ECHOWORX™

Guide

From First Wave to Second Generation Encryption

The Migration Playbook

This playbook outlines a proven methodology for transitioning from a first-wave solution to our second-generation encryption platform.

Honed through extensive experience guiding global enterprises, it provides a clear, step-by-step process for a seamless and successful transition.

Table of Contents

The Migration Strategy

Defining What Moves and What Stays

A successful migration isn't about moving everything. It's about strategically transitioning the core components of your security posture while leaving behind the technical debt of legacy systems. The goal is to enhance, not just replicate.

What We Migrate Together

- **Business Encryption Rules:** We document and transfer the logic that defines how and when messages are encrypted. This includes specific use cases, like S/MIME for one business unit and document encryption for another, ensuring your operational requirements are met from day one.
- **Corporate Branding & URLs:** The new encryption portal becomes a seamless extension of your brand. We migrate your look and feel, including logos, color schemes, and custom portal URLs (e.g., securemail.yourcompany.com), to maintain customer trust and familiarity.
- **S/MIME & PGP Keys:** To ensure uninterrupted secure communication, we facilitate the secure export and import of all essential keys. This includes internal employee key pairs and the library of third-party certificates you've built over the years.
- **Policies & Custom Resources:** Your existing privacy policies, cookie notices, and custom help guides are documented and implemented within the new Echoworx environment.

What Stays Behind (And Why)

- **Legacy Recipient Accounts:** For security reasons, user accounts, stored passwords, and security questions from the old system cannot be migrated. Users will seamlessly create new credentials upon receiving their first encrypted message from the new platform.
- **Previously Sent Messages:** Messages stored in your legacy provider's web portal cannot be exported. We'll plan to run the old system in parallel for a set period, giving recipients ample time to download and archive any important historical communications.
- **Your Primary Gateway:** Your existing Secure Email Gateway (SEG) for antivirus, anti-spam, and DLP remains in place. The Echoworx cloud integrates into your current mail flow, not replace it. Your MX record does not change.

The Environment Setup

Establishing Test vs. Production Sandboxes

A dedicated test environment is the single most important factor for a smooth, low-risk migration. It provides a sandbox to validate every configuration and gain stakeholder confidence long before you go live.

The Value of a UAT Environment

A User Acceptance Testing (UAT) environment is your proving ground. We work with you to set up a dedicated UAT profile in the Echoworx cloud, often using a separate test domain (e.g., company-test.com).

Key Benefits:

- **Risk Reduction:** Gives you a space to configure and test everything—from mail flow rules to branding—without impacting your production environment.
- **Stakeholder Sign-Off:** Allows marketing, business, and security teams to see, feel, and approve the new user experience early in the process.
- **Feature Validation:** Provides a safe place to test and compare security policies, such as enabling MFA or other optional features, to dial in the perfect balance of security and usability.
- **Flawless Promotion:** Once everything is signed off in UAT, the entire configuration can be promoted to your production tenant, ensuring what you tested is what goes live.

Technical Planning

Mapping Mail Flows, Certs, and Integrations

The pre-migration planning phase is where we build the blueprint for your new encryption architecture. With a dedicated technical engagement manager, we meet regularly to map out every technical detail.

Key Planning Steps

- **Mail Flow Mapping:** We work with you to understand and plan for every scenario:
  - **Outbound:** Messages from your gateway to Echoworx for encryption.
  - **Inbound:** Encrypted messages arriving at your gateway that are routed to Echoworx for decryption and signature verification.
  - **Internal Delivery:** Secure replies and decrypted messages routed back to your internal mailboxes.
- **IP Allow Lists & SSL Certificates:** We coordinate the necessary IP trusting on both sides and help you generate the SSL certificates for your new, custom-branded portal URL.
- **DKIM Signing:** We determine the best strategy for DKIM signing to ensure the authenticity of system-generated notifications and secure replies, whether it's handled by your gateway or by Echoworx.
- **Integrations:**
  - **Admin SSO:** We provide guided instructions to set up single sign-on for the admin console via OpenID, connecting with your M365 Entra ID for easy access.
  - **SIEM:** We provide the documentation for our audit APIs, allowing you to pull detailed logs into your SIEM for complete visibility.
  - **S/MIME & SMS:** We assist with optional integrations for automated S/MIME certificate generation (DigiCert, SwissSign) or SMS-based authentication (Twilio, Synch).

The User Experience

The Outlook Add-in and Client Communication

A successful migration prioritizes the user. This means empowering your internal staff with modern tools and providing clear communication to your external clients.

The Modern Outlook Add-in

The Echoworx Outlook Add-in is a crucial piece of the user experience. It's a modern, M365-based deployment with no desktop installation required. The add-in roams with the user's account across Outlook for Web, Mac, and Windows.

- **Empower Your Staff:** Give users a simple button to initiate encryption and select delivery options, such as setting a shared passphrase or choosing attachment-only encryption.
- **Custom Policies:** The add-in's menu and options can be fully customized to match your specific business use cases and security policies.
- **Phased Rollout:** You can easily assign the add-in to a small group of early adopters for feedback before rolling it out to the entire organization.

Client Communication Strategy

While the transition is designed to be seamless, proactive communication helps ensure a smooth experience for your customers.

- **Announce the Change:** Consider placing a notice on your legacy portal's login page informing users of the upcoming upgrade and the timeline for decommissioning.
- **Set Expectations:** Let recipients know how long the old system will remain online so they have time to download any messages they wish to keep.
- **Leverage New Templates:** For the first few months, the new email notification templates can include a message like, "Welcome to our new, enhanced secure email system," to ease the transition.

The Launch Sequence
Soft Launch, Live Cut-Over, and Decommissioning

A phased launch is the key to a controlled, zero-impact migration. We break the process down into manageable stages, giving you full control at every step.

Phase 1: Soft Launch (Optional, but Recommended)

A soft launch involves routing a small, controlled portion of production mail to the new Echoworx platform.

- **How it Works:** You can deploy the Outlook Add-in to a select group of "friendly" internal users or create rules to route mail from specific business units to Echoworx.

- **Benefits:** This allows you to run both systems in parallel, identify any surprises with limited impact, and gather real-world feedback before the full cut-over. A soft launch typically runs for 2-3 weeks.

Phase 2: Live Cut-Over

The live cut-over is when you update the mail routing rules in your primary gateway to send all encryption-bound traffic to Echoworx. This is typically scheduled for a weekend to minimize business impact. The cut-over itself can be split into two parts:

- **Inbound Cut-Over:** Update rules to route all incoming S/MIME and PGP messages to Echoworx for decryption. This can happen a week or two before the outbound cut-over to begin building up the new certificate library.

- **Outbound Cut-Over:** Update all outbound rules to direct mail that requires encryption to the Echoworx platform. At this point, 100% of your encrypted mail is flowing through the new system.

Phase 3: Decommissioning

The final step is to safely shut down the legacy system.

- **Grace Period:** You will leave the old system online for a predetermined period (typically 30-90 days) to allow all stored messages to expire and give users a final window to retrieve their data.

- **Redirect Traffic:** Once the grace period ends and activity ceases, you can shut the system down and redirect any lingering web traffic from the old portal URL to the new one.

This playbook provides the framework for your migration. Our team is here to guide you through every step, ensuring a seamless transition to a more secure, modern, and user-friendly encryption platform. We look forward to working with you.