

Office 365 Message Encryption (OME) Email Encryption Reference Guide

FSSA Privacy & Security Compliance Office



Version 1.0

Contents

Introduction.....	1
What is the cost to FSSA?	1
How does it work?	1
Why use OME?	1
How can FSSA Staff obtain access to OME?	2
Steps for Sending Encrypted Email through Outlook ProPlus Desktop App	4
How does the External Recipient get access to the encrypted email message?	4
OME Email Retention.....	9
Additional Support Options.....	9

Introduction

Office 365 Message Encryption (OME) is a service built on Azure Rights Management (Azure RMS) that lets you send encrypted email to people inside or outside the state network (i.e., to an email address that does not end with **fssa.in.gov**), regardless of the destination email address (Gmail, Yahoo! Mail, Outlook.com, etc.). Email sent to external recipients outside the state network can only be encrypted using OME. It is FSSA's policy that any email messages that contain **CPI** (Client Personal Information) sent outside the state network must be encrypted.

What is the cost to FSSA?

This service is provided to FSSA users and is hosted by the Indiana Office of Technology (IOT) at no additional cost. External users (e.g., those who are not using an **fssa.in.gov** email account) will be able to receive and read their encrypted messages without any additional cost or client software.

How does it work?

Office 365 Message Encryption is an online service that's built on Microsoft Azure Rights Management (Azure RMS) which is part of Azure Information Protection. This service includes encryption, identity, and authorization policies to help secure your email.

When someone sends an email message that matches an encryption mail flow rule, the message is encrypted before it's sent. Supported Outlook clients include Outlook desktop, Outlook Mac, Outlook mobile on iOS and Android, and Outlook on the web (formerly known as Outlook Web App).

Recipients of encrypted messages who receive encrypted email sent to their Outlook.com, Gmail, and Yahoo accounts receive an email that directs them to the OME Portal where they can easily authenticate using a Microsoft account, Gmail, or Yahoo credentials.

Why use OME?

Emails you send outside the state network (i.e., to an email address that does not end with **fssa.in.gov**) travel over the Internet. Because the email message is not encrypted it is possible for others to see the message content. Those messages often are retained by the recipient's email provider (e.g., Gmail, Yahoo, etc.), which means the email provider may be able to see the message content as well.

By encrypting the email message, it cannot be seen by others as it travels over the Internet or by any email provider.

In addition, certain federal laws require that we encrypt any emails that contain client personal information. This is done automatically when we send emails inside the state network; but it is not automatically done for emails sent outside the state network unless OME is used.

Overall, the use of OME minimizes the risk that an unauthorized person could see confidential, client personal information you send by email.

How can FSSA Staff obtain access to OME?

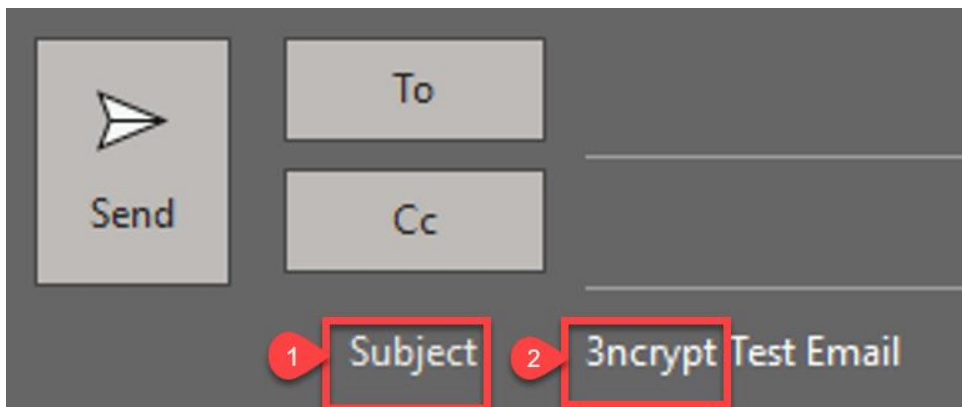
FSSA staff who have been approved by their business unit to send confidential emails to external recipients have three (3) options (see below) they can use to send an encrypted message. If you are uncertain whether you have been approved to send confidential email messages, please consult your supervisor.

Option #1 3ncrypt:

Type “3ncrypt” (i.e., replaces the letter “E” with the number “3” in the subject of the message; this will also result in the message being encrypted by OME. This method can be used on multiple devices such as smart phones, tablets, Outlook Web Access, and Outlook via Citrix (Figure 1.1).

Figure 1.1

In the **** (1) Subject line** of a message typing **(2) 3ncrypt** to an external recipient will encrypt the message.



****NOTE: Do not put confidential data in the subject line!**

The subject line is not encrypted.

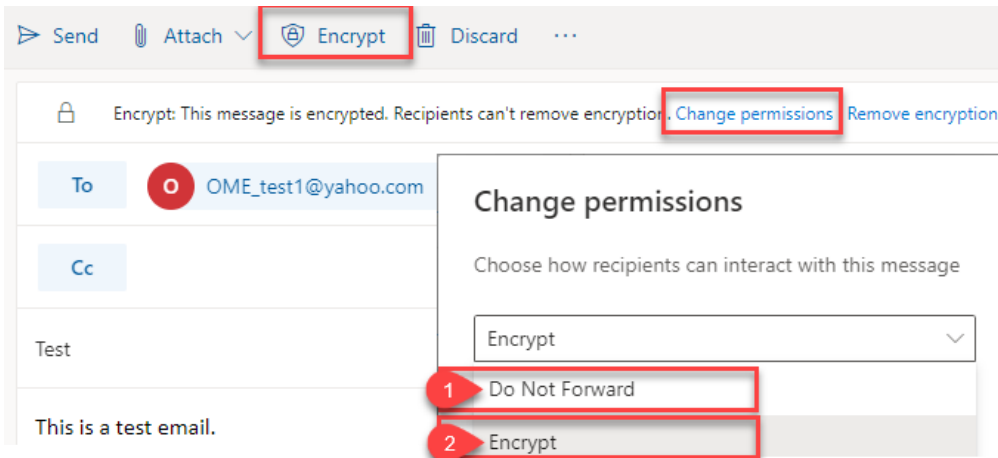
****NOTE:** When you receive a reply in your Outlook inbox from a message that you sent 3ncrypt, your email reply back is no longer secure. You can either delete the PII/PHI and send normally or you **must** add 3ncrypt back to the subject line prior to replying to the email.

Option #2: Outlook OWA (outlook.office365.com):

Figure 1.2

From a new message click the “**Encrypt**” button.

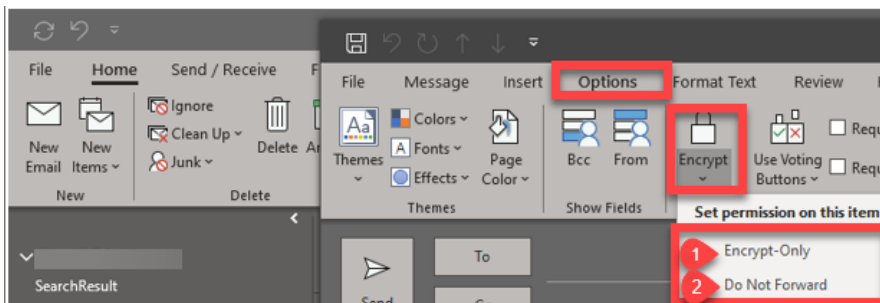
To change the encryption type, from (1) “**Encrypt**” to (2) “**Do Not Forward**” click “**Change permissions**” and then select the setting you want.



Option #3 Outlook ProPlus:

In the Outlook ProPlus Desktop App, FSSA users should have the Options Tab in the Outlook menu bar (Figure 1.3). The FSSA user should contact the IOT helpdesk if they do not have the options tab. FSSA users should click on the “Options” button and then the Encrypt button option 1. For **Encrypt-Only** for their message to be encrypted (when sent to external recipients Outside-the-State-Network). 2. For **Do Not Forward** – This option will encrypt an email and restricts the message from being forwarded, printed, or copied.

Figure 1.3 The “Encrypt” button is located in the Outlook message form Under “Options” when composing a new email message.



Steps for Sending Encrypted Email through Outlook ProPlus Desktop App:

- Step 1: Open Microsoft Outlook and select the “New” to open a new email.
- Step 2*: Enter the recipient of your email in either the “To...” or “Cc...”
- Step 3: Attach any documents (if necessary).
- Step 4: To send the email encrypted, click on the “Options” tab then click on the Encrypt button and choose the (1) “**Encrypt-Only**” or (2) “**Do Not Forward**” option.
- Step 5: Click on “**Send**” to send the email.

***NOTE: It’s very important that you use extreme caution when addressing your message to avoid sending the email to the wrong recipient. This may result in a breach of confidentiality since any user who receives your email will have the ability to open the encrypted message.**

How does the External Recipient get access to the encrypted email message?

OME will send an email to the recipient from the FSSA user (**Figure 1.4**). The email includes a box “**Read the message**”.

It’s very important to test this process with the external recipient when using OME with the recipient for the first time. Send a test message (without confidential data) just to confirm the recipient does not have any problems or questions about accessing the email message. Once verified, you may proceed with sending the confidential message.

Figure 1.4

The intended recipient will get an email message that looks like the image below, telling them that they have a Protected (encrypted) message from you, the recipient clicks **“Read the message”** box:

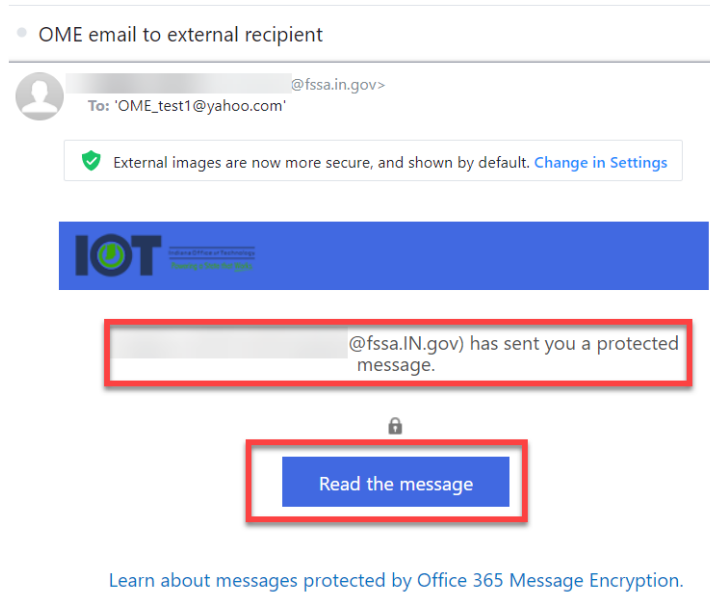
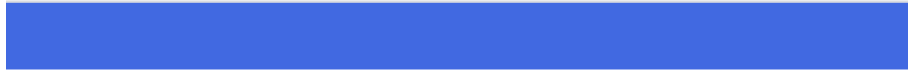
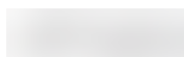


Figure 1.5

The recipient then clicks “**Sign in with a One-time passcode**”. A One-time passcode will be sent to the same email inbox that the recipient received the original message in. The recipient checks their email inbox for the passcode shown in (Figure 1.7).



@fssa.IN.gov has sent you a protected message

[Sign in with a One-time passcode](#)

[Need Help?](#)

[Privacy Statement](#)

Figure 1.6

The following figure is the page that results in clicking the “**Sign in with a One-time passcode**” link. This is where the recipient will enter the passcode that they received in another email shown in (Figure 1.7).



We sent a one-time passcode to OME_test1@yahoo.com.

Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.

One-time passcode

This is a private computer. Keep me signed in for 12 hours.

[Continue](#)

Didn't receive the one-time passcode? Check your spam folder or [get another one-time passcode](#).

Figure 1.7

The figure below is an email like the one the recipient will receive containing (Figure 1.8). **Microsoftoffice365@messaging.microsoft.com** is the URL that sends the passcode, make sure you don't miss it in your junk mail.

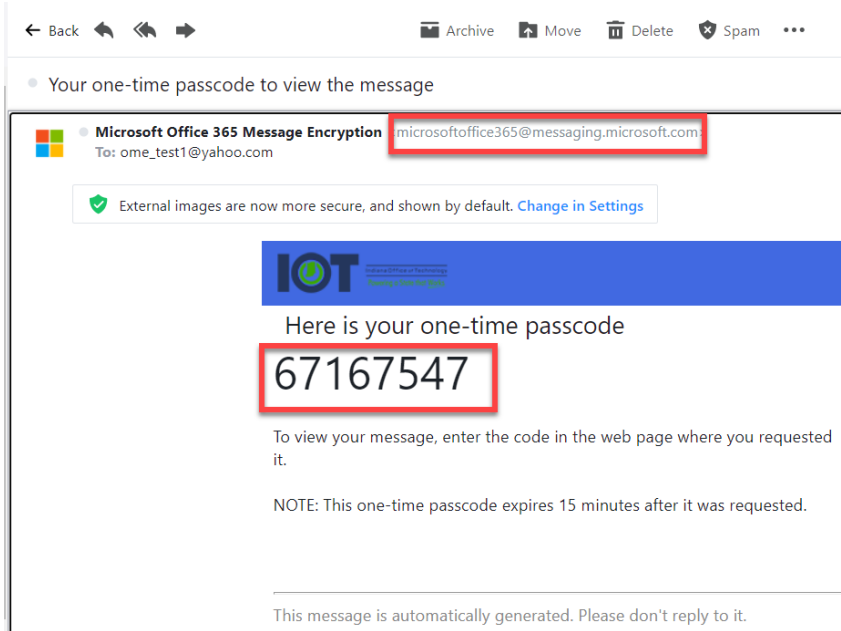


Figure 1.8

The recipient will enter the passcode from the email shown in (Figure 1.7) in the box provided. The recipient then clicks “continue”.

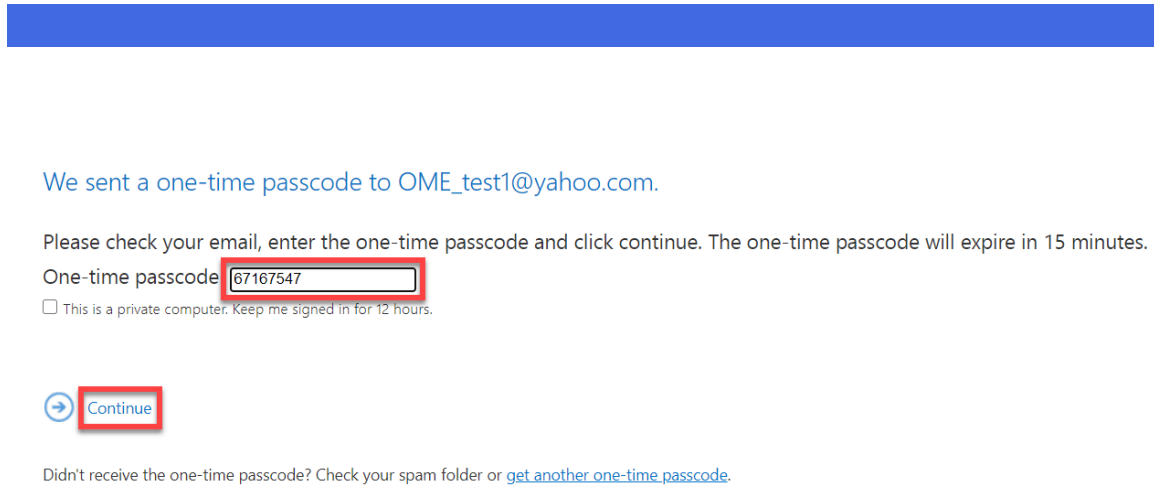
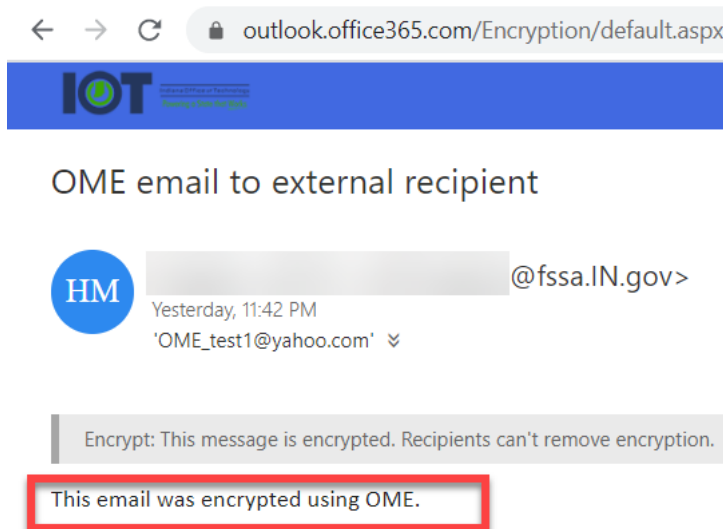


Figure 1.9

The recipient can now view the encrypted email.



To avoid an interruption in your business operations, it’s important to have a communications plan with your external partners to whom you will be sending OME emails. They should be alerted that they will be receiving an OME email in lieu of a direct email from your business unit.

OME Email Retention:

OME email messages sent from your FSSA Outlook account will be retained in your Outlook Sent Items folder.

Additional Support Options:

For Technical Support Questions please open an IOT Hepdesk ticket iot.in.gov/hda or call 317.234.4357.

Privacy and/or Security policy questions regarding the FSSA requirements for using OME may be sent to the following:

H. Cliff McCullough, Director
FSSA Privacy & Security Compliance Office
(317) 232-4732

FSSA.PrivacyOffice@fssa.in.gov