ECHOWORX™

IT PAYS TO BE SECURE

Microsoft 365 Setup for Echoworx Email Encryption on Pax8

Copyright ©2023 Echoworx Corporation

Proprietary and confidential – For use by the intended recipient only

Revision History

Version	Date	Amendment Details
1.0	July 19 2023	Initial release

Contents

1. Introduction 4
2. Prerequisites 4
3. Create a Microsoft 365 Transport Rule Connector 5
4. Create Mail Flow Rule for Encryption on Keyword in Subject 10
5. Create Mail Flow Rule for Sender User Outlook Encrypt Button 11
6. Sender Policy Framework 13
7. Test your Setup 13

1. Introduction

This document provides guidance with setting up your Microsoft 365 (M365) service to use Echoworx Email Encryption for your email encryption. It assumes your Echoworx Email Encryption services are provisioned and ready, and you will be using your M365 “mail rules” to determine which outbound email messages will be encrypted and which inbound messages will be sent for decryption.

In this document, two sample rule definitions are provided for encrypting a sender’s email message:

- containing a trigger keyword in the subject, or
- using the optional Email Encryption Add-in for Outlook

These are the sample rules for getting up and running with Echoworx email encryption on M365. These rules can be used as a basis for creating additional rules based on customer-specific business requirements.

2. Prerequisites

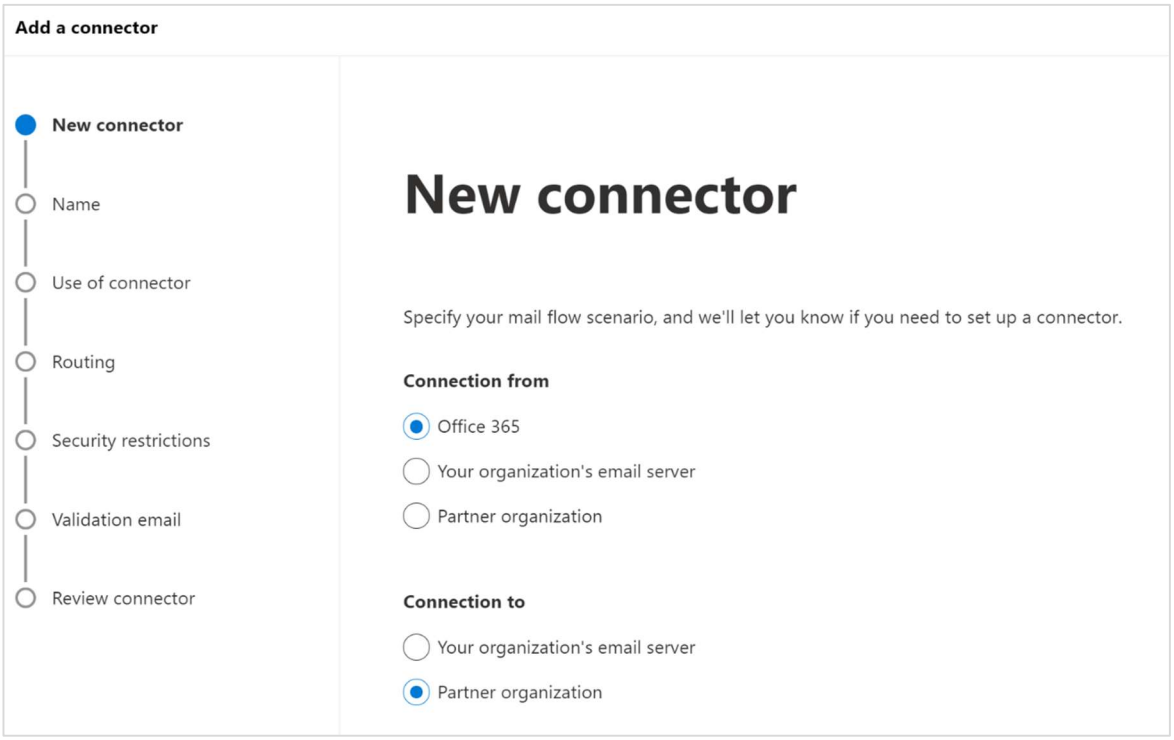
You must have administrative access to M365 admin center.

3. Create a Microsoft 365 Transport Rule Connector

This section explains the steps to create an outbound mail connector to Echoworx from Microsoft 365.

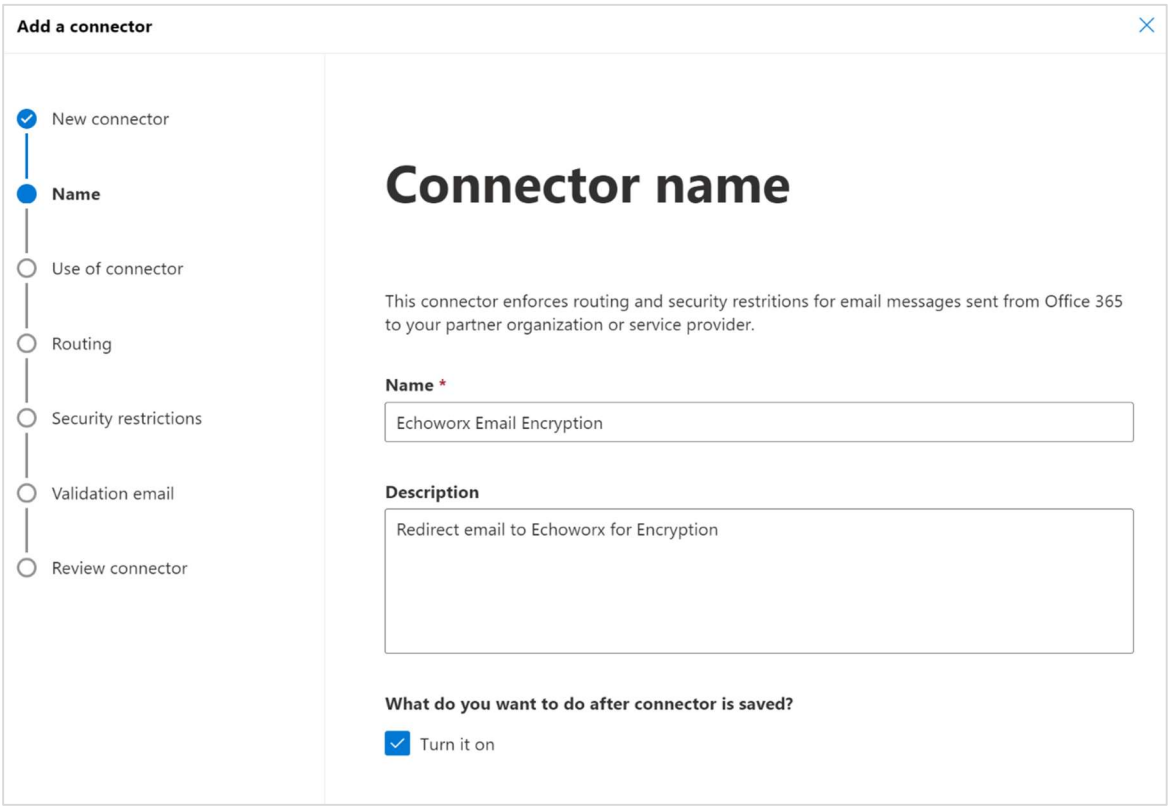
To create a Transport Rule Connector, follow the below steps:

1. Log in to Microsoft 365 admin center and navigate to **Exchange** Admin center. The Exchange admin center opens.
2. Click **Mail Flow** from the left navigation panel.
3. Click **Connectors**.
4. To create a new connector, click the + **Add a connector** option. A dialog box opens and the **New connector** page appears
5. Select the following:
    a. **Connection from** - Select the **Microsoft 365** radio button.
    b. **Connection to** - Select **Partner organization** from the drop-down list.



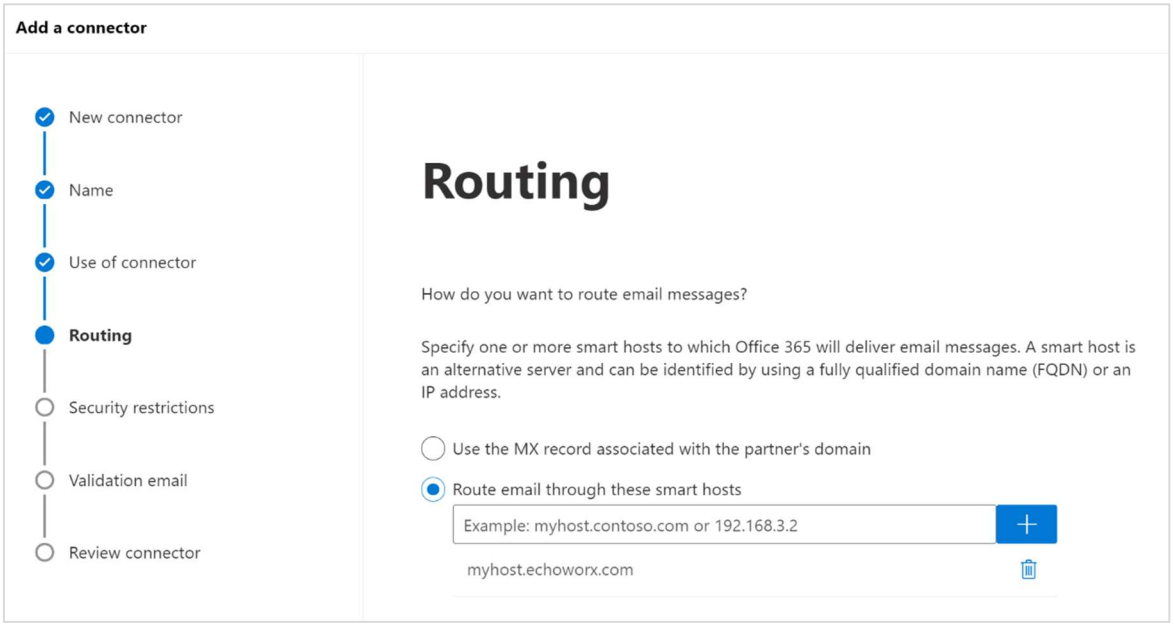
6. Click **Next**. The **Connector name** page appears.

7. Enter or select values of the following:
    a. **Name** * - Enter appropriate name of the connector to be created as **Echoworx Email Encryption**.
    b. **Description** - Enter appropriate description of the connector to be created.

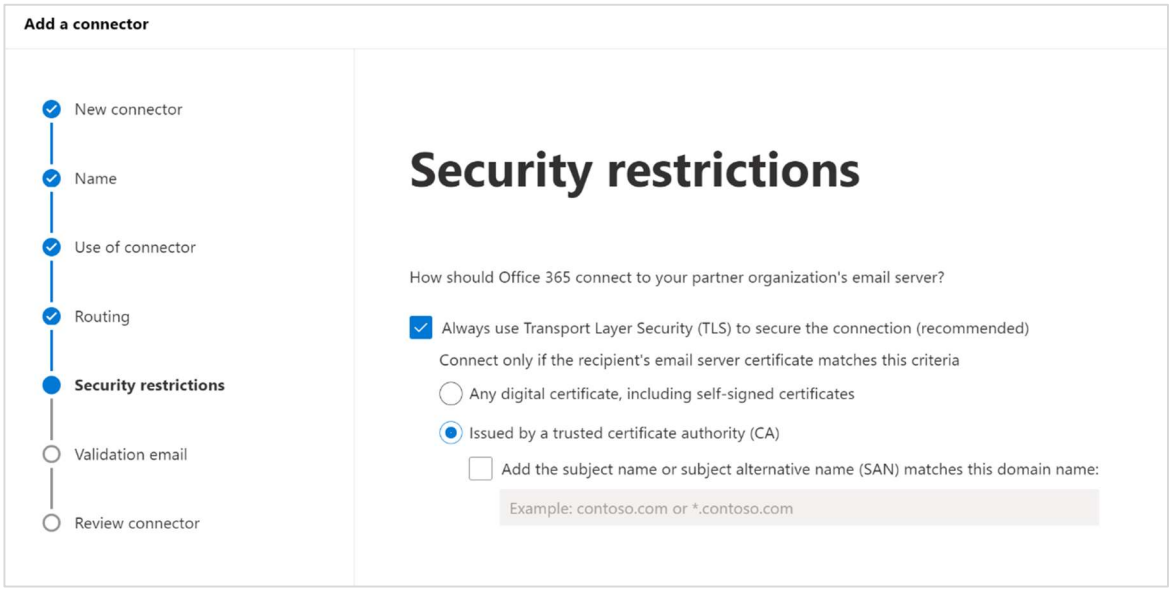


8. Click **Next**.
9. Select the value for **Specify when you want to use this connector.** as *Only when I have a transport rule set up that redirects messages to this connector*.
10. Click **Next**. The **Routing** page appears.
11. Select the value for **How do you want to route email messages?** as *Route email through these smart hosts*
    a. Specify the smart host's fully qualified domain name in the **Route email through these smart hosts** field.
    b. Click the + icon.

Note: The Echoworx Smart Host for Pax8 customers is will be smtp.mobilencrypt.com



12. Click **Next**. The **Security restrictions** page appears.
13. For **How should Microsoft 365 connect to your partner organization's email server?**, select *Always use Transport Layer Security (TLS) to secure the connection (recommended)*.
    a. Select **Issued by a trusted certificate authority (CA)**.



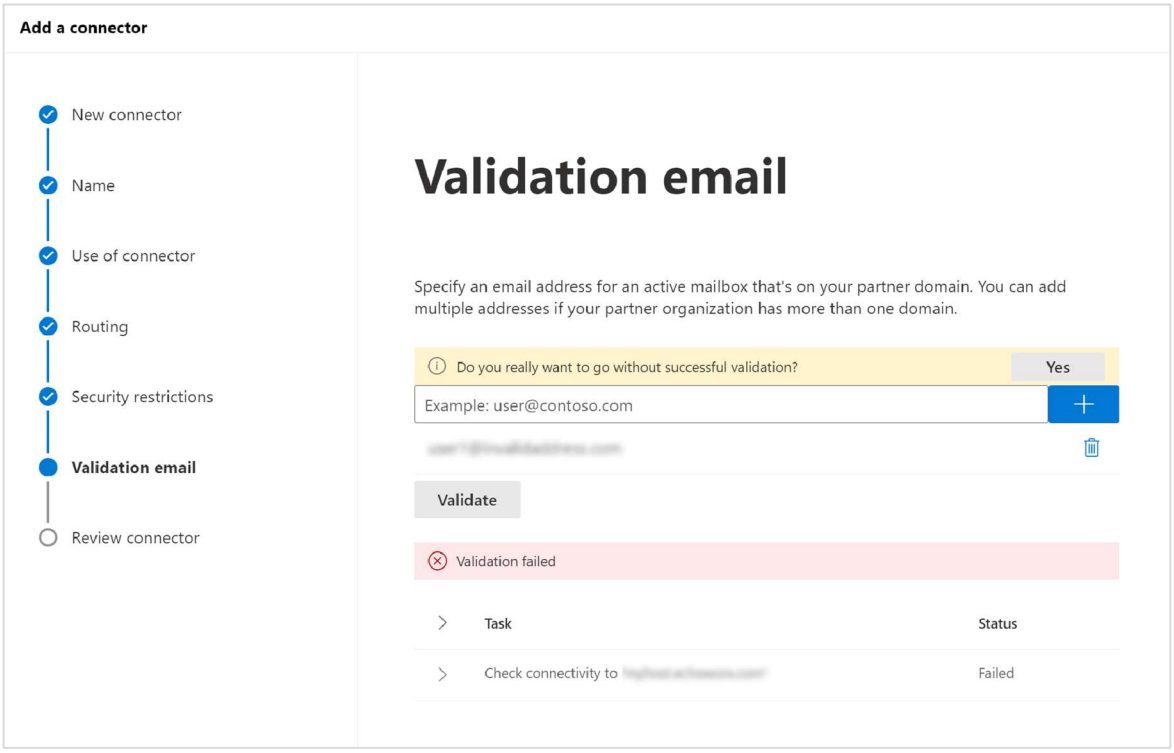
14. Click **Next**. The **Validation email** page appears.

15. Perform the following:

    a. Enter any valid or invalid recipient email address in **add email** field to test.

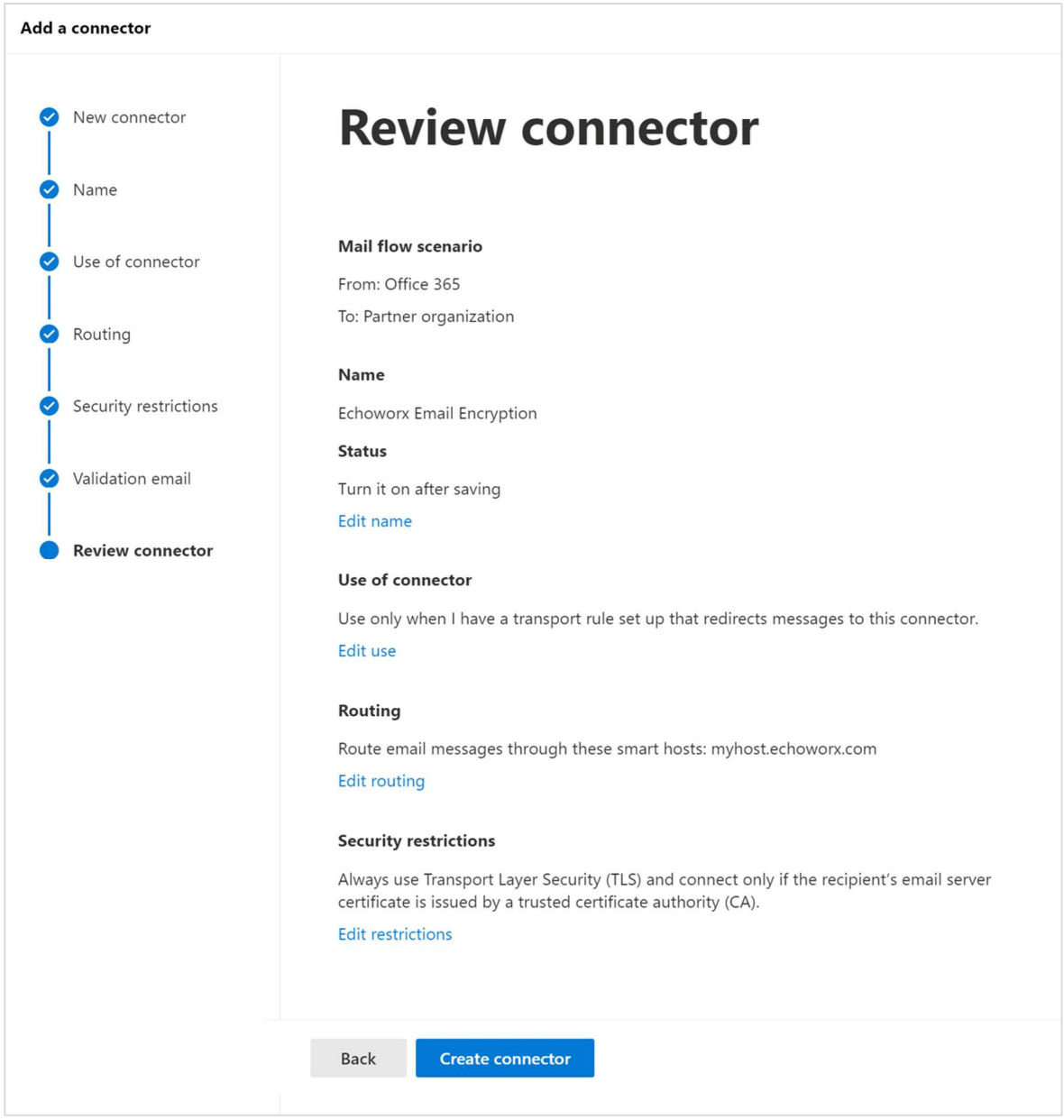
    b. Click the + icon, then click **Validate**.

    c. Validation should fail. Click **Yes** next to *Do you really want to go without successful validation?*



    d. Click **Next**. The Review connector page appears.

16. Review the connector settings and click **Create connector**.



17. Wait for the **Connector created** confirmation and click **Done**.

4. Create Mail Flow Rule for Encryption on Keyword in Subject

This section explains the steps to create an outbound rule that detects the message to be encrypted and routes over an outbound connector.

To create a sample rule to encrypt sender email messages that contain “secure:” or “encrypt:” in the subject header, follow the below steps:

1. Log in to Microsoft 365 admin center and navigate to **Exchange** Admin center. The Exchange admin center opens.
2. Click **Mail Flow** from the left navigation panel.
3. Click **Rules**.
4. To create a new rule, click + **Add a Rule**, and select **Create a new rule** from the list of options. A dialog box opens and the **Set rule conditions** page appears.
5. Perform the following in each section:
    a. **Name:** – Enter an appropriate name of the rule to be created as **Outbound Encryption based on keyword**.
    b. **Apply this rule if*** – Click the drop-down list and select **The subject or body** value. Click the sub-list beside and select the **subject includes any of these words** value. A dialog box opens. If the dialog box does not open, then click the ✎ icon. Enter or select values of the following:
        i. Enter the keyword **secure:** in **specify words or phrases** field.
        ii. Click **Add** to add the keyword.
        iii. Enter another keyword **encrypt:** in **specify words or phrases** field.
        iv. Click **Add** to add the keyword.
        v. Click **Save**. The dialog box closes.
    c. **And** – Select the + beside **Apply this rule if*** to add if unavailable. Click the drop-down list and select **The sender** value. Click the sub-list beside and select the is **external/internal** value. A dialog box opens. If the dialog box does not open, then click the ✎ icon. Enter or select values of the following:
        i. Click the drop-box under **select sender location** and select **inside the organization**.
        ii. Click **Save**.
    d. **Do the following*** – Click the drop-down list and select the **Redirect the message to** value. Click the sub-list beside and select **the following connector** value. A dialog box opens. If the dialog box does not open, then click the ✎ icon. Enter or select values of the following:
        i. Select **Echoworx Email Encryption** from the **select connector** drop-down list.
        ii. Click **Save**.

e. **Except if** – Click the drop-down list and select **The recipient** value. Click the sub-list beside and select the **is external/internal** value. A dialog box opens. If the dialog box does not open, then click the icon. Enter or select values of the following:

   i. Click the drop-box under **select recipient location** and select **inside the organization**.

   ii. Click **Save**.

6. Click **Next**. The **Set rule settings page** appears.
7. Perform the following in each section:

   a. **Rule mode** – Select **enforce**.

   b. **Stop processing more rules** – Check this checkbox.

> **Note**: Accept or modify other defaults as required.

8. Click **Next**. The **Review and finish** page appears.
9. Review and click **Finish**.

5. Create Mail Flow Rule for Sender User Outlook Encrypt Button

This section explains the steps to create a sample rule to encrypt sender email messages where the sender used the Echoworx Encryption Add-in for Outlook.

To create a rule, follow the below steps:

1. Log in to Microsoft 365 admin center and navigate to **Exchange** Admin center. The Exchange admin center opens.
2. Click **Mail Flow** from the left navigation panel.
3. Click **Rules**.
4. To create a new rule, click + **Add a Rule**, and select **Create a new rule** from the list of options. A dialog box opens and the **Set rule conditions** page appears.
5. Perform the following in each section:

   a. **Name:** – Enter an appropriate name of the rule to be created as **Outbound Encryption based on Outlook Encrypt Button**.

   b. **Apply this rule if*** – Click the drop-down list and select **The message headers…** value. Click the sub-list beside and select the **includes any of these words** value.

      i. Click the icon. A dialog box appears.

      ii. Specify the header name as **x-echoworx-encrypt**.

      iii. Click **Save**. The dialog box closes.

      iv. Click **Enter words**. A dialog box appears.

v. Enter **yes** in the **specify words or phrases** field.

vi. Click **Add** to add the keyword.

vii. Click **Save**. The dialog box closes.

c. **Do the following*** – Click the drop-down list and select the **Redirect the message to** value. Click the sub-list beside and select **the following connector** value. A dialog box opens. If the dialog box does not open, then click the icon. Enter or select values of the following:

i. Select **Echoworx Email Encryption** from the **select connector** drop-down list.

ii. Click **Save**.

d. **And** – Select the + beside **Apply this rule if*** to add if unavailable. Click the drop-down list and select **The sender** value. Click the sub-list beside and select the is **external/internal** value. A dialog box opens. If the dialog box does not open, then click the icon. Enter or select values of the following:

i. Click the drop-box under **select sender location** and select **inside the organization**.

ii. Click **Save**.

e. Click the + icon to add a new **Except if** row.

f. **Except If** – Click the drop-down list and select **The Recipient** value. Click the sub-list beside and select the **is external/internal** value. A dialog box opens. If the dialog box does not open, then click the icon. Enter or select values the following:

i. Click the drop-box under **select recipient location** and select **inside the organization**.

ii. Click **Save**.

6. Click **Next**. The **Set rule settings** page appears.
7. Perform the following in each section:
   a. **Rule mode** – Select **enforce**.
   b. **Stop processing more rules** – Check this checkbox.

   Note: Accept or modify other defaults as required.
8. Click **Next**. The **Review and finish** page appears.
9. Review and click **Finish**.

6. Sender Policy Framework

You are required to have DNS Sender Policy Framework (SPF) configured for the email domain(s) configured for email encryption.

Note: The following must appear in the email domain DNS SPF record:

include:_spf-us.echoworx.com

For more information on Sender Policy Framework, see:

- https://tools.ietf.org/html/rfc7208
- https://www.sparkpost.com/resources/email-explained/spf-sender-policy-framework/
- https://en.wikipedia.org/wiki/Sender_Policy_Framework
- https://support.google.com/a/answer/33786?hl=en

7. Test your Setup

With the Transport Rule Connector and sample rules created, waiting for some time for the changes to be replicated across the M365 infrastructure, and propagation of your DNS changes, you should be able to test email encryption by sending an email message from one of the email domains configured for email encryption to an external email recipient. The recipient should receive the encrypted email message. The recipient should also test the secure reply method provided by the encrypted message they received.

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
Echoworx