ECHOWORX™

IT PAYS TO BE SECURE

Mimecast Setup for Email Encryption

Integrating Mimecast with Echoworx

Contents

Note: If you want to copy spacing-sensitive text from this document, please use Acrobat Reader to view this PDF document. Content copied from this document while it is opened in other PDF readers may not retain its formatting.

Integrating Mimecast with Echoworx Corporation

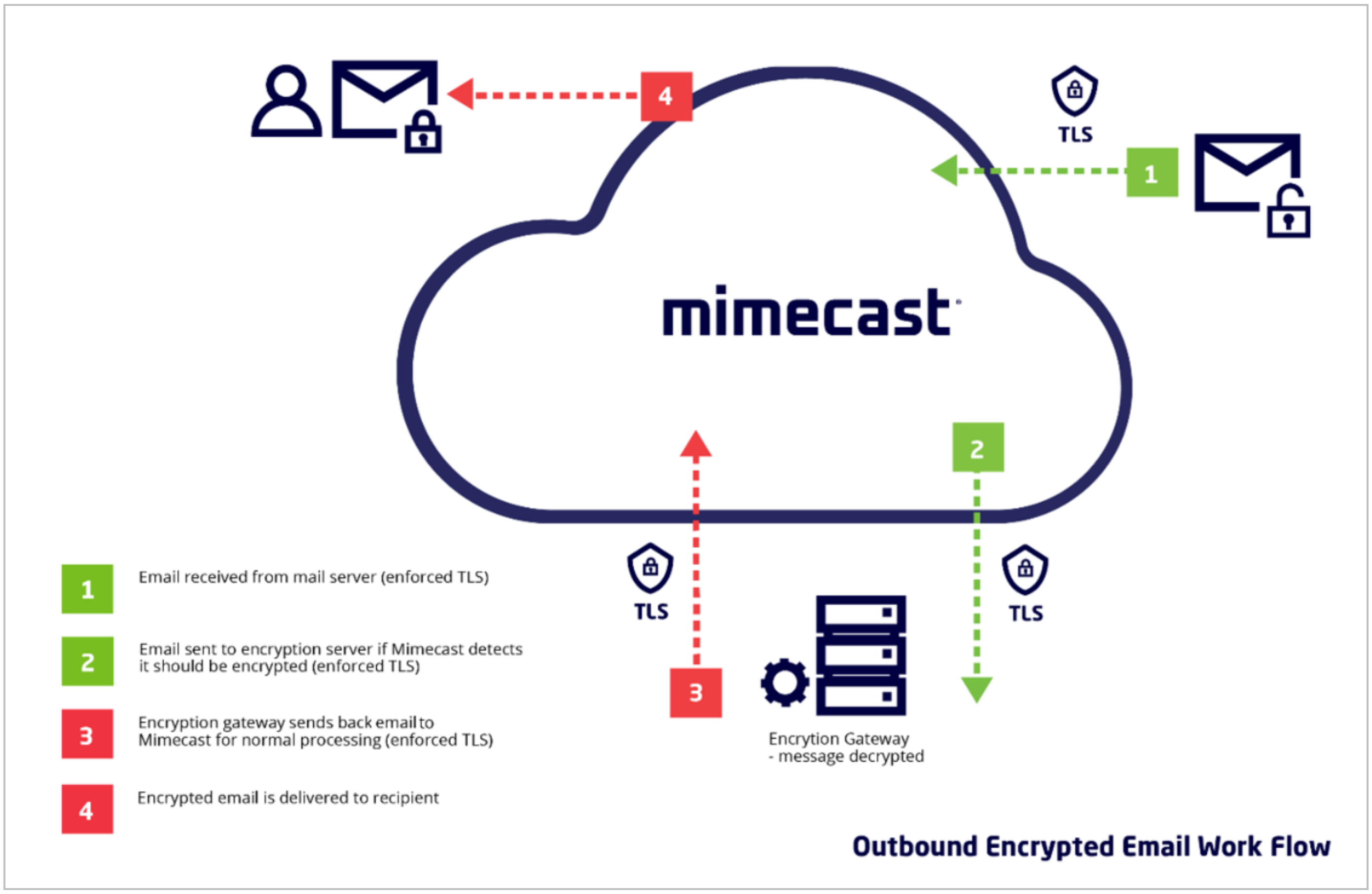
This document provides guidance for Mimecast customers to integrate with Echoworx Email Encryption. It assumes your Mimecast & Echoworx services are provisioned and ready. For more specific instructions on Mimecast configurations, please contact Mimecast support. Echoworx Email Encryption support is available through online help, product documentation, email, and live support resources. Please contact your Echoworx representative for further assistance.

Mimecast and Echoworx Email Encryption integration is a supported deployment that is recognized by both vendors. Mimecast has published their own guidance for this deployment type, available here (https://community.mimecast.com/s/article/Configuring-3rd-Party-Encryption-Gateway-Solutions).

Successful intergration requires performing the contents of this guide in order.

1: Echoworx Accepts Mail from Mimecast

Standard Mimecast deployment routes messages that trigger a content examination policy to Echoworx Encryption Gateway, which routes encrypted messages back to the customer's Mimecast tenant for final delivery. Mimecast typically serves as the 'last hop' for SMTP communication. This concept is outlined in the following diagram:


4
TLS
1
mimecast
2
TLS
TLS
3
1 Email received from mail server (enforced TLS)
2 Email sent to encryption server if Mimecast detects it should be encrypted (enforced TLS)
3 Encryption gateway sends back email to Mimecast for normal processing (enforced TLS)
4 Encrypted email is delivered to recipient
Encrytion Gateway - message decrypted
Outbound Encrypted Email Work Flow

This first step relies on information shared with Echoworx at the time of provisioning (using the customer provisioning form). Customers provide Echoworx with their regionally specific Mimecast outbound SMTP servers that will deliver messages to Echoworx for encryption. Echoworx will add these servers to an Allow List for any provisioned email Domains. For example:

SMTP Server Public DNS Name(s)	SMTP Server Public IP Address(es)
`eu-smtp-outbound-1.mimecast.com`	91.220.42.202, 91.220.42.212, 91.220.42.242
`eu-smtp-outbound-2.mimecast.com`	195.130.217.202, 195.130.217.212, 195.130.217.242

2: Mimecast Relays Mail from Echoworx

Encrypted Messages and Notifications

To route Echoworx encrypted messages back to the customer's Mimecast tenant for outbound delivery, the Mimecast service must be configured to relay messages from Echoworx. This Cloud connection is referred to by Mimecast as 'relaying messages from shared or dynamic IPs'. This Mimecast article available here provides further details.

To support this connection, Mimecast customers will provision a Mimecast account for SMTP authentication (rather than set specific IP allow lists as 'Authorized Outbounds'). Echoworx will require the following information for provisioning:

Connector Details

Address: <Echoworx_encryption_relay@customer.com>

Password: <long, complex password recommended>

Port: <e.g. 587>

> **Note:** Mimecast outbound servers are used to relay outbound mail as in this use case (e.g. `eu-smtp-outbound-1.mimecast.com`)

Customer-Specific System Email

Customers will define an email address at Onboarding using the customer's Domain for system-generated messages (e.g. securemail-noreply@customer.com). The Echoworx-generated messages that use this connection include the following:

- First time registration and new message notifications (& reminders) to external recipients
- System generated notices to external recipients (e.g. password resets)
- Message Encrypted and Message Read/Expired notices back to internal senders

Inbound Secure Replies and Decrypted S/MIME and PGP Messages

Secure replies are authored using the Secure Portal (replies or composed messages). These messages are generally sent to the customers public MX servers for the Domain (e.g. eu-smtp-inbound-1.mimecast.com). These are sent from the customer defined system email (e.g. securemail-noreply@customer.com) to the internal user. Echoworx SMTP servers should be added to the IP allow list for this connection. Echoworx SMTP IP lists are region specific and provided to the customer at Onboarding.

Decrypted S/MIME and PGP messages will also be sent to the customer's public MX servers. These are messages which have been decrypted by the Echoworx service to be delivered in the clear to internal users over a forced TLS connection. These are typically sent from the original external sender email address.

3: Mimecast Connectors and Policies

Route Mimecast to Echoworx SMTP Servers

Please contact Mimecast support for step-by-step instructions on the setup of Mimecast Connectors and Content Examination Policies. Customers determine what to send to Echoworx for encryption based on the customer's own data classification requirements. Policy triggers can include a keyword, such as "**secure**:" (without quotes) in the message subject or a message header such as **x-echoworx-encrypt: yes** (for example to support the optional Echoworx Outlook plug-in).

Avoid Loops through Exceptions

Once a message has been processed by Echoworx and routed back to the customer's Mimecast tenant for final delivery, it is important to set exceptions so that these messages aren't mistakenly routed back to Echoworx, creating a loop.

Mimecast supports exceptions through negative scoring on conditions in the Content Examination Policies. Where a customer 'Word / Phrase Match List' is looking for specific message indicators, a list of negative score indicators must be added to cancel the total of any preceding indicators that may match in the policy.

The negative indicators will examine the message for headers that Echoworx adds to messages after processing, such as:

- `x-echoworx-emg-preprocessed` message header includes a keyword `"Y"`
- `x-echoworx-emx-notification-type` message header includes a keyword `"Y"`
- `x-echoworx-portal-composed` message header includes a keyword `"true"`

For example, where a customer may add the following positive indicators to a Word / Phrase Match List:

- `1 "x-echoworx-encrypt: y"`
- `1 "x-echoworx-portal: y"`

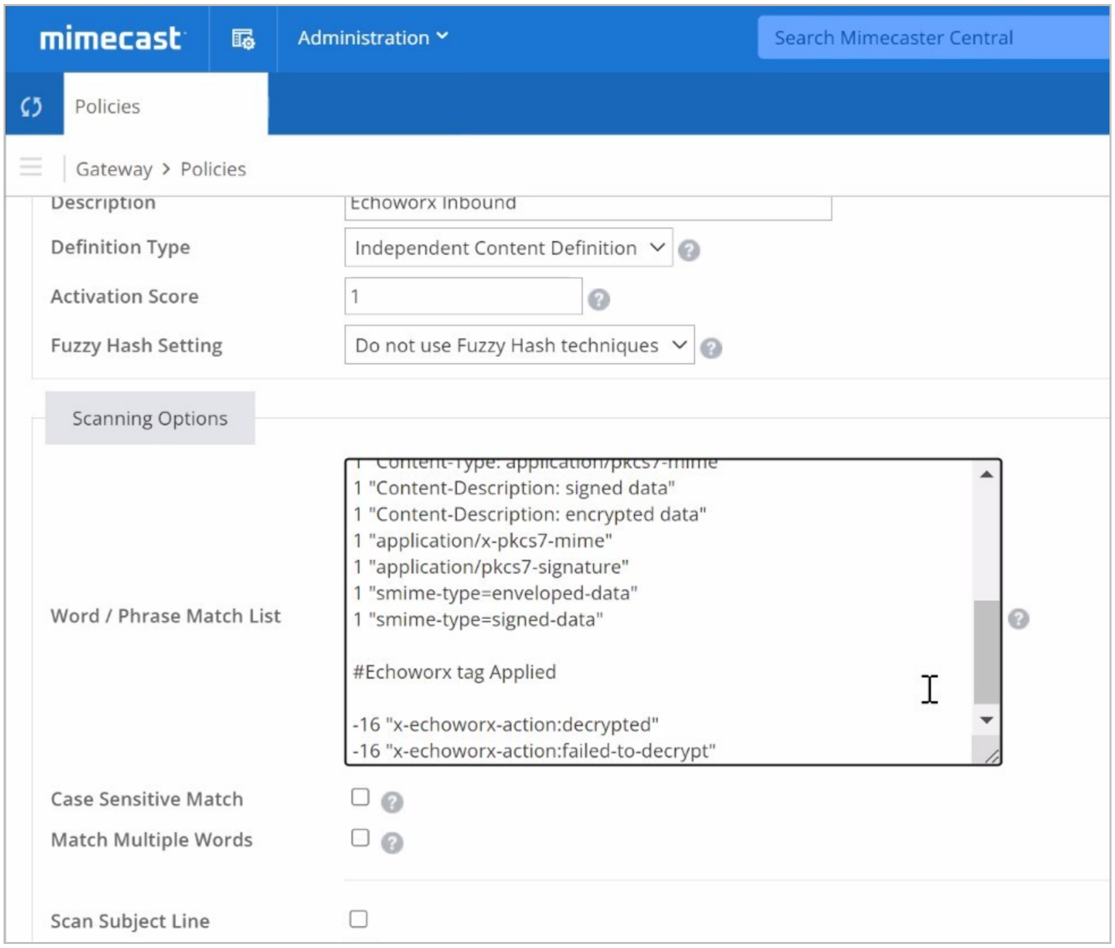
Negative score indicators must also be added to avoid loops. The Word / Phrase Match List would be as follows:

- # Echoworx Encryption Indicators
  - `1 "x-echoworx-encrypt: yes"`
  - `1 "x-echoworx-portal: yes"`
- # Echoworx Exception Indicators

- `-2 "x-echoworx-emg-preprocessed: y"`
- `-2 "x-echoworx-emx-notification-type: y"`
- `-2 "x-echoworx-portal-composed: true"`

> **Note:** The “-2” is calculated by adding the total score of possible encryption indicators in the Word / Phrase Match List so that if any or all of those conditions match, any combination of exception indicators will cancel the policy.

The following is a sample Mimecast Policy page that demonstrates these instances:



Description: Echoworx Inbound

Definition Type: Independent Content Definition

Activation Score: 1

Fuzzy Hash Setting: Do not use Fuzzy Hash techniques

Word / Phrase Match List:

```
1 "Content-Type: application/pkcs7-mime"
1 "Content-Description: signed data"
1 "Content-Description: encrypted data"
1 "application/x-pkcs7-mime"
1 "application/pkcs7-signature"
1 "smime-type=enveloped-data"
1 "smime-type=signed-data"

#Echoworx tag Applied

-16 "x-echoworx-action:decrypted"
-16 "x-echoworx-action:failed-to-decrypt"
```

Case Sensitive Match □

Match Multiple Words □

Scan Subject Line □

4: Mimecast Policies for Inbound PGP and S/MIME Decryption

Encrypted (PGP or S/MIME) messages that a customer receives are routed to Echoworx for decryption, using hosted private keys managed by the Echoworx gateway:

a. Configure a Mimecast Content Examination Policy to detect encrypted PGP or S/MIME messages and route these to your Echoworx connector (see steps 1 – 4 above for more details)

b. Configure policy Word / Phrase Match List to detect PGP or S/MIME encrypted messages for routing to Echoworx:

- #PGP encryption indicators
    - `1 "application/pgp-encrypted"`
    - `1 "application/pgp-keys"`
    - `1 "multipart/encrypted"`
- # SMIME encryption indicators
    - `1 "application/pkcs7-mime"`
    - `1 "application/x-pkcs7-mime"`

c. As described in #4 above, please ensure messages that have already been processed by Echoworx are not mistakenly routed back to Echoworx, using policy exceptions. PGP or S/MIME messages that have been processed will be tagged with any of the following mime headers: `x-echoworx-action: decrypted, x-echoworx-action: failed-to-decrypt, x-echoworx-action: delivered`. The Word / Phrase Match List for this example will be as follows:

- #PGP encryption indicators
    - `1 "application/pgp-encrypted"`
    - `1 "application/pgp-keys"`
    - `1 "multipart/encrypted"`
- # SMIME encryption indicators

    - `1 "application/pkcs7-mime"`
    - `1 "application/x-pkcs7-mime"`
  - # Echoworx Exception Indicators
    - `-5 "x-echoworx-action: decrypted"`
    - `-5 "x-echoworx-action: failed-to-decrypt"`
    - `-5 "x-echoworx-action: delivered"`

d. If your organization also sends digitally signed PGP or S/MIME messages without encryption, please also include exceptions for the following headers, so these ‘signed only’ messages are not routed to Echoworx:

  - # Signed Only Exceptions (Do not route to Echoworx)
    - `-5 "multipart/signed"`
    - `-5 "application/x-pkcs7-signature"`
    - `-5 "application/pkcs7-signature"`
    - `-5 "smime-type=signed-data\"`