

Search Content in Microsoft Purview

Use Case: If an email was sent in error or a malicious email has been sent to a large number of recipients, one can find and remove that data using Microsoft 365 Security and Compliance Powershell.

First, [Connect to Microsoft 365 Exchange Online](#)

Second, [Connect to Microsoft 365 Security and Compliance](#)

Create the search

```
New-ComplianceSearch -Name "An Email Search" -ExchangeLocation All -ContentMatchQuery  
'From:externalsender@example.com'
```

Refine the search

This example has a date range and subject specified in the query.

```
New-ComplianceSearch -Name "An Email Search" -ExchangeLocation All -ContentMatchQuery  
'(Received:M/DD/YYYY..M/DD/YYYY) AND (Subject:"An email not to be seen")'
```

This example searches [specific folders](#) in a specific mailbox.

```
New-ComplianceSearch -Name "An Email Search" -ExchangeLocation recipient@example.com -  
ContentMatchQuery "((folderid:YFDRIJRBV4ZOBALB0F9E170RM3MQGBLYD8KY7YZZTJFCO14I) and  
(folderid:NC5MOAYATELI8Y477ALCKE9E5L08Z4OJLD4Z1I71YD836M33P) and
```

```
(folderid:N34157DZ541GZQXLG0EKP5F8E9AC91558845M1GYJLBV7AOVS))"
```

Start the search; after you create the search, you will have to start it.

```
Start-ComplianceSearch -Identity "An Email Search"
```

Perform an action on the results; once you have the results, do something with it.

```
New-ComplianceSearchAction -SearchName "An Email Search" -Purge -PurgeType SoftDelete
```

Running the command in variables enables you to create the search and then start it with one stroke of the return key.

```
$Search=New-ComplianceSearch -Name "Remove an email" -ExchangeLocation All -ContentMatchQuery  
'(From:sender@example.com) AND (Subject:"An email subject") AND (Received:M/DD/YYYY..M/DD/YYYY)'  
Start-ComplianceSearch -Identity $Search.Identity
```

To check the status of a running search, run the command below. Pipe it to `fl` (Format-List) to see details.

```
Get-ComplianceSearch -Identity "An Email Search"
```

SoftDelete removes the email, but it is still recoverable. **HardDelete** removes the email and it is not recoverable. It does not move it to the recipient's *Deleted Items* folder.

[Microsoft Learn: New-ComplianceSearch](#)

[Microsoft Learn: Search Conditions](#)

Revision #12

Created 18 August 2024 20:23:18 by orngbnch

Updated 4 September 2024 13:19:57 by B.B.B.Ben E. N. Agents