**Minimum Requirements**

* ATP Plan 1 or 2
* Global admin or exchange admin privileges
* Oauth Authentication configured within exchange

**Turn on Add-in (For up to date information, visit** [**https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/enable-the-report-message-add-in?view=o365-worldwide#get-and-enable-the-report-message-add-in-for-your-organization**](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/enable-the-report-message-add-in?view=o365-worldwide#get-and-enable-the-report-message-add-in-for-your-organization)**)**

1. In the Microsoft 365 admin center, go to the Settings, integrated Apps & Add-ins page at <https://admin.microsoft.com/AdminPortal/Home#/Settings/AddIns>, and then click Deploy Add-In.



1. In the Deploy a new add-in flyout that appears, review the information, and then click Next.
2. On the next page, click Choose from the Store.



1. In the Select add-in page that appears, click in the Search box, enter Report Message, and then click Search . In the list of results, find Report Message and then click Add.



1. In the dialog that appears, review the licensing and privacy information, and then click Continue.
2. In the Configure add-in page that appears, configure the following settings:
	* Assigned users: Select one of the following values:
		+ Everyone (default)
		+ Specific users / groups
		+ Just me
	* Deployment method: Select one of the following values:
		+ Fixed (Default): The add-in is automatically deployed to the specified users and they can't remove it.
		+ Available: Users can install the add-in at Home > Get add-ins > Admin-managed.
		+ Optional: The add-in is automatically deployed to the specified users, but they can choose to remove it.



When you're finished, click Deploy.

1. In the Deploy Report Message page that appears, you'll see a progress report followed by a confirmation that the add-in was deployed. After you read the information, click Next.



1. On the Announce add-in page that appears, review the information, and then click Close.



**Create a mail-flow rule to view user submitted messages. (for up to date information, visit https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-mail-flow-rules-to-see-what-your-users-are-reporting-to-microsoft?view=o365-worldwide#use-the-eac-to-create-a-mail-flow-rule-to-receive-copies-of-reported-messages)**

1. In the EAC, go to Mail flow > Rules.
2. Click Add  and then select Create a new rule.
3. In the New rule page that opens, configure the following settings:
4. Name: Enter a unique, descriptive name for the rule. For example, Bcc Messages Reported to Microsoft.
5. Click More Options.
6. Apply this rule if: Select The recipient > address includes any of these words: In the Specify words or phrases dialog that appears, enter one of the following values, click Add , and repeat until you've entered all the values.

junk@office365.microsoft.com

abuse@messaging.microsoft.com

phish@office365.microsoft.com

false\_positive@messaging.microsoft.com

1. To edit an entry, select it and click Edit . To remove an entry, select it and click Remove .
2. When you're finished, click OK.
3. Do the following: Select Add recipients > to the Bcc box. In the dialog that appears, find and select the recipients that you want to add. When you're finished, click OK.

**Search and Delete emails that are reported:**

1. Go to Office 365 Security & Compliance Center
2. Under Search & investigation > select Content Search



1. Click on the + symbol to create a new search
2. Select a name for the search
3. Choose “search all mailboxes” > click next
4. Enter key qualities about the email, that will isolate it from other emails. You can use different keyword queries and search conditions to modify your search. Learn more about it [here](https://support.office.com/en-us/article/Keyword-queries-and-search-conditions-for-Content-Search-c4639c2e-7223-4302-8e0d-b6e10f1c3be3?ui=en-US&rs=en-US&ad=US)
5. Run the search. Then you can review the results.
6. Open Powershell and connect to the security & compliance center
7. Open Microsoft Exchange Powershell
8. Run the commands below:

NOTE: IF MFA IS ENABLED USE the Exchange Powershell Module and THIS COMMAND TO CONNECT

* Connect-IPPSSession -UserPrincipalName UPN HERE

 Then run this command to find the search you created and delete the emails it found (NOTE: put the name of the content search you created in quotes after

 -SearchName):

* New-ComplianceSearchAction -SearchName “SEARCH NAME HERE" -Purge –PurgeType SoftDelete

Example below:

 

1. Type Y then hit enter
2. Be sure to disconnect the remote PowerShell session when you're finished.To disconnect the remote PowerShell session, run the following command.
* Remove-PSSession $Session