

# Powershell

- [Search Content in Microsoft Purview](#)
- [Show Mailbox Rules for a Mailbox](#)
- [Connect to Exchange Powershell](#)
- [Grant Purview Export Permission](#)
- [Connect to Security and Compliance Powershell](#)
- [Exchange Mailbox Statistics](#)
- [Connect to Sharepoint](#)
- [Get Intune Managed Device Information](#)
- [Manually Sync macOS Device with Intune](#)
- [Change Intune macOS Personal Ownership to Company](#)

# 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](#)

# Show Mailbox Rules for a Mailbox

Prerequisites: [Connect to Exchange Powershell](#)

Get the rules for a mailbox

```
Get-InboxRule -Mailbox "name@example.com"
```

# Connect to Exchange Powershell

Prerequisites: Install Exchange Powershell

To connect to Exchange Powershell with Multi-Factor Authentication, in a Microsoft Powershell window, run the following command.

```
Connect-ExchangeOnline
```

This will open a new login window. After login, the window will close and the Exchange Powershell session will be active.

[Microsoft: connect-to-exchange-online-powershell](#)

# Grant Purview Export Permission

When exporting the results of a Microsoft Purview Content Search, the user must have the permission. This permission cannot be granted by the same user to which it is being granted.

First, [Connect to the Security and Compliance Powershell](#)

Add eDiscovery Manager Role to admin:

```
Add-RoleGroupMember "eDiscovery Manager" -Member <username>
```

Promote admin to Case Admin

```
Add-eDiscoveryCaseAdmin -User <username>
```

[Microsoft Answers: user-with-global-administrator-and-compliance-admi](#)

# Connect to Security and Compliance Powershell

To connect to the Microsoft 365 Security and Compliance Powershell:

- Open a Powershell Window
- Type the following command, where `<UPN>` is the admin username

```
Connect-IPPSSession -UserPrincipalName <UPN>
```

# Exchange Mailbox Statistics

Get size, date or `FolderId` for folders in an Exchange Mailbox.

```
Get-MailboxFolderStatistics -Identity <mailbox-identity>
```

To see folders outside of the [IPM Subtree](#), add the `-FolderScope` flag.

```
-FolderScope NonIPMRoot
```

Export Results to a CSV

```
Get-MailboxFolderStatistics -Identity <mailbox-identity> | Export-Csv <path-to-csv>
```

To make the information easier to read, pipe to the `Format-Table` command and specify which columns to view.

```
ft Name,FolderPath,LastModifiedTime,FolderType,FolderSize
```

According to the [Microsoft Documentation](#), the User folders count toward the storage quota.

The group mailbox is distributed in various `TargetQuota`, namely System, Recoverable and User. The folders matching `TargetQuota` "User" is the only one considered in the calculation of the group quota.

To check the size of only User folders, pipe to the `where` command.

```
where { $_.TargetQuota -like 'User' }
```

To check the size of a specific folder, pipe to the `where` command.

```
where { $_.FolderPath -like '/Inbox' }
```

[Microsoft Documentation - Get-MailboxFolderStatistics](#)

# Connect to Sharepoint

Connect to the Sharepoint Powershell

```
Connect-SPOService -Url https://example-admin.sharepoint.com -credential admin@example.com
```

# Get Intune Managed Device Information

To get device information for Intune managed devices, use the `Get-MgDeviceManagementManagedDevice` cmdlet using the [Exchange Powershell module](#).

Get all devices.

```
Get-MgDeviceManagementManagedDevice -All:$true
```

Filter devices by device name.

```
-Filter "contains(DeviceName,'<device_name>')"
```

Get specific devices from a CSV.

```
Import-Csv <csv_name>.csv | % { Get-MgDeviceManagementManagedDevice -All:$true -Filter  
"contains(DeviceName,'${_}.Name')"
```

# Manually Sync macOS Device with Intune

In Company Portal, click the ellipses and **Check Status** or press **command+option+S**.

To trigger a sync from the CLI, force close the Intune Agent process.

Use `ps` to list running processes; the `-A` flag specifies all running processes. Pipe the output to the `grep` command and search for the Intune MDM agent.

```
ps -A | grep IntuneMdmAgent
```

This confirms the agent is running in the following location.

```
/Library/Intune/Microsoft Intune Agent.app/Contents/MacOS/IntuneMdmAgent
```

Kill the Intune MDM Agent. The agent will automatically restart and trigger a check-in and sync with Intune.

```
killall IntuneMdmAgent
```

# Change Intune macOS Personal Ownership to Company

```
Get-MgDeviceManagementManagedDevice -All | Where-Object {$_.ManagedDeviceOwnerType -eq "unknown" -  
and $_.OperatingSystem -like "macOS"} | % { Update-MgDeviceManagementManagedDevice -ManagedDeviceId  
$_ .Id -ManagedDeviceOwnerType company }
```