both sides control over access.
- **Customized, Branded Message Body:** Headers and footers can carry a password management link or a subtle hint for the shared passphrase, so recipients always know they are in the right place.

Additional Features

- Read secure documents anywhere, on any device, wherever your recipients work.
- Keep the message body in clear text while only the attachments are encrypted, so routine context stays readable.
- Send multiple encrypted attachments in their original formats within a single email.
- Reach a global audience with multilingual support in 28 languages.
- Deliver directly to the recipient's inbox, no portal visit required.
- Protect encrypted attachments at rest, so files stay secure long after they arrive.
- Choose flexible password options set by senders or recipients, including Phone Verification and Passkeys.
- Open secure documents offline, whenever and wherever recipients need them.

Tech Note

Echoworx recommends ZIP software capable of opening AES 256-bit files, including WinZip, Secure ZIP, WinRAR, and our favorite, 7-Zip. Keep in mind that push encryption delivers each email immediately to the recipient, so messages sent this way cannot be recalled by Echoworx.

What this means for you: Your recipients get a familiar email with a secure file they can open on any device, your team can reach even non-technical contacts in seconds using verification codes and inclusive Voice Call Verification, and your sensitive documents stay protected from send to open.

TLS Encryption with Fallback

Some messages need to move quietly and instantly, with no passwords, no portals, and no extra steps for anyone involved. TLS Encryption with Fallback does exactly that, encrypting your messages and attachments in transit and delivering them straight to the recipient. When a recipient's domain cannot support TLS, the platform never leaves a message exposed. It shifts automatically to another secure channel, so protection stays constant and delivery stays effortless.

Key Features

- **On-the-fly TLS validation:** The platform verifies the validity of every TLS connection in real time, so each message is checked for a genuinely secure path before it is sent.
- **Allow List control:** Configure an Allow List to send messages only to trusted TLS domains, giving you tight command over where secure mail can travel.
- **Block List control:** Create a Block List to exclude specific TLS domains, closing off any route you do not want to use.
- **Automatic secure fallback:** When a domain is not eligible for TLS delivery, Echoworx switches seamlessly to an alternative secure method, such as the Web Portal or Secure PDF, so protection is never interrupted.
- **Effortless compliance:** This seamless fallback enforces your security policy without manual intervention, supporting resilient controls expected under frameworks like DORA and NIS2.

Additional Features

- Senders simply send, while the encryption platform decides when to use TLS and when to fall back to another method.
- Recipients change nothing, because transparent delivery keeps the experience familiar from end to end.
- Extensive branding options let you customize headers and footers so every message looks unmistakably yours.
- Ideal for B2B environments where both parties already rely on TLS for secure exchange.

Tech Note

Once a message is delivered over TLS, it is not encrypted at rest in the recipient's mailbox. Secure replies travel outside the Echoworx platform and rely on the recipient's own TLS connection for protection in transit.

What this means for you: Your senders keep sending without a second thought, your recipients receive secure mail with nothing new to learn, and your organization keeps its security policy enforced automatically, right down to the compliance controls regulators expect.

Certificate Encryption

When your recipients already hold a trusted S/MIME or PGP certificate, Certificate Encryption puts it to work automatically. Messages and attachments are encrypted end to end, signed for authenticity, and delivered without asking anyone to change how they work.

Key Features

- **Flexible certificate discovery:** Recipient certificates are located automatically through external lookups across LDAP directories, so trusted exchange starts without manual effort.
- **Dynamic recipient key lookups:** Echoworx discovers PGP keys at an LDAP key server using a standard URI at the recipient's domain, streamlining secure delivery across your entire partner ecosystem.
- **Recipient self-service uploads:** Recipients upload their own x509 certificate or PGP public key directly through the web portal, or generate a self-signed S/MIME certificate when they hold none.
- **Trusted roots on demand:** Seamless integration with DigiCert and SwissSign retrieves and generates trusted S/MIME credentials for your employees the moment a key is needed.
- **Real-time PGP key generation:** Echoworx creates PGP public/private key pairs for senders on the fly, and the recipient of the encrypted message receives the sender's public key as an attachment, keeping every exchange self-contained.
- **Policy-driven signing with fallback:** Outbound messages are digitally signed using a key tied to the sender's email address, whether uploaded or generated. If none is available, an enterprise-level, domain-wide key steps in so messages are always signed.
- **PGP 'Sender Only' signing:** Any message the gateway cannot validly sign is bounced back with a non-delivery response, extending the same proven safeguard already trusted for S/MIME to PGP-signed communication.
- **Configurable key sizes:** Set auto-generated S/MIME and PGP key sizes at the profile level — 2048-, 3072-, or 4096-bit RSA — with the default now raised to 3072-bit to keep cryptographic strength aligned with modern standards.
- **Inbound decryption:** Inbound S/MIME and PGP-encrypted messages are decrypted using private keys stored securely within the Echoworx platform, then delivered with branded headers and footers applied.
- **Self-service PGP decryption:** Route legacy endpoint-encrypted messages through the gateway for decryption, keeping historical records accessible, auditable, and intact.

Additional Features

- **Automatic renewal of expiring S/MIME keys:** For DigiCert and SwissSign customers, employee certificates regenerate automatically before they expire, moving security from reactive to proactive and preventing last-minute service interruptions.
- **Signature verification insight:** When Echoworx verifies an inbound signed message, the system injects additional MIME headers to flag verification issues and delivers a detailed report as `signature_verification_results.html` for a cleaner administrative workflow.
- **Granular LDAP server control:** Enterprise administrators can enable or disable specific LDAP directories within their profiles, giving precise command over which servers are searched.
- **Separate S/MIME and PGP LDAP lookups:** Enable external key server lookups independently for S/MIME, PGP, or both, so key discovery follows your rules, not a fixed default.
- **PGP private key export API:** Export PGP private keys programmatically through a REST endpoint, supporting portability, continuity, and the key sovereignty regulators expect.
- **Smooth migration and global reach:** Import all your employees' certificates and key pairs at once, auto-generate new keys as needed, and deliver securely to any email address in the world — all under one consolidated platform for PGP and S/MIME.

Tech Note

To decrypt inbound messages and extract certificates from incoming communications, configure additional rules in your gateway to route those messages to Echoworx. Once that routing is in place, discovery, decryption, and signature verification all run automatically.

What this means for you: Your recipients keep working exactly as they do today, your senders always reach trusted partners with the right key, and your administrators gain proactive renewal, precise directory control, and clear verification insight — all under one platform built to keep certificate-based communication secure from send to open.