Microsoft 365

- 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
- Admin Center
- Exchange
  - Prevent Spoofing of Executives
- Azure/Entra
  - Azure Dynamic Groups
  - Add user to Azure AD Application
- Intune
  - Reset a Windows Device
- Sharepoint
  - Share content with external users
  - Manage OneDrive Profiles
- Security and Compliance

- Outlook
  - Change filter settings in Outlook on the Web
  - Send as a Group in Outlook
  - Setup Microsoft 365 Account

Powershell

Powershell

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:YFDRIJRBV4ZOBAULB0F9E170RM3MQGBLYD8KY7YZZTJFCO14I) 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]

Powershell

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 windo, 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

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>
```

Powershell

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 specifc folder, pipe to the `where` command.

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

[Microsoft Documentation - Get-MailboxFolderStatistics]

Powershell

Connect to Sharepoint

Connect to the Sharepoint Powershell

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

Powershell

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)')" }
```

Powershell

Manually Sync macOS Device with Intune

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

To trigger a sync form 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
```

Powershell

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 }
```

Admin Center

https://admin.microsoft.com/

Exchange

Exchange

Prevent Spoofing of Executives

To add a disclaimer for incoming emails that bear the name of an executive, go to the Exchange Transport Rules and create a rule.

https://admin.exchange.microsoft.com/#/transportrules

Rule Conditions:

The Message Header `From` **Contains** `executive names`

AND

The message is from an external sender

Then Prepend Disclaimer

```
'<h1 style="front-size: 150%;"><span style="text-decoration: underline; color: #ff0000;"><strong>WARNING!</strong></span><span style="color: #ff0000;"><strong> -</strong>This might be a phishing attempt.<strong>- Orange Bench</strong></span></h1>'
```

Azure/Entra

Azure Dynamic Groups

Azure Dynamic Group Membership Rules

Rule Syntax to add group members based on the criteria

- Account is active
- Primary Email Address is at domain `example.com`

```
(user.accountEnabled -eq true) -and (user.mail -contains "@example.com")
```

- License includes `Exchange Online (Plan 1)`
- Plan is enabled

```
user.assignedPlans -any (assignedPlan.servicePlanId -eq "9aaf7827-d63c-4b61-89c3-182f06f82e5c" -and assignedPlan.capabilityStatus -eq "Enabled")
```

- Users that are members of group with Object ID `9dba4c67-5cd4-449d-a1c3-51865c374cab`

```
user.memberof -any (group.objectId -in ['9dba4c67-5cd4-449d-a1c3-51865c374cab'])
```

- Username contains `@example`
- Email Alias contains `@example`
- Company Name is `Example Company`

```
(user.userPrincipalName -contains "@example") or (user.proxyAddresses -any (_ -contains "@example")) or (user.companyName -eq "Example Company")
```

Microsoft Learn | Dynamic Rules

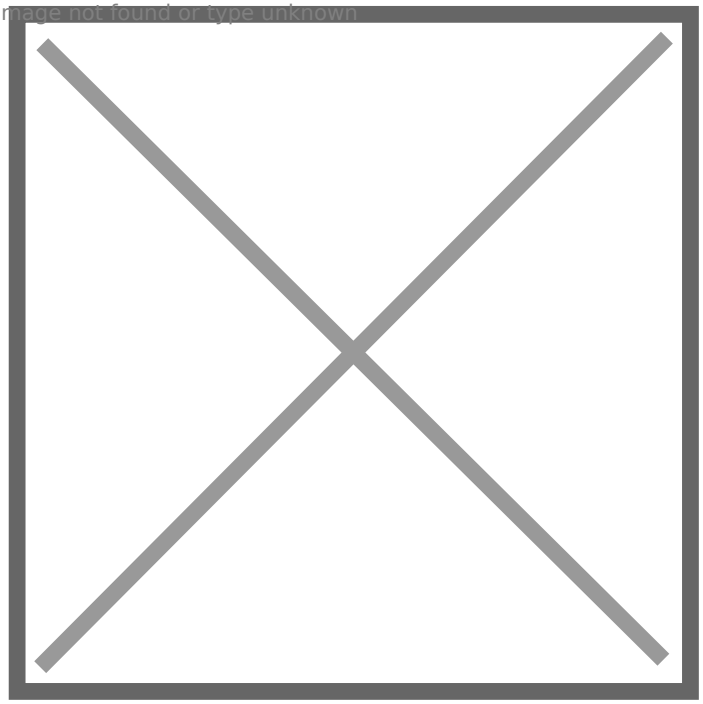
Azure/Entra

Add user to Azure AD Application

Azure applications are used for Single Sign On, among other things. To use SSO, the user has to have access to the application.

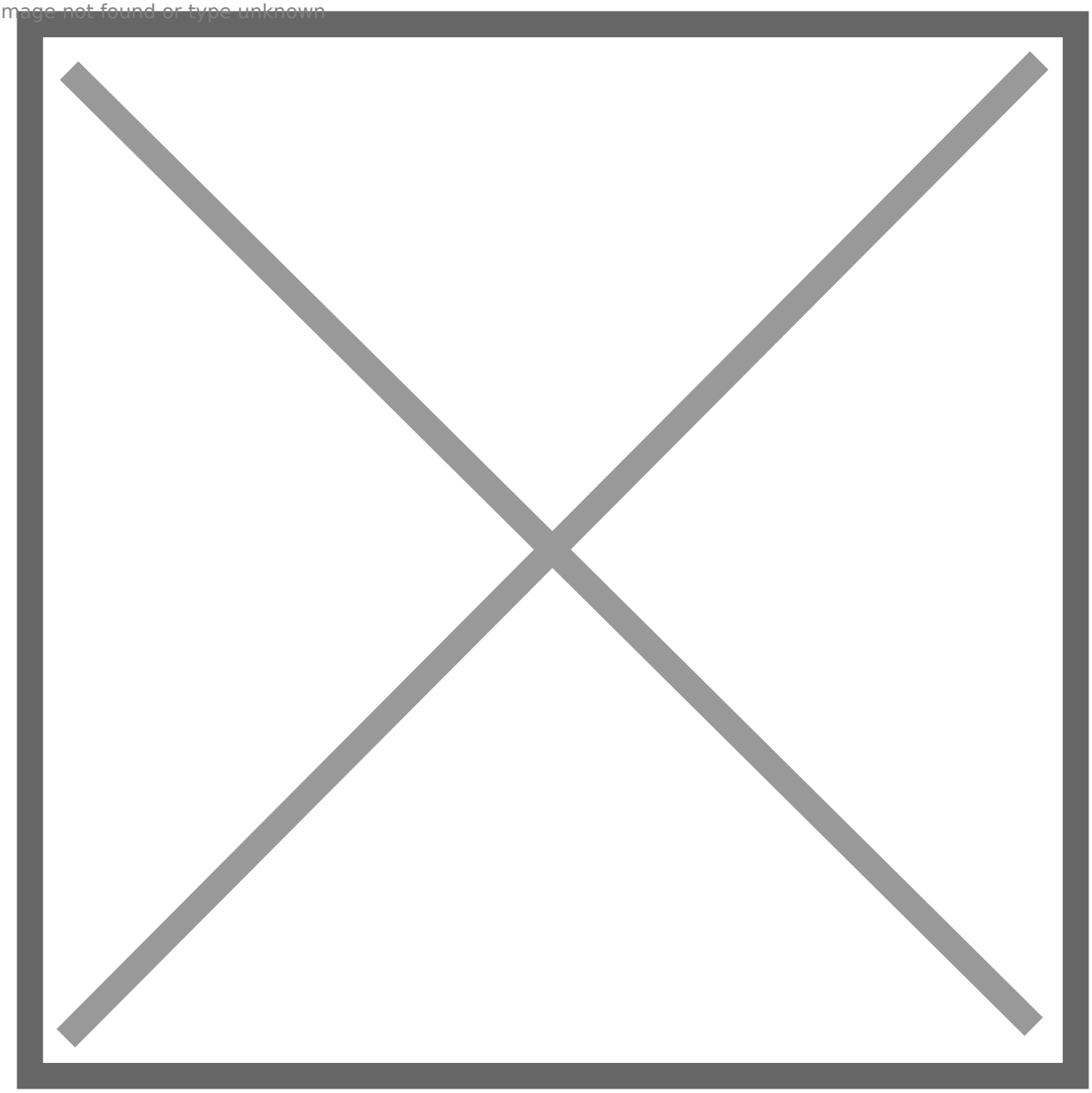
First, login to the Microsoft Admin Portal then go to Azure Active Directory (or skip this step and go directly to Azure Active Directory).

Image not found or type unknown



Go to Enterprise Applications > All Applications and search for the application. Then select it from the list.

Image not found or type unknown



Select ***Assign users and groups***. Then click ***Add users/group***.

Image not found or type unknown

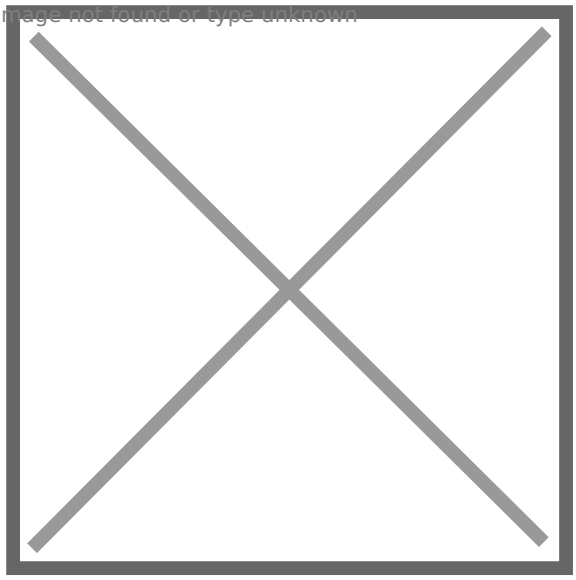
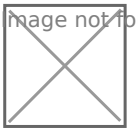
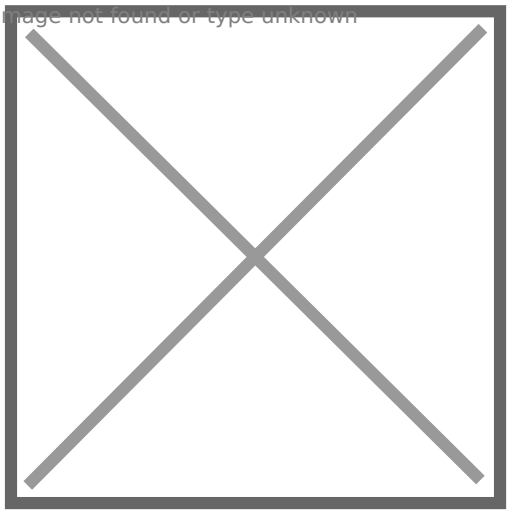


Image not found or type unknown



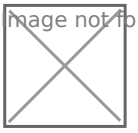
In Add Assignment click **None Selected** under Users and Groups.

Image not found or type unknown



Search for the user, then select from the list. Then click the **Select** button.

Image not found or type unknown



Then click the **Assign** button. The status box will pop up to show progress. Once it shows it's complete, the user has been assigned to the application.

Image not found or type unknown

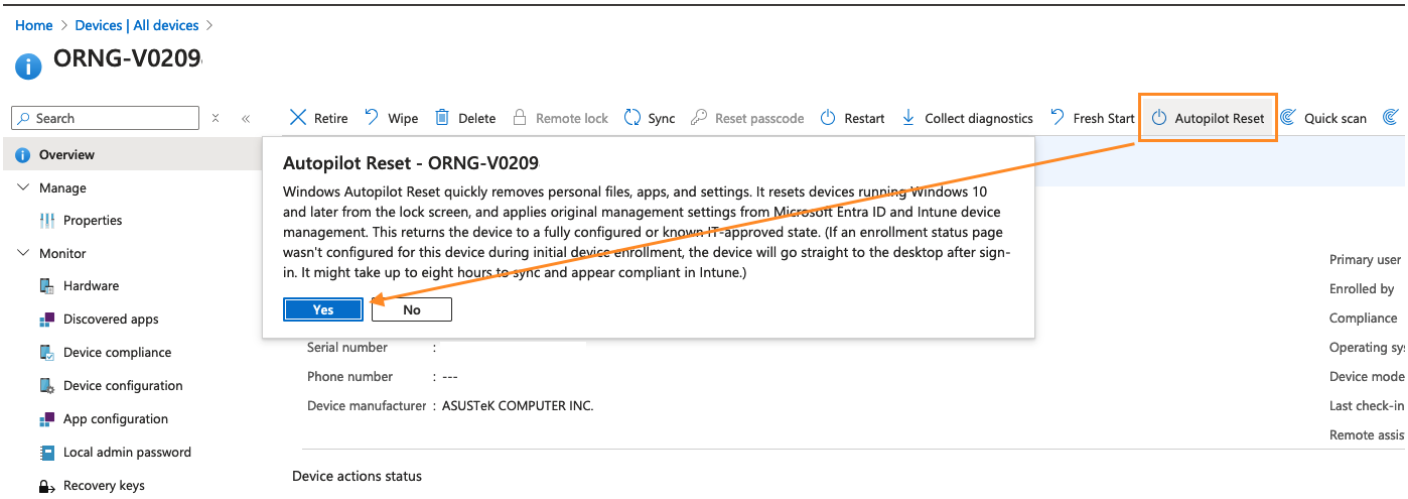
Intune

Reset a Windows Device

Prepare Device for Reprovisioning

Navigate to the Intune Admin Portal https://intune.microsoft.com/ > Devices > All Devices and select the device.

Select `Autopilot Reset` and then confirm.

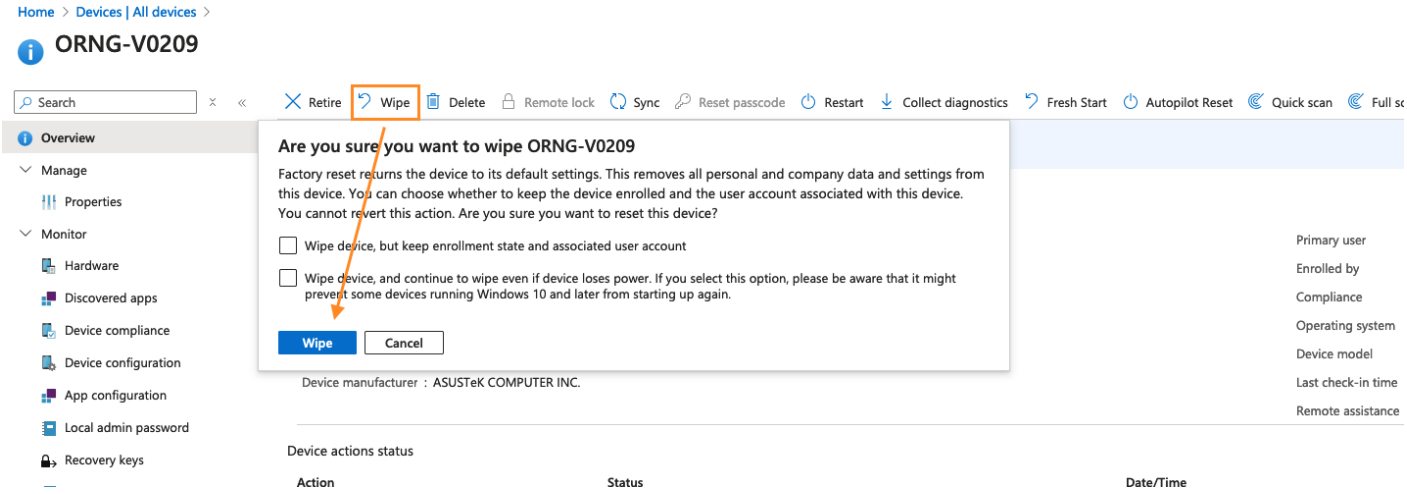


This will return the device an IT approved state and make it ready for a new user.

Prepare Device for Deprovisioning

To factory reset the device, navigate to the Intune Admin Portal https://intune.microsoft.com/ > Devices > All Devices and select the device.

Click `Wipe` and confirm.



This will return the device the factory state and make it ready for disposal.

Sharepoint

Sharepoint

Share content with external users

To share a Sharepoint folder with an external user, first select the folder and then click **Share.**

Image not found or type unknown

Select the type of sharing by clicking the **People in...** link and then change it to **Specific People**.

Image not found or type unknown

Select **Specific People**. Optionally, check the box to allow editing.

Image not found or type unknown

Type in the email address of the external user(s) to share with. Then click **Send**.

Image not found or type unknown

Then it will confirm that it was successful.

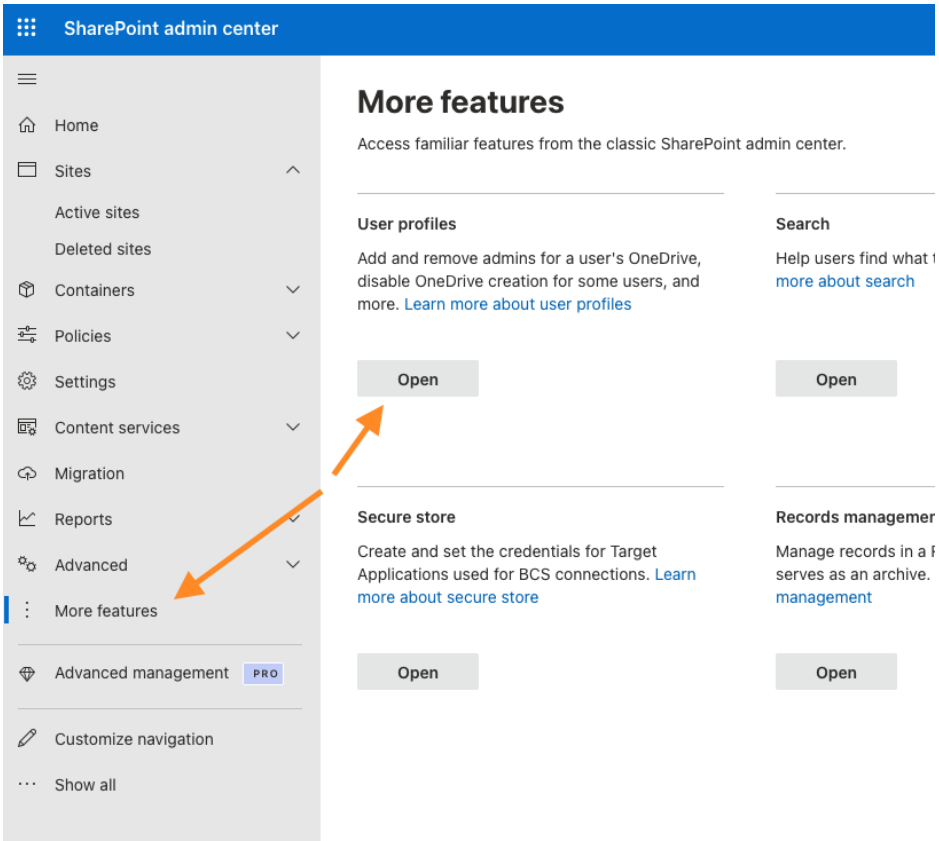
Image not found or type unknown

Sharepoint

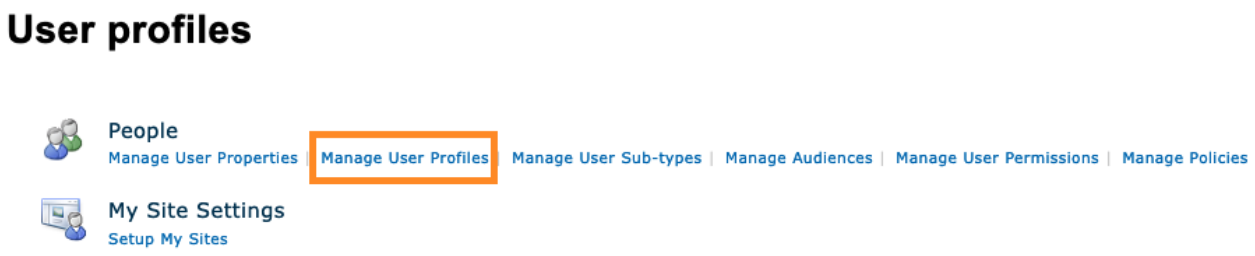
Manage OneDrive Profiles

To get OneDrive Profiles for licensed users or users that were previously licensed, go to the Sharepoint Admin center. You can grant a user access to another user's OneDrive files. This is useful for the successor of a departed employee.

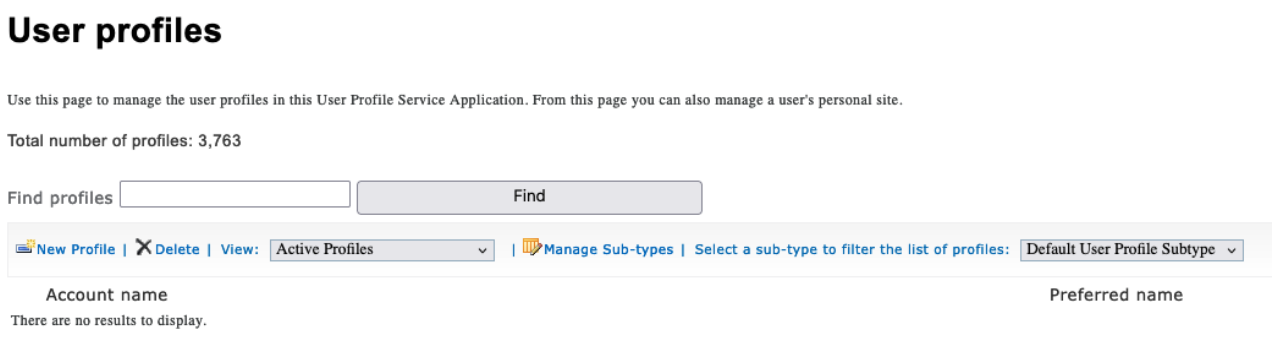
In the Sharepoint Admin Center, click **More Features**. Under **User profiles**, click **Open**.



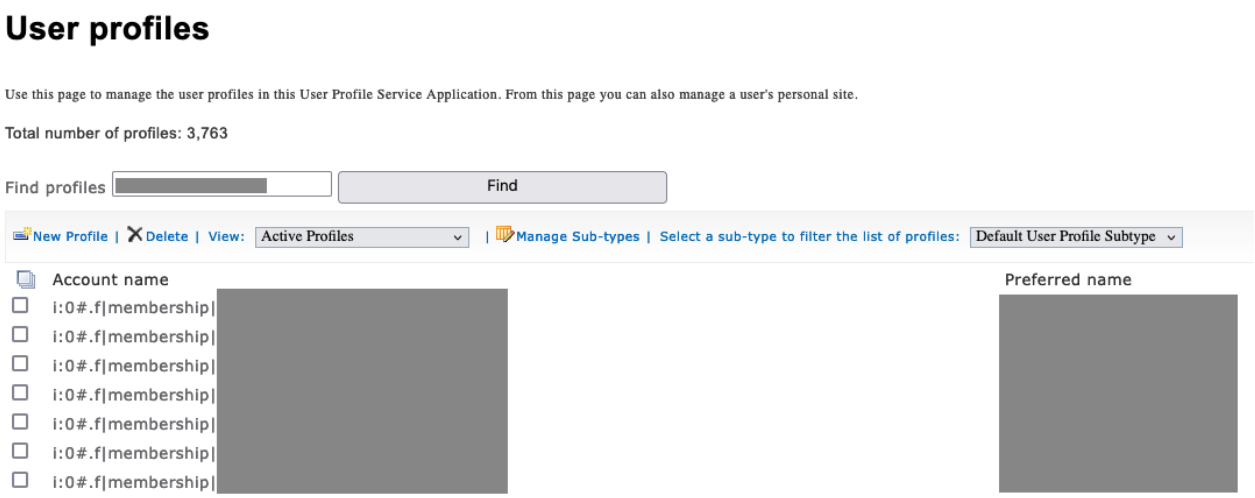
Click **Manage User Profiles**.



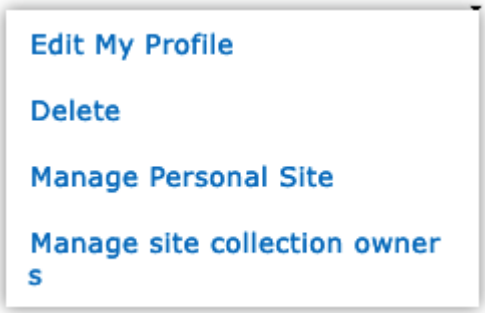
In the search box, type the name of the user and click **Find**.



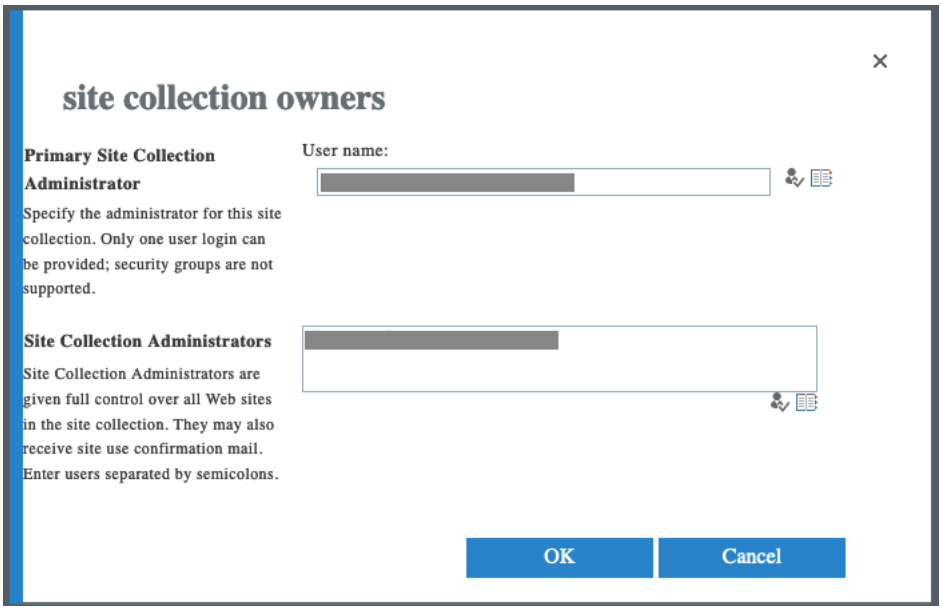
In the search results, click the profile you want to manage.



A menu pops open; click **Manage site collection owner**.



In the **Site Collection Administrators** box, type the name of an administrator to add, or choose from the list. Then click **OK**.



The account that was granted access can access the files by going to the OneDrive URL of that specific account. In the example below, replace `<tenantname>` with the Tenant name and `user_name_example_com` with the account's email address, replacing the @, periods and dashes with underscores.

`https://<tenantname>-my.sharepoint.com/personal/user_name_example_com/`

Security and Compliance

Outlook

Outlook on the Web

Outlook

Change filter settings in Outlook on the Web

Change filter settings in Office365 Outlook on the Web

Login to your account at https://outlook.office.com

1. Click the gear icon on the top right of the page.
   - Image not found or type unknown
2. Click **Mail** in the right column toward the bottom.
   - Image not found or type unknown
3. In the left column of the Mail settings, click **Block or Allow**.
   - Image not found or type unknown
4. Add acceptable email addresses to the **Safe Senders** list.
   - Image not found or type unknown
5. Add unacceptable email address to the **Blocked** list.
   - Image not found or type unknown
6. Once you are done with your changes, click **Save** at the top of the page.
   - Image not found or type unknown

Alternatively, you could allow all senders to be delivered to the inbox by selecting **Don't move email to my Junk Email folder** and click **Save**.

Outlook

Send as a Group in Outlook

To send a message as a group or shared mailbox from your own account, first the admin has to grant **Send-As** permissions for your account on the target group.

In Outlook, start a new message. By default, the **From** address is not shown. First, you need to **Show From**.

On the **Options** tab, select the **three dots** on the right side. Under **Show Fields**, choose **From**.

Image not found or type unknown

Your account email address will show in the from box. Drop-down the From menu and select **Other Email Address**.

Image not found or type unknown

Type the group or shared mailbox email address to send from. Then click **OK**. If you don't know the email address, you can click the **From button** and find the address in the directory.

Image not found or type unknown

Once you have sent from a group or shared mailbox, when you drop-down the from list, the recently used email addresses will be in the list.

Outlook

Setup Microsoft 365 Account

The first time you sign-in to your account on Microsoft 365, there are some account setup tasks to be done.

office.com

To get started, first go to office.com and click **Sign in**.

Image not found or type unknown

Enter your **username** (your username is in the form of an email address). Click **Next** and then enter your **Password**.

Image not found or type unknown

Change Password

After successful login, you will be prompted to change your password. Enter your temporary password first, then choose a password that is complex.

Image not found or type unknown

Multi-Factor Authentication

After updating your password, you will need to setup **Multi-Factor Authentication (MFA)**. Click **Next**.

Image not found or type unknown

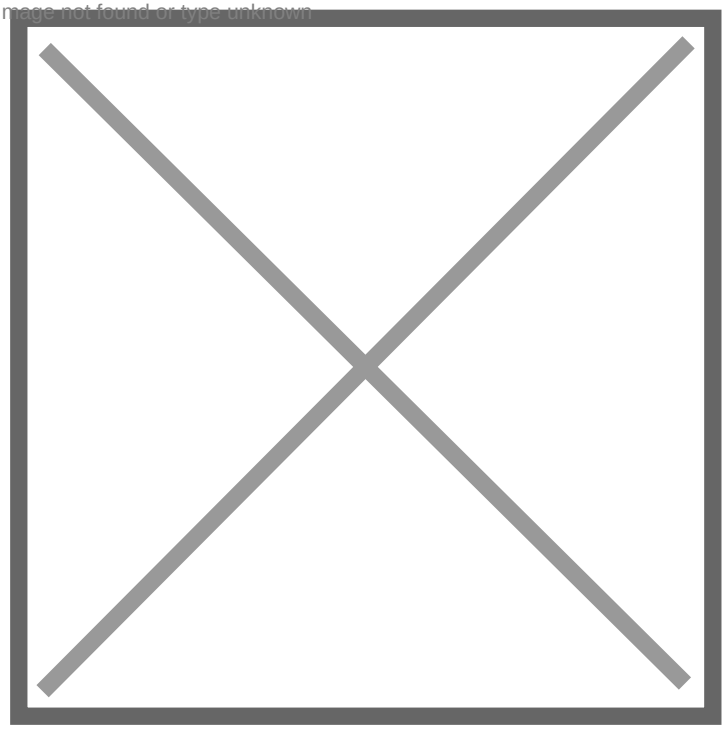
Mobile App

You will need to download the **Microsoft Authenticator** app.

Apple: https://apps.apple.com/us/app/microsoft-authenticator/id983156458

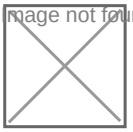
Android: https://play.google.com/store/apps/details?id=com.azure.authenticator&pli=1

Image not found or type unknown



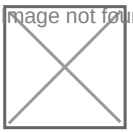
Back to your account setup, click **Next** to start the authenticator enrollment.

Image not found or type unknown



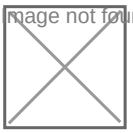
Click **Next**.

Image not found or type unknown



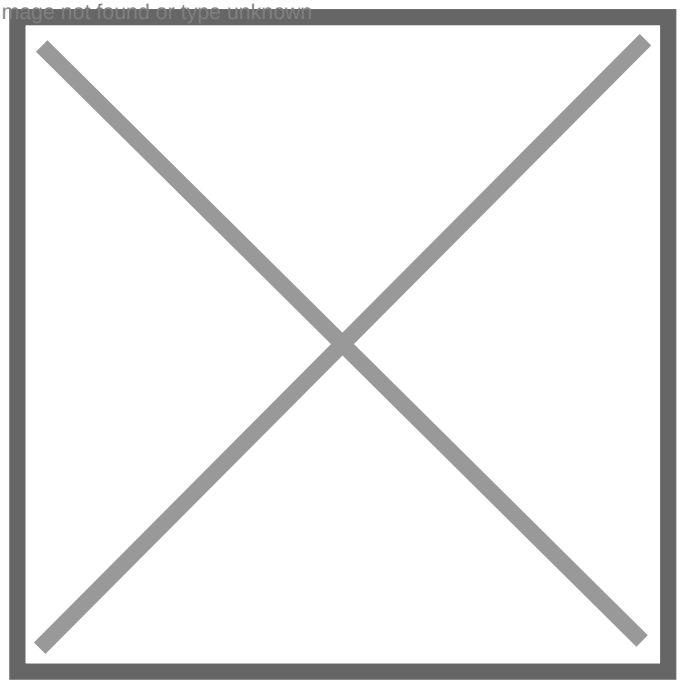
You should see a QR code that looks like a pixelated square.

Image not found or type unknown



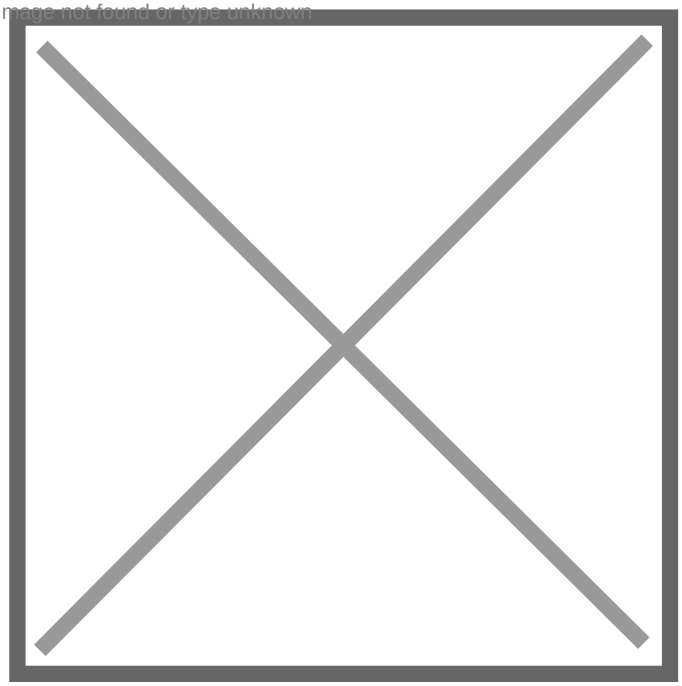
On the Authenticator app, click the plus +, or click **Sign-In** or **Add Account**.

Image not found or type unknown



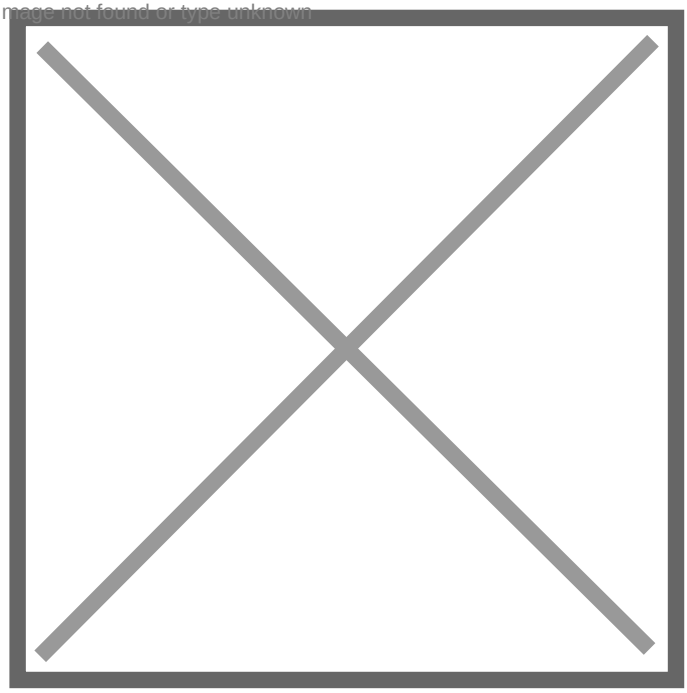
Choose the **Work or school account** option.

Image not found or type unknown



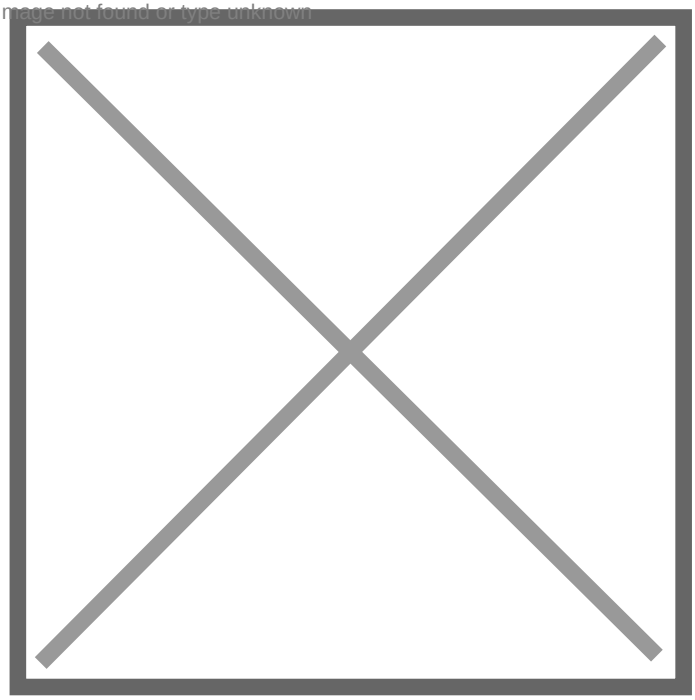
Choose **Scan QR code**. You will be asked to grant the app permission to use the camera. Click **Yes** or **Allow**. You can disable camera access after the enrollment process.

Image not found or type unknown



Scan the QR code with your smartphone's camera.

Image not found or type unknown



Once the code has been scanned, the account is added. Click **Next**. Your authenticator app on your smartphone will receive a notification to allow the sign-in. Click **Allow** and then enter the number shown on your screen and press **Yes**.

Image not found or type unknown

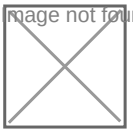
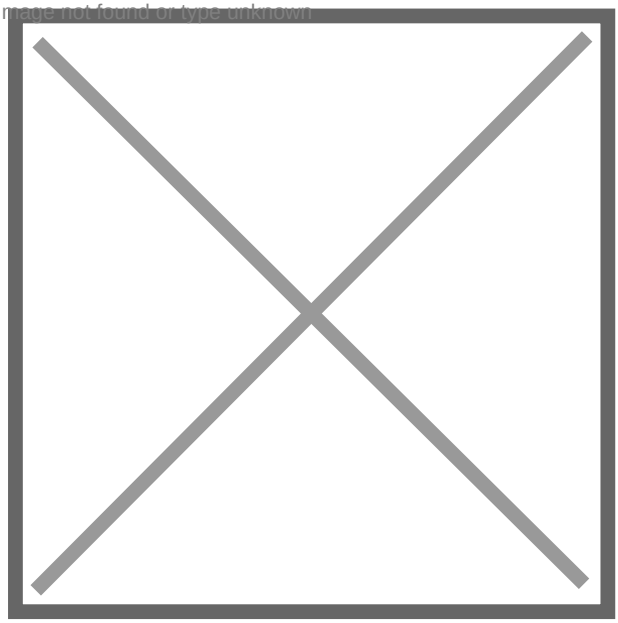
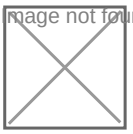


Image not found or type unknown



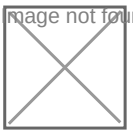
After you have approved the sign-in, a confirmation will be displayed on the screen. Click **Next**.

Image not found or type unknown



Your authenticator app has been enrolled. Click **Done**.

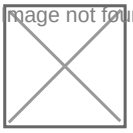
Image not found or type unknown



Signed-In

Your sign-in and MFA enrollment has been completed. Click **Yes** to stay signed-in on this device. If you are using a public computer, choose **No**.

Image not found or type unknown



Finally, a **welcome - get started** message will be displayed. Click the right arrow on the screen to click through the tutorial and then click the check mark to close it.

Image not found or type unknown

You are now signed-in. At this point you can choose an application to open from the left hand shortcut menu or the waffle application launcher at the top left corner.

Image not found or type unknown