

There are 3 phases to setting up Encrypted Emails from O365.

PHASE 1 – ENABLE AZURE RIGHTS MANAGEMENT

1. First check to see if you have “Azure Rights Management” enabled on your account.
 - a. Sign in the Office 365 as an administrator and go to the Admin Portal.
 - b. Expand “Service Settings”
 - c. If “Rights Management” appears, skip to step 3c.
2. To order Azure Rights Management (free):
 - a. Go to this webpage: <https://portal.office.com/commerce/catalog.aspx?empty=1>
 - b. Find “Azure Rights Management for Faculty”. It should be listed as £0.
 - c. Follow the screens to order enough copies to cover all your staff. Don’t worry, you can always amend this for free at a later date.
3. Once you have Azure Rights Management added to your account, you need to enable it.
 - a. Go to the Admin Portal of Office 365
 - b. Expand “Service Settings”
 - c. Click on “Rights Management”
 - d. On the Rights Management page, select “Manage” (just a small text link)
 - e. Now click on “Activate”
 - f. Follow the prompts to activate Rights Management

PHASE 2 – ENABLE IRM LICENSING

If you attempt to use Office 365 Message Encryption before first enabling IRM licensing, the operation will fail and give you this message:

You can't create a rule containing the ApplyOME or RemoveOME action because IRM licensing is disabled.

To remediate this, we need to enable IRM licensing using the Admin portal and PowerShell. Follow these steps:

1. These steps will be done in PowerShell. Open Windows Azure Active Directory Module for Windows PowerShell, found here:
<http://technet.microsoft.com/library/jj151815.aspx>
2. Connect your PowerShell session to your Office 365 tenant and Exchange Online by entering the following:
`$msolcred = Get-Credential` (Answer the credential prompt with your Office 365 tenant administrator credentials)
`Connect-MsolService -Credential $msolcred`

`$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $msolcred -Authentication Basic -AllowRedirection`
`Import-PSSession $Session`
4. Enable IRM licensing by typing:
`Set-IRMConfiguration -RMSOnlineKeySharingLocation https://sp-rms.eu.aadrm.com/TenantManagement/ServicePartner.svc`
5. After setting the key sharing location, the next step is to import the Trusted Publishing Domain (TPD). Do so by entering the following:
`Import-RMSTrustedPublishingDomain -RMSOnline -name “RMS Online”`
6. The final step is to activate the internal IRM licensing. Do so by entering the following:
`Set-IRMConfiguration -InternalLicensingEnabled $True`
7. After enabling IRM licensing, verify the functionality by entering:
`Test-IRMConfiguration -RMSOnline`

The test should pass with the result OVERALL RESULT: PASS.

NOTE: Enabling IRM licensing might need several hours for the change to take effect. If possible, allow 8 hours to pass before proceeding with STEP 2.

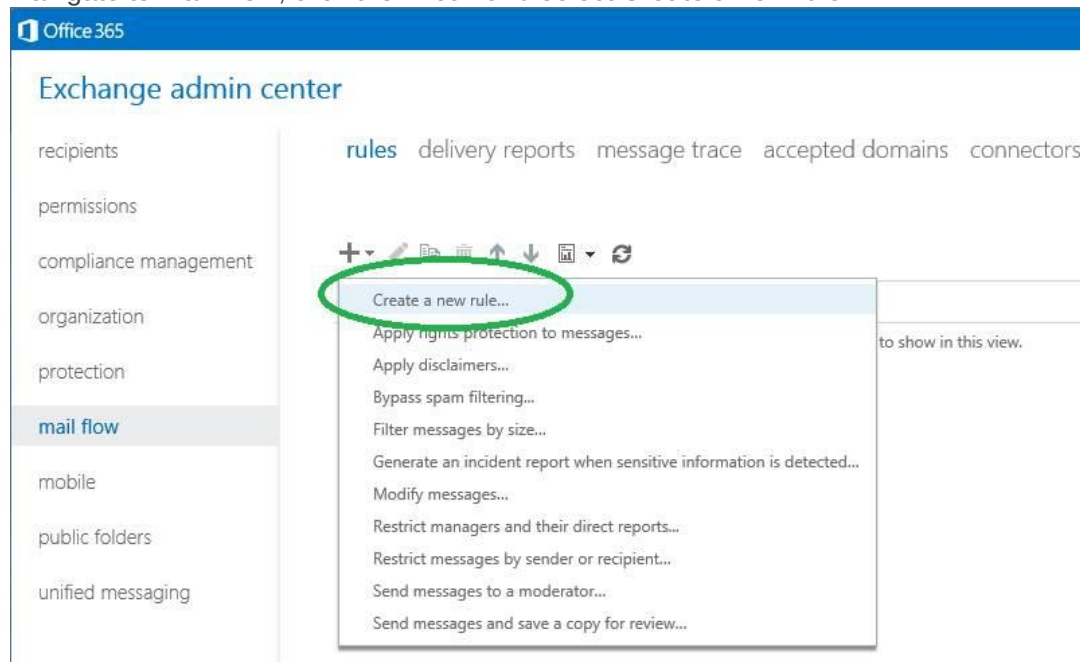
PHASE 3 – CREATE THE OME TRANSPORT RULE

We will create a transport rule that enables Office 365 Message Encryption if the message is sent to a recipient outside the organization and the Sensitivity header have been set to Confidential.

PLEASE NOTE: You can change this functionality however you see fit, but this was the one that confused our end users the least!

Follow these steps:

1. Log in to your Office 365 Admin Portal and navigate to Exchange Control Panel (Admin\Exchange).
2. Navigate to Mail Flow, click the + icon and select Create a new rule...



3. Give the rule a suitable name and click More options...

[Help](#)

new rule

Name:

*Apply this rule if...

*Do the following...

Properties of this rule:

☒ Audit this rule with severity level:

Choose a mode for this rule:

☒ Enforce
☐ Test with Policy Tips
☐ Test without Policy Tips

[More options...](#)

Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. [Learn more](#)

4. From here you can set your condition as it fits your needs, but for this example wil will inspect the Sensitivity header and apply Message Encryption based on that. To do so, select the following conditions:

Apply this rule if... A message header includes any of these words

new rule

Name:

*Apply this rule if...

Select one

Select one

The sender... ▶

The recipient... ▶

The subject or body... ▶

Any attachment... ▶

The message... ▶

The sender and the recipient... ▶

The message properties... ▶

A message header... ▶ includes any of these words

[Apply to all messages] matches these text patterns

5. Complete the Apply this rule if-condition by clicking the properties Enter text and Enter word so that the condition makes 'Sensitivity' header includes 'Confidential'

new rule

Name:
Message Encryption Rule

*Apply this rule if...

A message header includes... 'Sensitivity' header includes 'Confidential'

add condition

6. Click Add condition and select The recipient... Is external/internal. Click Select one... and select Outside the organization and hit OK

*Apply this rule if...

☒ A message header includes... 'Sensitivity' header includes 'Confidential'

and

☒ The recipient is located... Outside the organization

add condition

7. Proceed with clicking Do the following... and select Modify the message security... and select Apply Office 365 Message Encryption
- new rule

Name:
Message Encryption Rule

*Apply this rule if...

☒ A message header includes... 'Sensitivity' header includes 'Confidential'

and

☒ The recipient is located... Outside the organization

add condition

*Do the following...

Select one

Select one

Forward the message for approval...

Redirect the message to...

Block the message...

Add recipients...

Apply a disclaimer to the message...

Modify the message properties...

Modify the message security...

Prepend the subject of the message with...

Notify the sender with a Policy Tip...

Generate incident report and send it to...

Apply rights protection

Require TLS encryption

Apply Office 365 Message Encryption

Remove Office 365 Message Encryption

save cancel

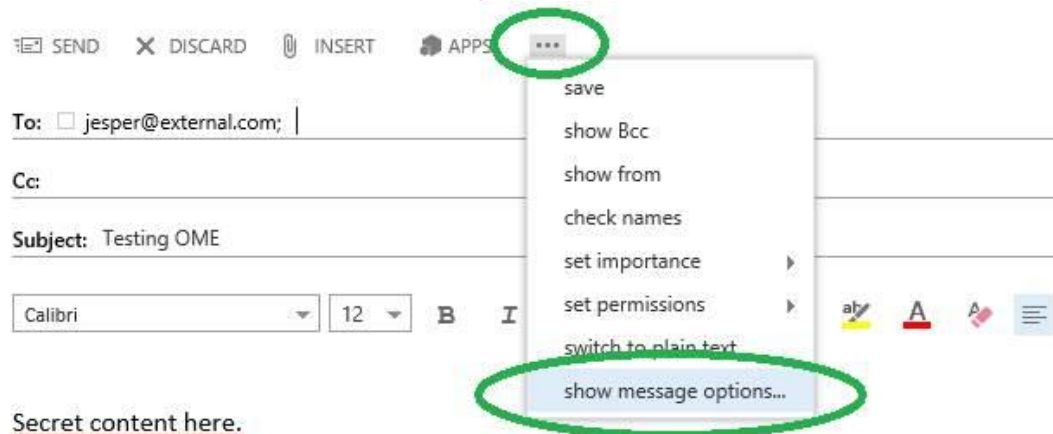
8. Hit Save at the bottom of the New rule editor. (If you get the message that IRM licensing is not enabled and have completed STEP 1 – please allow more time for the change to take effect, as stated in the Note after STEP 1).

TESTING – SEND A CONFIDENTIAL MESSAGE WITH OME

We will create a message with the sensitivity level set to Confidential and send this to a recipient outside our organization. Our transport rule will apply Office 365 Message Encryption to the message.

Follow these steps:

1. Open Outlook or Outlook Web App. Both clients have the native functionality to set the sensitivity header. In the example, I will use OWA, but the procedure is the same in Outlook.
2. Compose a new message. Enter an external recipients, give the message a subject and some content, then click ... and Show message options...



3. Set the message Sensitivity level to Confidential and hit OK

message options

Sensitivity:

Confidential

☐ Request a delivery receipt

☐ Request a read receipt

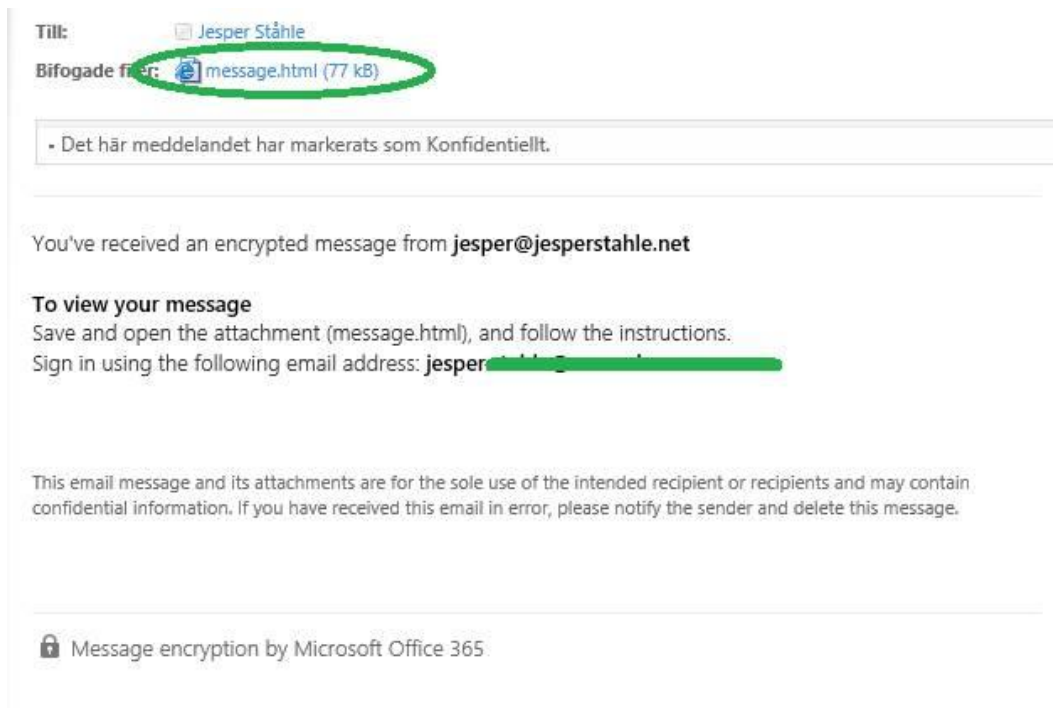
ok cancel

NOTE: In the rich Outlook client, Sensitivity options are found under Message Options\More options\Sensitivity.

4. Send the message.

RECEIVE AND OPEN THE ENCRYPTED MESSAGE

1. Open the inbox of the external mailbox and find the encrypted message



2. As you can see, the message includes an attached HTML-document. Open the attachment.
3. Click VIEW YOUR ENCRYPTED MESSAGE to continue



encrypted message from
jesper@jesperstahle.net

To view your message, sign in using the following email address:
jesper@jesperstahle.net



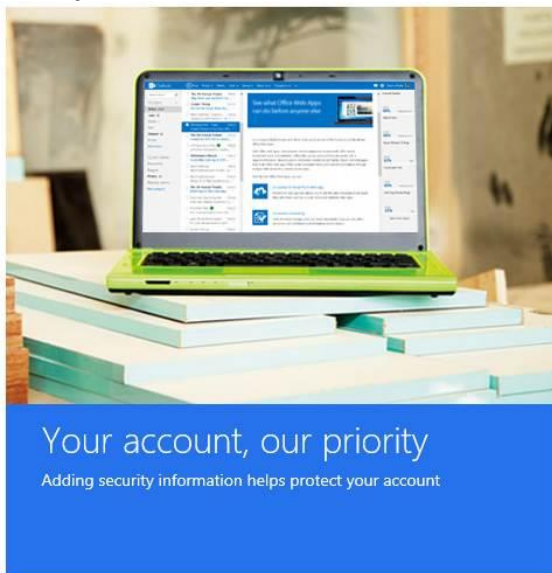
Message encryption by Microsoft Office 365

4. To be able to read the encrypted message, you are required to sign in with a Microsoft Account or Corporate Credentials (WAAD/Office 365 account) that has a username that matches the e-mail address to which the encrypted message was sent. This is the same principle as External Sharing in SharePoint Online/OneDrive for Business. In the example, I will login with a Microsoft Account.

Which account would you like to sign in with to view your encrypted message?



5. Enter your Microsoft Account credentials.



Sign in

Microsoft account [What's this?](#)

jesper@external.com

••••••••••

☐ Keep me signed in

Sign in

[Can't access your account?](#)

[Sign in with a single-use code](#)

The message will now load and be displayed in the browser.

Encrypted Message

Jesper Ståhle

Sign Out



Testing OME

← REPLY ← REPLY ALL → FORWARD



Jesper Ståhle <jesper@jesperstahle.net>

Sun 2/16/2014 12:38 AM

To: jesper. [redacted]

• This message has been marked as Confidential.

Secret content here.