Microsoft 365 Exchange Online Administration

What is Exchange Online?

Exchange Online is Microsoft's **cloud-based email, calendar, and contacts service**. It's part of **Microsoft 365 (Office 365)** and provides organizations with enterprise-grade email without needing on-premises Exchange servers.

- Users get access to **mailboxes, shared mailboxes, calendars, contacts, and tasks**.
- It integrates with **Outlook (desktop and web), Teams, and SharePoint**.
- Microsoft handles the **infrastructure, updates, and security**, reducing IT overhead.

Key Features of Exchange Online

A. Email and Mailboxes

- Enterprise-class email with custom domains.

- Mailbox sizes:
    - **Plan 1 / E1:** 50 GB per user
    - **Plan 2 / E3/E5:** 100 GB per user, plus auto-expanding archive
- Shared mailboxes for teams or departments.
- Alias emails and multiple addresses per mailbox.

B. Calendars and Scheduling

- Shared calendars for team coordination.
- Scheduling assistant to find free/busy times across users.
- Room & equipment mailboxes for booking conference rooms or devices.

C. Compliance & Security

- Anti-spam and anti-malware protection.
- Data Loss Prevention (DLP) policies to prevent sensitive data leaks.
- Litigation hold & In-Place hold for legal compliance.
- Archiving and retention policies for long-term data management.
- Advanced Threat Protection (ATP) in E5 for malware, phishing, and Safe Links.

D. Mail Flow and Transport Rules

- Rules to redirect, block, or add disclaimers to emails.
- Automatic forwarding control.
- Message trace for troubleshooting email delivery issues.

E. Integration

- Works seamlessly with **Microsoft Teams, SharePoint, OneDrive, and Outlook**.
- Supports **mobile access** (iOS, Android) and web access (OWA).

Licensing Overview

Exchange Online can be licensed:

- **Standalone Exchange Online Plans:** Plan 1 (basic) or Plan 2 (enterprise).
- **Included in Microsoft 365 Suites:**
    - Business Basic / Standard / Premium
    - Office 365 E1 / E3 / E5
    - Microsoft 365 E3 / E5

Key differences:

- Plan 1 / E1: 50 GB mailbox, basic email and web access.
- Plan 2 / E3: 100 GB mailbox, compliance features, DLP, litigation hold, archiving.
- E5: Adds advanced security like ATP and auditing.

1. Standalone Exchange Online Licenses

License	Mailbox Size	Archive	DLP / Compliance	Outlook Web Access	Hosted Voicemail	Use Case
Exchange Online Plan 1	50 GB	Optional (100 GB)	❌	✅	❌	Small business or standard email users

Exchange Online Plan 2	100 GB	Auto-expanding archive	✅	✅	✅	Enterprises needing compliance & archiving

2. **Microsoft 365 / Office 365 Suite Licenses Including Exchange Online**

License	Plan	Mailbox	DLP/Compliance	Archiving	Office Apps	Security	Use Case
Microsoft 365 Business Basic	1	50 GB	❌	Optional	Web & Mobile	Basic Anti-spam	Small businesses, email only
Microsoft 365 Business Standard	1	50 GB	❌	Optional	Desktop + Web	Basic Anti-spam	Small business with Office apps
Microsoft 365 Business Premium	1	50 GB	❌	Optional	Desktop + Web	Advanced Security + Intune	Small business with security
Office 365 E1	1	50 GB	❌	Optional	Web only	Basic security	Enterprise web-only users

Office 365 E3	2	100 GB	✅	Auto-expanding	Desktop + Web	DLP, retention, litigation hold	Enterprises needing compliance
Office 365 E5	2	100 GB	✅	Auto-expanding	Desktop + Web	Advanced Security (ATP, Safe Links/Attachments)	Enterprises needing advanced security
Microsoft 365 E3	2	100 GB	✅	Auto-expanding	Desktop + Web	Compliance + Security	Enterprise productivity & compliance
Microsoft 365 E5	2	100 GB	✅	Auto-expanding	Desktop + Web	Compliance + Advanced Security + Analytics	Full-featured enterprise package

---

1. Create a Microsoft 365 E3 Trial Account

✅ Purpose

- Set up a Microsoft 365 tenant for **testing, training, or proof of concept**.
- Provides a sandbox environment without impacting production.

✅ Configuration Steps

Portal

1. Go to Microsoft 365 E3 Trial.
2. Click **Start Free Trial** → enter business email.
3. Create tenant domain (e.g., `contoso.onmicrosoft.com`).
4. Create the **first Global Admin** account.
5. Verify phone/email → finish signup.

PowerShell (after tenant created)

```
# Connect to Microsoft Online
Connect-MsolService

# View available licenses
Get-MsolAccountSku
```

✅ **Validation**

- Login at https://admin.microsoft.com.
- Navigate to **Billing** → **Licenses** → Confirm **Microsoft 365 E3 Trial** listed.

✅ **Best Practices**

- Use a **non-production domain** for labs.
- Document Global Admin credentials.
- Enable **MFA** immediately.

✅ **Use Case**

- IT teams test **Exchange Online, Purview, Intune**.
- Pilot compliance/security policies before production rollout.

2. Create Exchange Online User Mailbox and Assign License

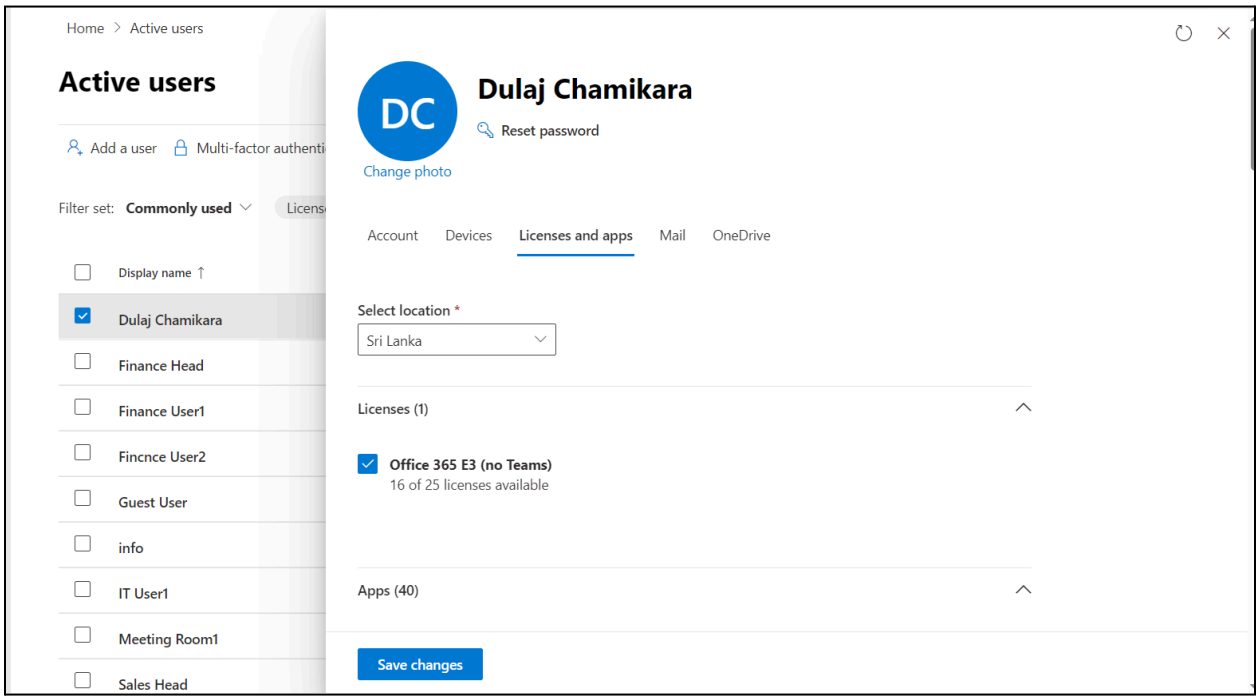
✅ Purpose

- Create new users in Microsoft 365 with mailboxes.
- Assign licenses for Exchange Online access.

✅ Configuration Steps

Portal

1. Microsoft 365 Admin Center → **Users** → **Active users** → **Add a user**.
2. Enter name, username, domain.
3. Assign **Microsoft 365 E3/E5** license.
4. Ensure **Exchange Online** service enabled.



PowerShell

```
# Connect to MSOnline
Connect-MsolService

# Create new user
New-MsolUser -UserPrincipalName user1@contoso.com -DisplayName "User
One" -FirstName User -LastName One -UsageLocation US
-LicenseAssignment contoso:ENTERPRISEPACK
```

✅ **Validation**

- Login as user → access **Outlook on the Web** (https://outlook.office.com).
- Send/receive test email.

✅ **Best Practices**

- Always set **Usage Location** before assigning licenses.
- Automate user creation with **PowerShell scripts** for bulk onboarding.

✅ **Use Case**

- Onboarding new employees with mailbox & Teams access on Day 1.

---

3. Create Office 365 User Account without License in Exchange Online

✅ **Purpose**

- Create accounts for **contractors, staging, or future employees** without consuming licenses.

✅ **Configuration Steps**

Portal

1. Admin Center → **Users** → **Active users** → **Add a user**.

2. Enter details → **Do not assign a license**.

PowerShell

```
New-MsolUser -UserPrincipalName user2@contoso.com -DisplayName "User Two" -FirstName User -LastName Two -UsageLocation US
```

✅ **Validation**

- User appears under **Active Users**.
- No mailbox created (check **Exchange Admin Center** → Mailboxes).

✅ **Best Practices**

- Use for **service accounts** or pre-provisioning.
- Assign license later when mailbox/app access is required.

✅ **Use Case**

- HR creates accounts early, IT assigns licenses on employee start date.

---

4. Assign or Remove License to Microsoft 365 User Account

✅ **Purpose**

- Manage Microsoft 365 subscriptions for users dynamically.
- Enable/disable Exchange Online, Teams, OneDrive, etc.

✅ **Configuration Steps**

Portal

1. Admin Center → **Users** → **Active users**.
2. Select user → **Licenses and apps**.
3. Assign/remove **Microsoft 365 E3/E5**.

PowerShell

```
# Assign License
Set-MsolUserLicense -UserPrincipalName user2@contoso.com -AddLicenses
contoso:ENTERPRISEPACK

# Remove License
Set-MsolUserLicense -UserPrincipalName user2@contoso.com
-RemoveLicenses contoso:ENTERPRISEPACK
```

✅ **Validation**

- User mailbox is provisioned (assign).
- User mailbox removed (remove license).

✅ **Best Practices**

- Use **Azure AD Group-based licensing** for automation.
- Regularly audit unused licenses to reduce cost.

✅ **Use Case**

- Temporary employees: assign license only for project duration.

---

5. How to Reset User Password in Exchange Online

✅ **Purpose**

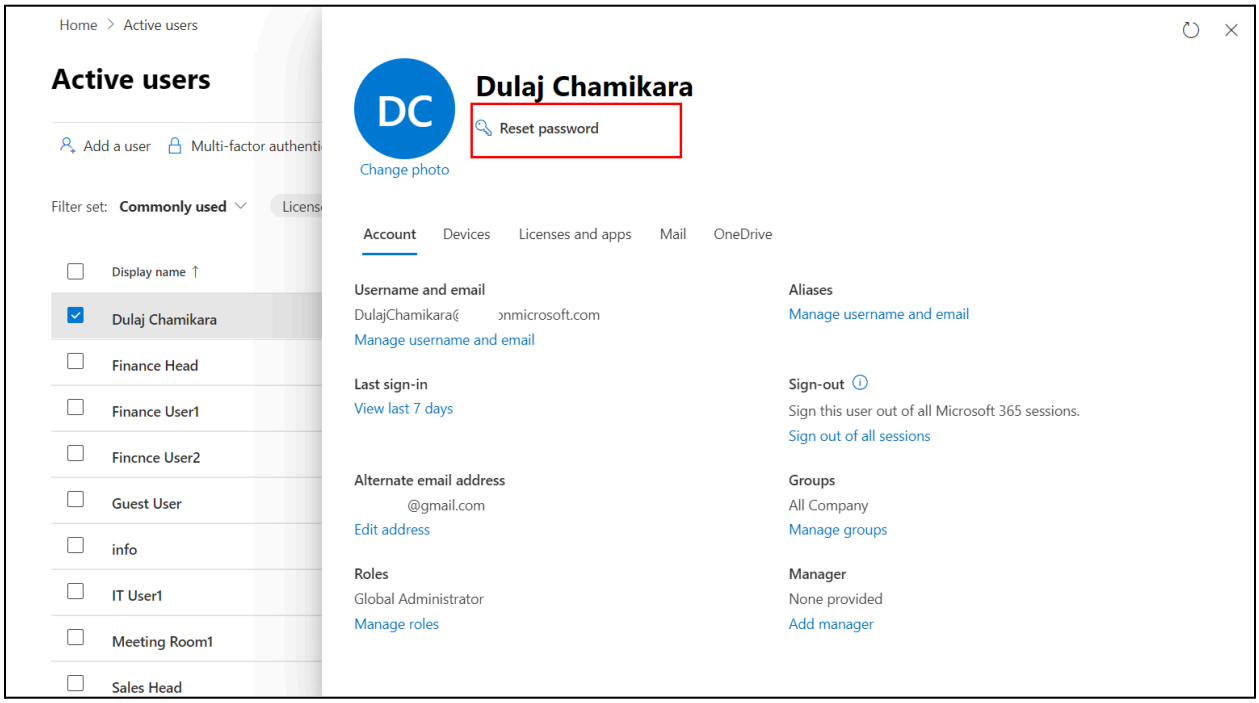
- Reset forgotten or compromised passwords for users.

- Maintain security & business continuity.

✅ Configuration Steps

Portal

1. Admin Center → **Users** → **Active users**.
2. Select user → **Reset password**.
3. Auto-generate or set custom password.
4. Choose “Require user to change password at next sign-in.”



PowerShell

```
Set-MsolUserPassword -UserPrincipalName user2@contoso.com -NewPassword "TempPassw0rd!" -ForceChangePassword $true
```

✅ Validation

- The user signs in with a new password.

- Must change password on first login (if forced).

✅ **Best Practices**

- Always enforce **MFA** after reset.
- Encourage **self-service password reset (SSPR)** for users.

✅ **Use Case**

- Helpdesk resets passwords for users locked out of accounts.
- Security team resets credentials after suspected compromise.

---

6. Add an Alias Email Address for a Mailbox

✅ **Purpose**

- An **alias** is an additional email address for a user mailbox.
- Useful when a user needs multiple addresses (e.g., `sales@contoso.com`, `info@contoso.com`) but **doesn't need a separate mailbox**.
- All emails sent to alias addresses are delivered to the **primary mailbox**.

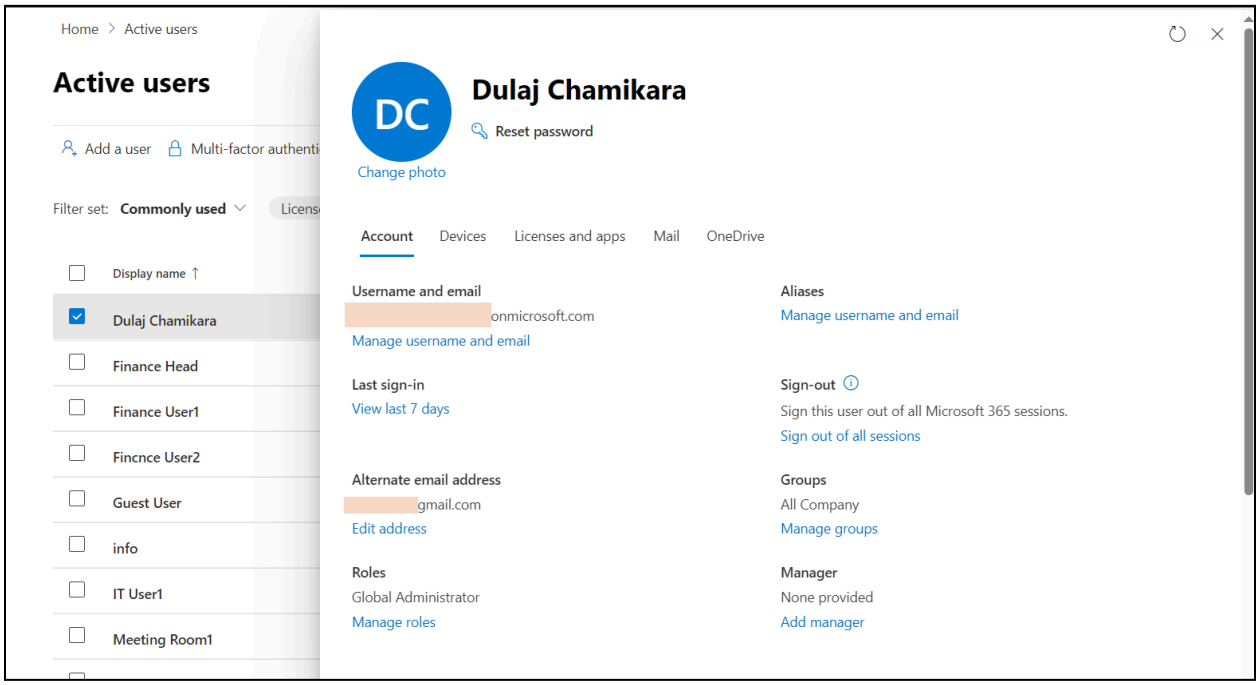
✅ **Configuration Steps**

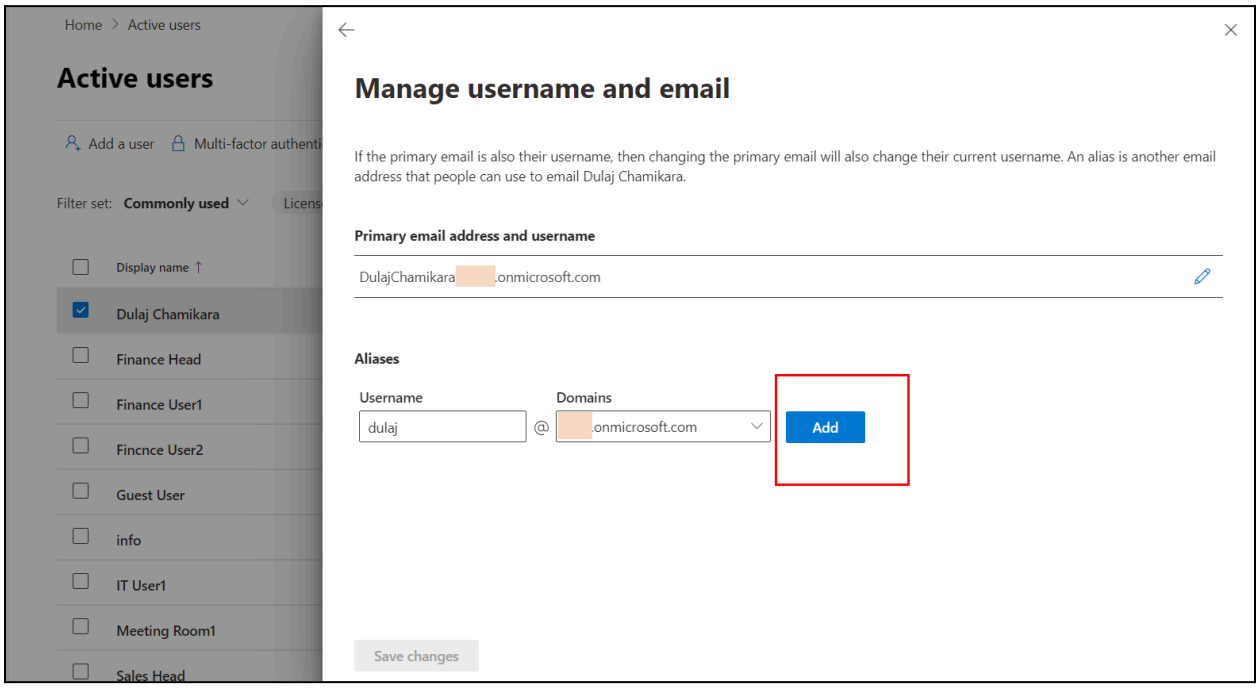
Portal (Microsoft 365 Admin Center)

1. Go to **https://admin.microsoft.com** → Sign in as Global/Exchange Admin.
2. Navigate → **Users** → **Active Users**.
3. Select the user → **Mail** → **Manage email aliases**.
4. Click **Add alias** → enter new email (e.g., `sales@contoso.com`).

5. Choose the domain (e.g., `contoso.com`).

6. Save → alias added immediately





Exchange Admin Center (EAC)

1. Go to **https://admin.exchange.microsoft.com**.
2. Navigate → **Recipients** → **Mailboxes**.
3. Select the mailbox → **Email addresses**.
4. Click **Add email address** → Choose **SMTP**.
5. Enter alias (e.g., `support@contoso.com`) → Save.

PowerShell (Exchange Online)

```
# Connect to Exchange Online
Connect-ExchangeOnline

# Add Alias (SMTP Address)
Set-Mailbox user1@contoso.com -EmailAddresses
@{Add="sales@contoso.com"}

# View all addresses
Get-Mailbox user1@contoso.com | Select-Object -ExpandProperty
EmailAddresses
```

✅ **Validation**

- Send a test email to alias (e.g., `sales@contoso.com`).
- Confirm email is delivered to **User1's primary mailbox**.
- Check via **OWA** or Outlook.

✅ **Best Practices**

- Use aliases instead of creating extra mailboxes to **reduce license costs**.
- Use a **naming convention** (e.g., `role@contoso.com` or `location@contoso.com`).

- Avoid using aliases for **shared functions** where multiple users need access (use **Shared Mailbox** instead).

✅ Use Case

- A **sales manager** has the primary mailbox `john@contoso.com`.
- Company wants him to also receive emails sent to `sales@contoso.com` and `info@contoso.com`.
- Instead of creating multiple mailboxes, add aliases → all emails flow into **one inbox**.

---

7. Configure Email Forwarding for a Mailbox

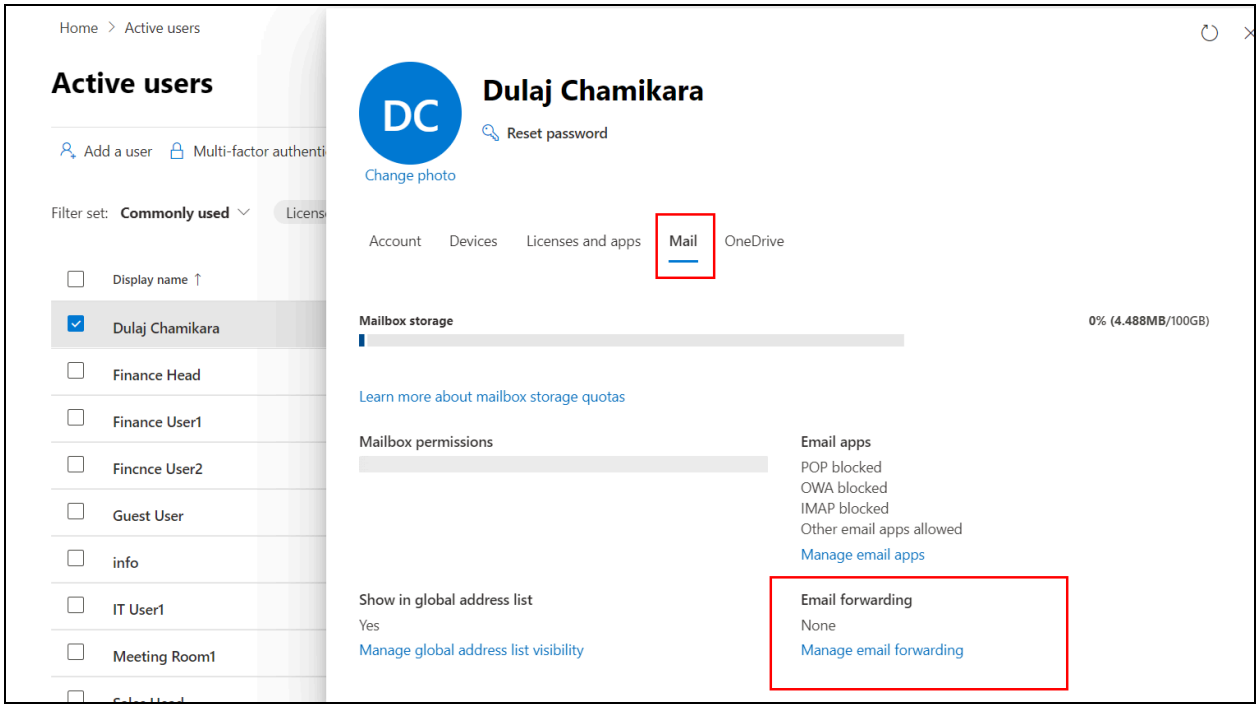
✅ Purpose

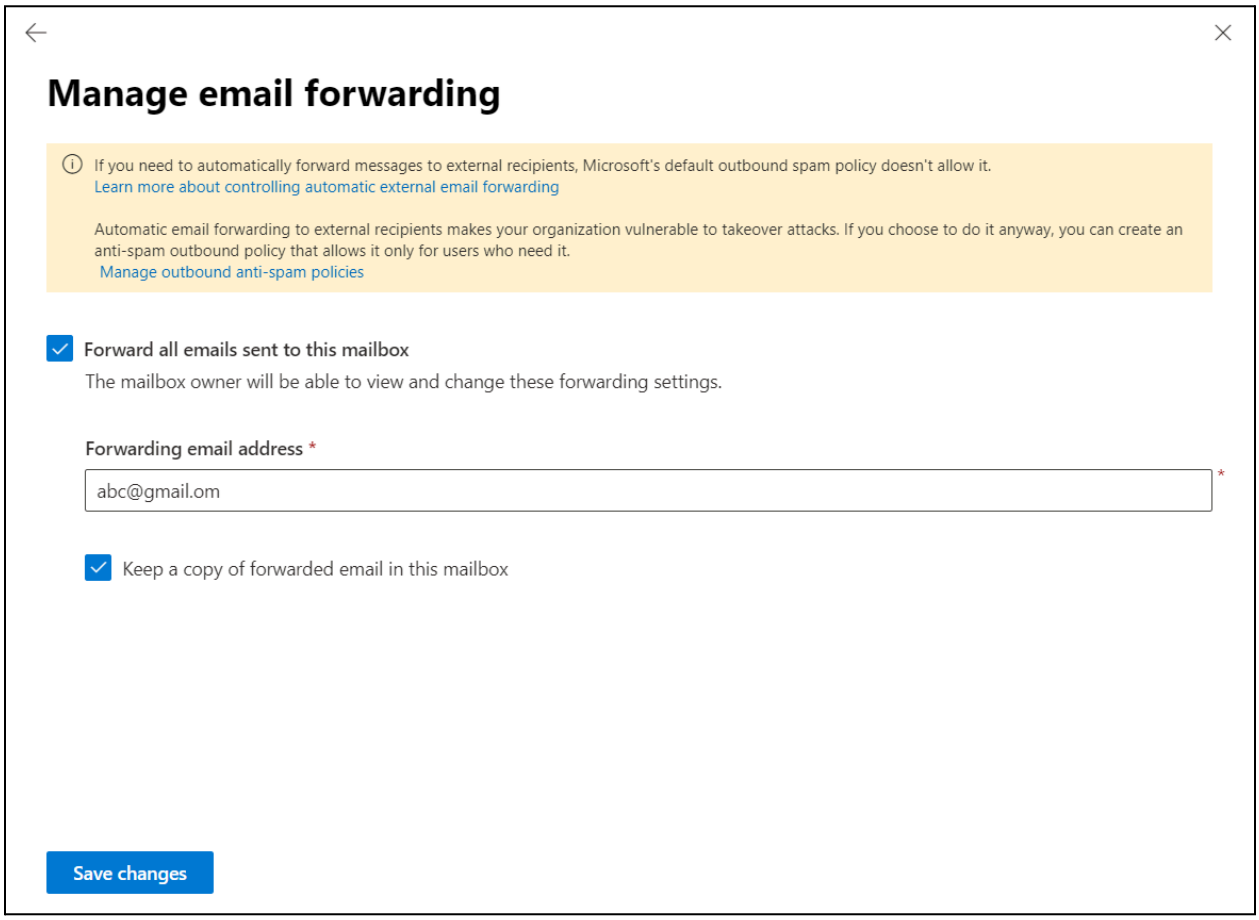
- Email forwarding automatically redirects incoming emails from one mailbox to another.
- Useful when an employee leaves the company, is on extended leave, or when centralizing communication in a shared mailbox.

✅ Configuration Steps

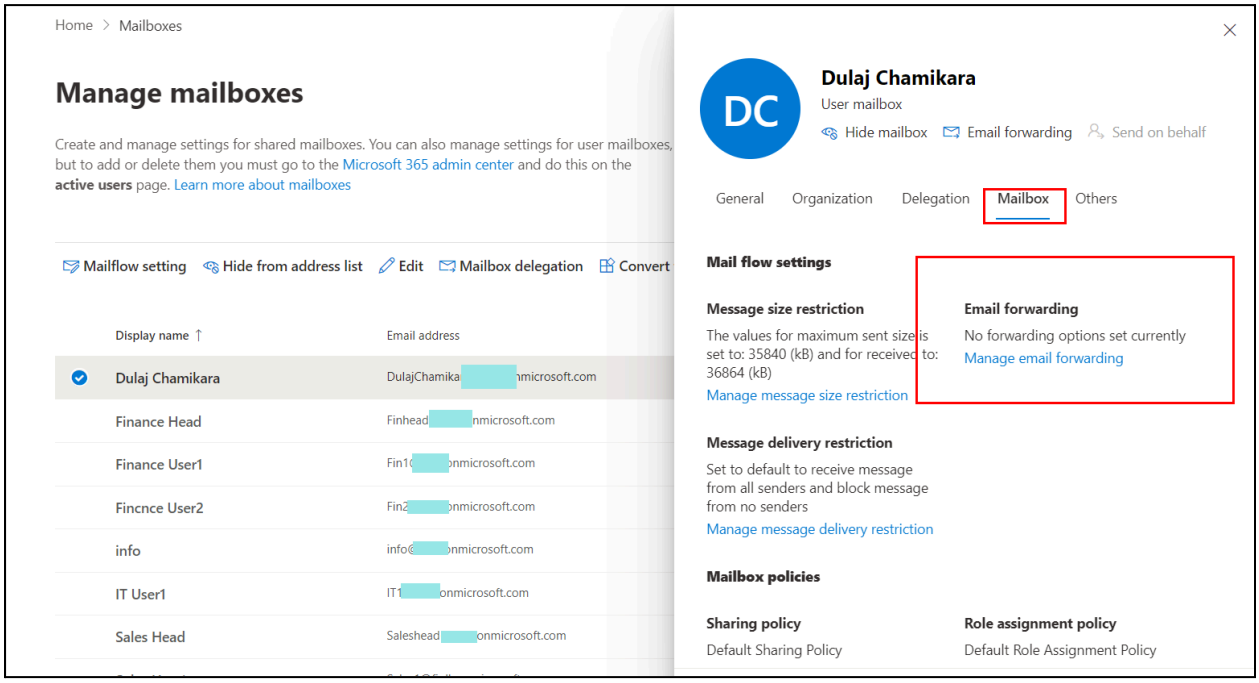
Portal (Microsoft 365 Admin Center)

1. Go to **https://admin.microsoft.com** → Sign in as Global/Exchange Admin.
2. Navigate → **Users** → **Active Users**.
3. Select the user → **Mail** → **Manage email forwarding**.
4. Enable **Forward all emails sent to this mailbox**.
5. Enter the forwarding address (e.g., `manager@contoso.com`).
6. (Optional) Check **Keep a copy of forwarded email** → user keeps emails too.
7. Save changes.


Home > Active users
Active users
Add a user
Multi-factor authenti
Filter set: Commonly used
Display name
Dulaj Chamikara
Finance Head
Finance User1
Fincnce User2
Guest User
info
IT User1
Meeting Room1
DC
Change photo
Dulaj Chamikara
Reset password
Account
Devices
Licenses and apps
Mail
OneDrive
Mailbox storage
0% (4.488MB/100GB)
Learn more about mailbox storage quotas
Mailbox permissions
Email apps
POP blocked
OWA blocked
IMAP blocked
Other email apps allowed
Manage email apps
Show in global address list
Yes
Manage global address list visibility
Email forwarding
None
Manage email forwarding


Manage email forwarding
If you need to automatically forward messages to external recipients, Microsoft's default outbound spam policy doesn't allow it.
Learn more about controlling automatic external email forwarding
Automatic email forwarding to external recipients makes your organization vulnerable to takeover attacks. If you choose to do it anyway, you can create an anti-spam outbound policy that allows it only for users who need it.
Manage outbound anti-spam policies
Forward all emails sent to this mailbox
The mailbox owner will be able to view and change these forwarding settings.
Forwarding email address *
abc@gmail.om
Keep a copy of forwarded email in this mailbox
Save changes

Exchange Admin Center (EAC)

1. Go to **https://admin.exchange.microsoft.com**.
2. Navigate → **Recipients** → **Mailboxes**.
3. Select the mailbox → **Manage email forwarding**.
4. Enter destination mailbox → Save.
5. 

PowerShell (Exchange Online)

```
# Connect to Exchange Online
Connect-ExchangeOnline

# Configure Forwarding (without keeping a copy)
Set-Mailbox user1@contoso.com -ForwardingSMTPAddress
"manager@contoso.com" -DeliverToMailboxAndForward $false

# Configure Forwarding (with keeping a copy in original mailbox)
Set-Mailbox user1@contoso.com -ForwardingSMTPAddress
"manager@contoso.com" -DeliverToMailboxAndForward $true

# View forwarding settings
```

```
Get-Mailbox user1@contoso.com | Select-Object
DisplayName,ForwardingSMTPAddress,DeliverToMailboxAndForward
```

✅ **Validation**

- Send a test email to the original user (e.g., `user1@contoso.com`).
- Confirm that it is forwarded to the destination (e.g., `manager@contoso.com`).
- If **DeliverToMailboxAndForward = $true**, check both mailboxes receive the email.

✅ **Best Practices**

- Always document **who has mail forwarding enabled** (for auditing & compliance).
- Use forwarding **temporarily**; for permanent shared access, consider **delegation or shared mailbox**.
- Avoid forwarding emails to **external addresses** unless explicitly approved by security/compliance teams.
- Regularly review forwarding rules using reports (`Get-Mailbox | Where { $_.ForwardingSMTPAddress -ne $null }`).

✅ **Use Case**

- An employee leaves the company but their mailbox is still receiving customer queries.
- Forward all emails from `john@contoso.com` to `sales@contoso.com` so no communication is lost.
- Optionally, keep a copy in John's mailbox for **archival or legal hold purposes**.

---

8. Configure Message Delivery Restrictions for a Mailbox

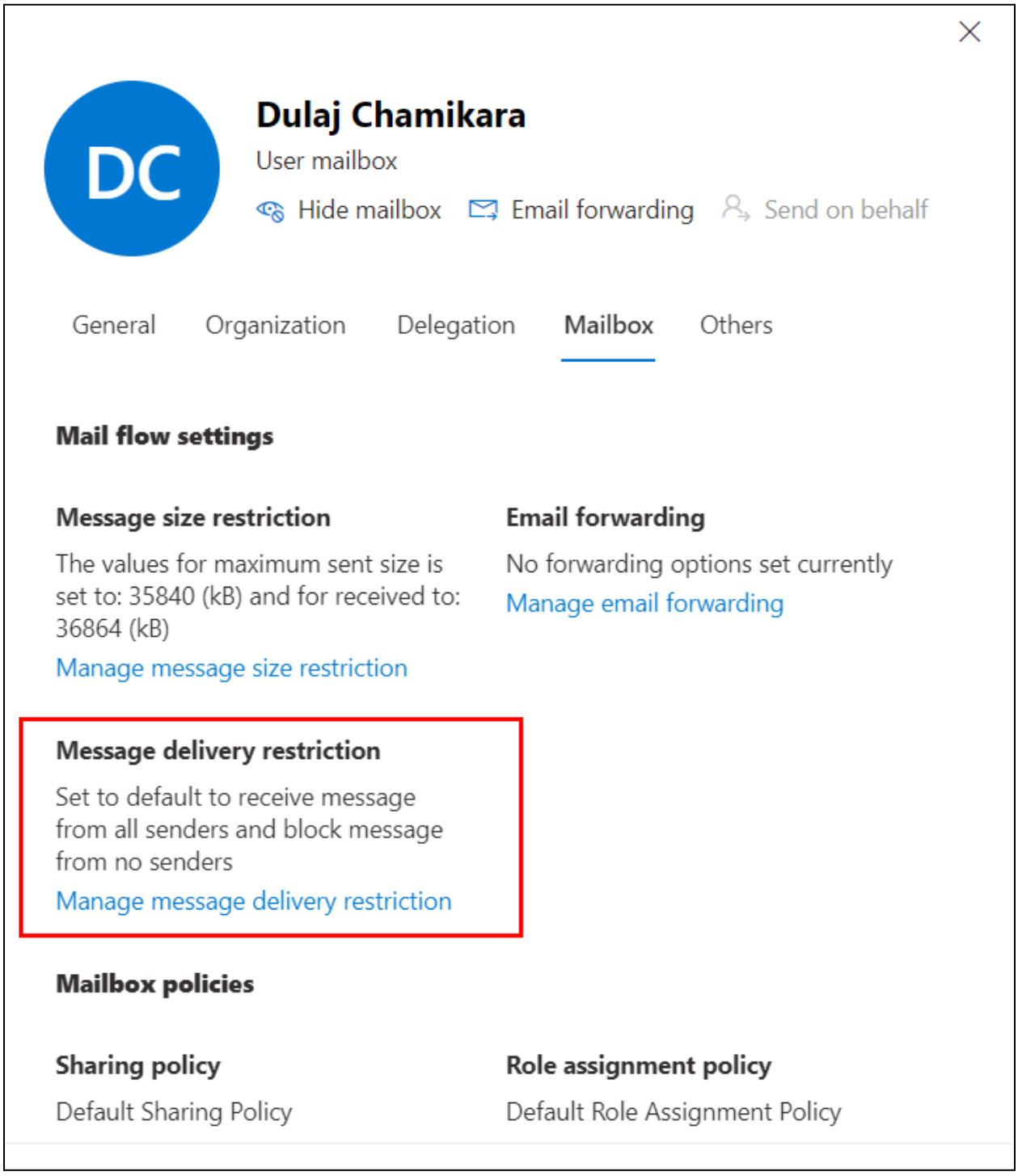
✅ **Purpose**

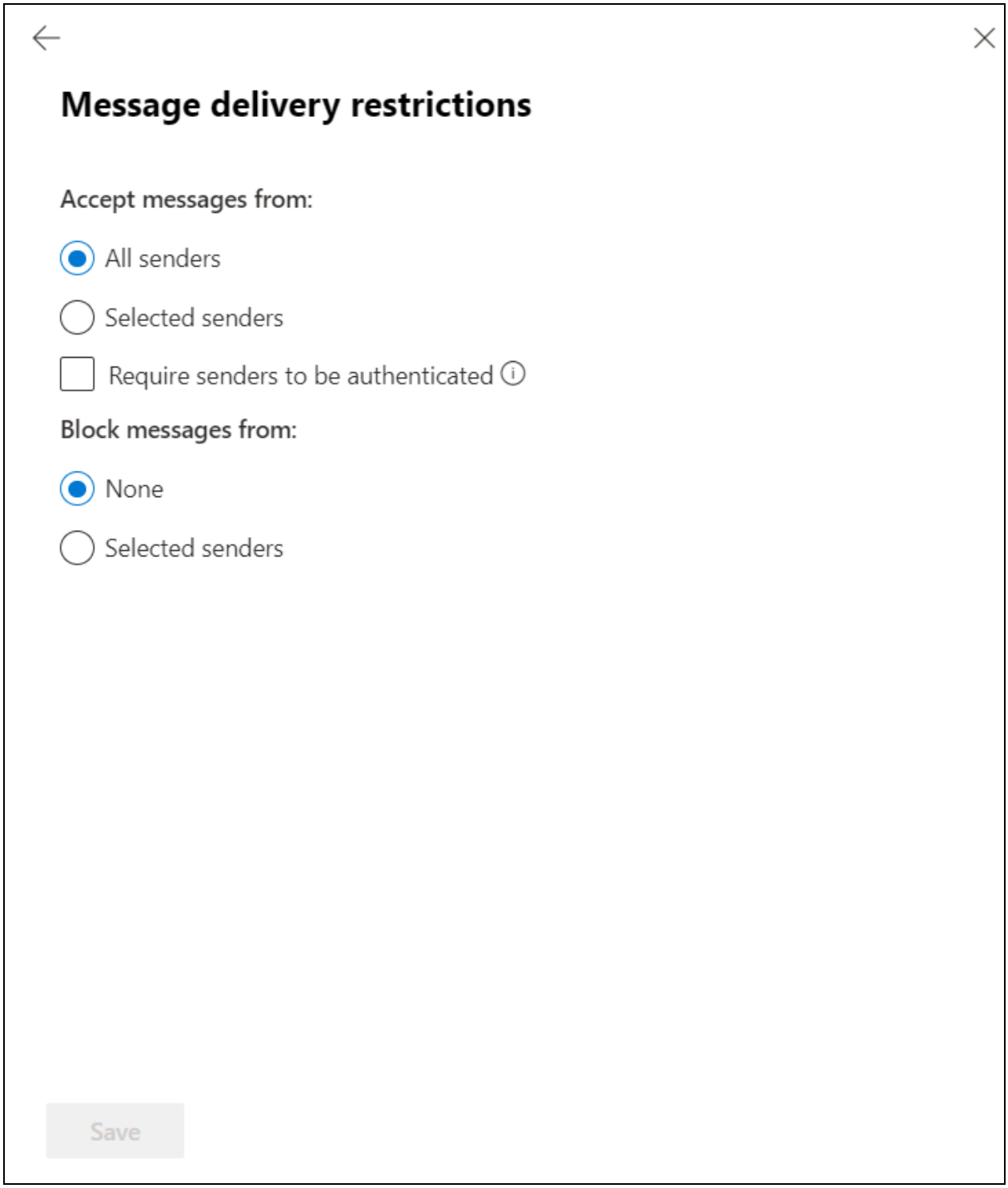
- Message delivery restrictions **control who can send emails** to a specific mailbox.
- Useful for high-profile mailboxes (e.g., CEO, HR, Finance) to prevent spam, internal misuse, or unwanted messages.
- Can restrict by:
    - **Internal only**
    - **Specific users or groups**
    - **Block external senders**

Exchange Admin Center (EAC)

1. Go to **https://admin.exchange.microsoft.com**.
2. Navigate → **Recipients** → **Mailboxes**.
3. Select mailbox → **Mail flow settings** → **Message delivery restrictions**.

4. Configure allow/block lists → Save.





PowerShell (Exchange Online)

```
# Connect to Exchange Online
Connect-ExchangeOnline
```

```
# Allow only specific users to send to this mailbox
Set-Mailbox ceo@contoso.com -AcceptMessagesOnlyFrom
user1@contoso.com,user2@contoso.com

# Allow only members of a group (e.g., Executives) to send to CEO
Set-Mailbox ceo@contoso.com -AcceptMessagesOnlyFromDLMembers
"Executives"

# Block specific senders
Set-Mailbox ceo@contoso.com -RejectMessagesFrom spammer@contoso.com

# Block a distribution group
Set-Mailbox ceo@contoso.com -RejectMessagesFromDLMembers
"ExternalVendors"
```

✅ **Validation**

- Send a test email from an **authorized user** → should be delivered.
- Send from a **non-authorized user** → should be rejected with a Non-Delivery Report (NDR).
- Check logs using:

```
Get-MessageTrace -Recipients ceo@contoso.com -StartDate
(Get-Date).AddHours(-1) -EndDate (Get-Date)
```

✅ **Best Practices**

- Use **security groups** instead of individual users for easier management.
- Apply restrictions to **executive, finance, HR, and sensitive mailboxes**.
- Combine with **anti-spam/anti-phishing policies** for maximum security.
- Regularly review restrictions to ensure correct access.

✅ **Use Case**

- The CEO's mailbox (`ceo@contoso.com`) should only receive emails from the Executives **group**.
- Prevents spam and accidental emails from all-staff distribution lists.
- Keeps inbox secure and **prioritizes critical communication**.

---

9. Configure Message Size Limits for a Mailbox

✅ Purpose

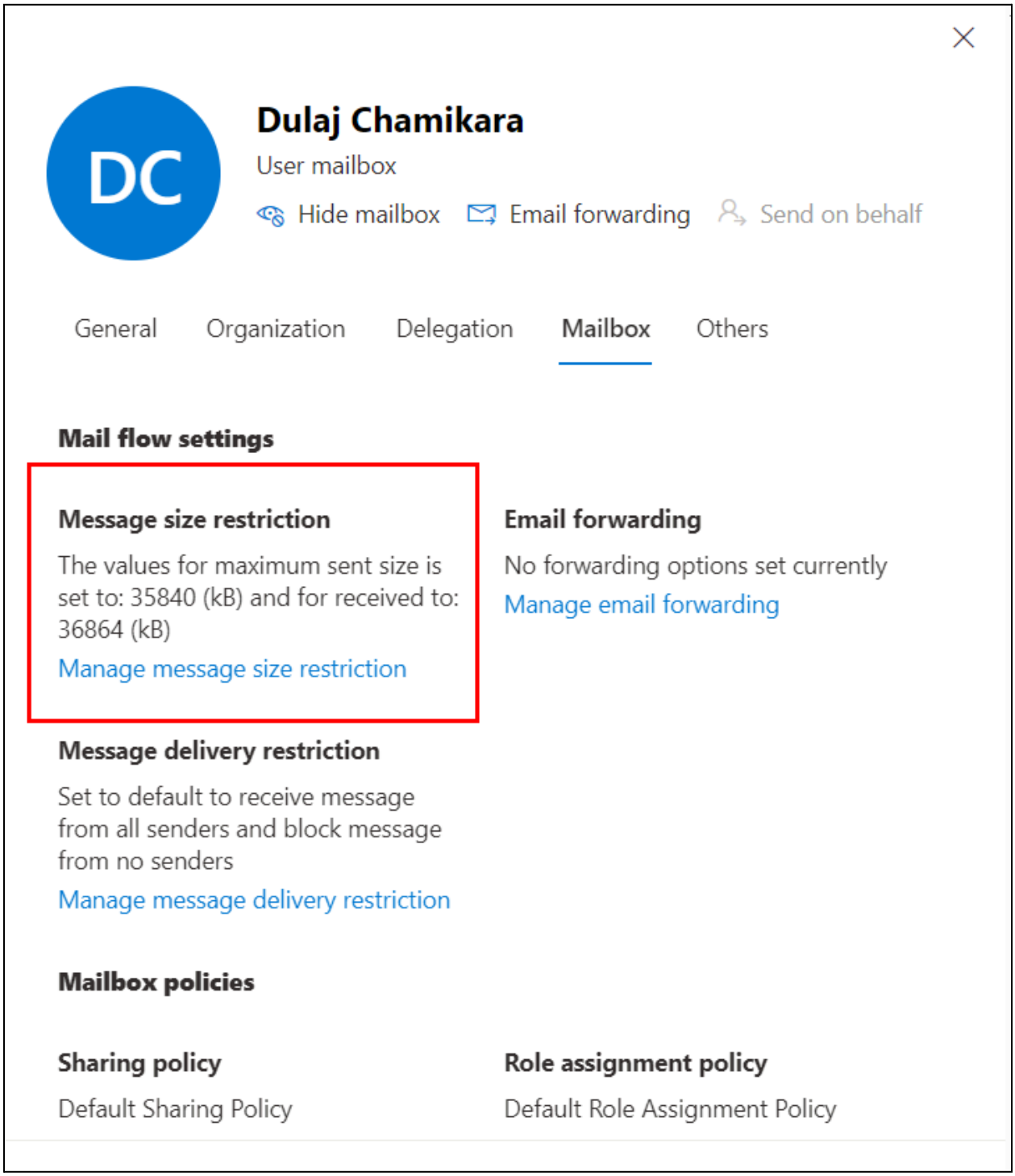
- Controls the **maximum size of emails** (including attachments) a user can **send or receive**.
- Prevents large attachments from consuming bandwidth/storage.
- Ensures compliance with company policy (e.g., limiting to 25 MB per email).

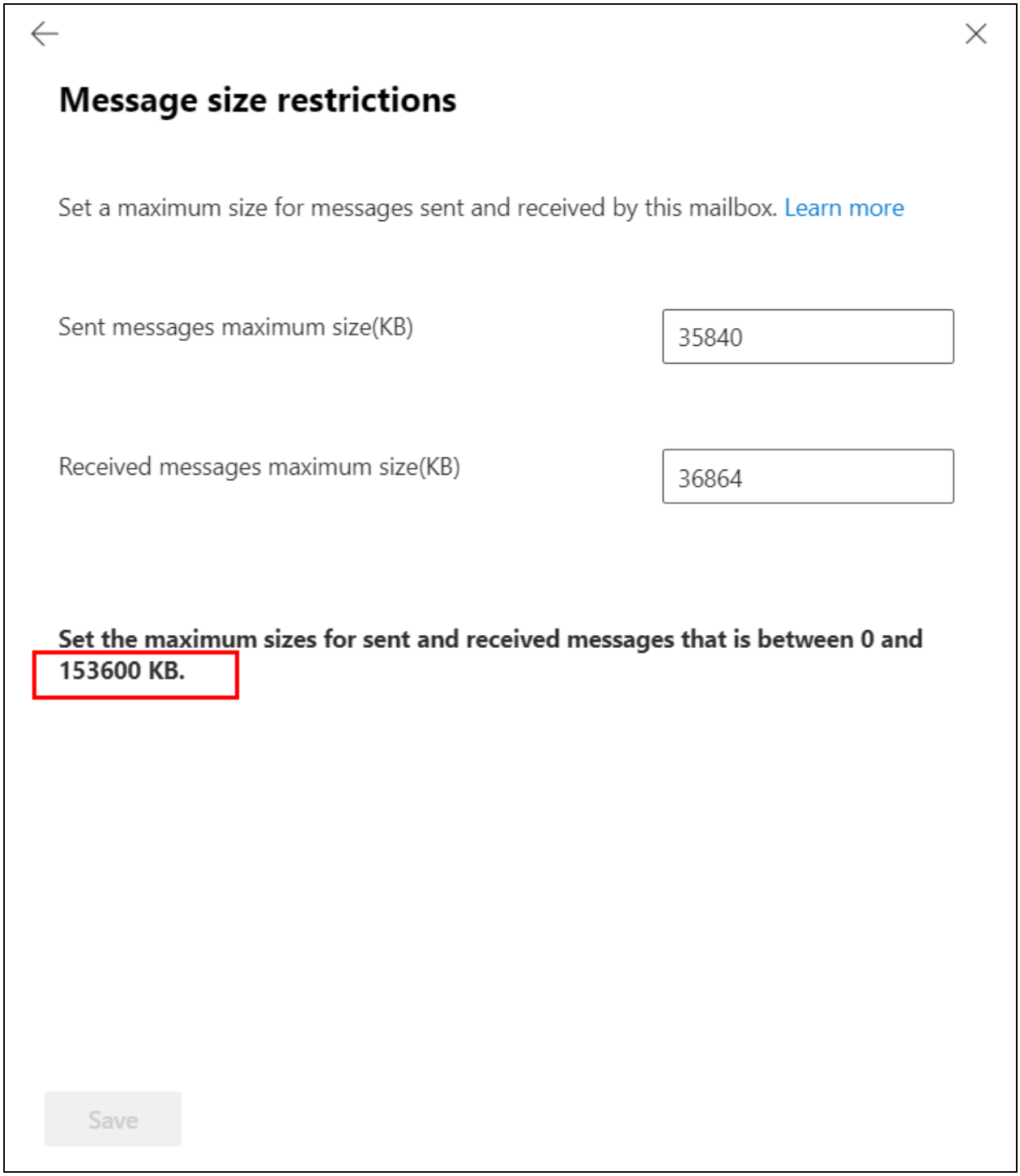
✅ Configuration Steps

Exchange Admin Center (EAC)

1. Go to **https://admin.exchange.microsoft.com**.
2. Navigate → **Recipients** → **Mailboxes**.
3. Select the mailbox → **Mail flow settings** → **Message size restrictions**.
4. Configure:
    - **Maximum send message size (KB)**.
    - **Maximum receive message size (KB)**.

5. Save changes.





Microsoft 365 Admin Center

- Limited options are available here; for detailed size limits, use **EAC or PowerShell**.

PowerShell (Exchange Online)

```
# Connect to Exchange Online
Connect-ExchangeOnline

# Set max send and receive size (25 MB example)
Set-Mailbox user1@contoso.com -MaxSendSize 25MB -MaxReceiveSize 25MB

# Allow larger attachments (e.g., 50 MB)
Set-Mailbox user1@contoso.com -MaxSendSize 50MB -MaxReceiveSize 50MB

# View current settings
Get-Mailbox user1@contoso.com | Select DisplayName, MaxSendSize,
MaxReceiveSize
```

✅ Validation

- Send a test email **larger than the limit** → should be rejected with an NDR (e.g., "Message size exceeds limit").
- Send a test email **within the limit** → should deliver successfully.
- Confirm via message trace:

```
Get-MessageTrace -Recipients user1@contoso.com -StartDate
(Get-Date).AddHours(-1) -EndDate (Get-Date)
```

✅ Best Practices

- Keep message size **aligned with Microsoft's default (35 MB send, 36 MB receive)** unless business requires more.
- Encourage users to use **OneDrive or SharePoint links** instead of large attachments.
- Apply consistent limits across mailboxes for predictable behavior.
- Monitor users who frequently hit limits → may need workflow redesign.

✅ **Use Case**

- A sales team often shares **large presentations (20–30 MB)** via email.
- Configure their mailboxes to allow **up to 50 MB** send size, while standard users remain at **25 MB**.
- Reduces friction while maintaining control for the wider org.

---

10. How to Create a Microsoft 365 Group

✅ **Purpose**

- A **Microsoft 365 Group** provides a shared space for collaboration, including:
    - Shared mailbox
    - Shared calendar
    - SharePoint document library
    - OneNote notebook & Planner integration
- Replaces legacy **distribution lists** by enabling **collaboration + communication**.
- Great for **teams, projects, and departments**.

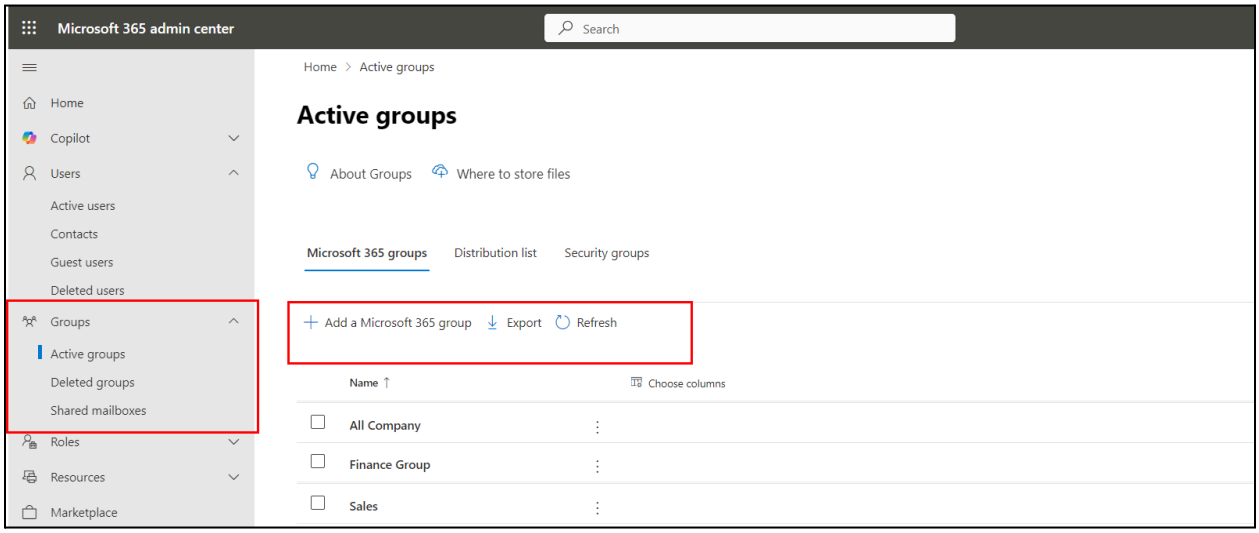
✅ **Configuration Steps**

Microsoft 365 Admin Center

1. Go to **https://admin.microsoft.com** → Sign in as Global/Exchange Admin.
2. Navigate → **Teams & groups** → **Active teams & groups** → **Add a group**.
3. Select **Microsoft 365 Group** → Next.
4. Configure:
    - Group name & email address.

- Privacy: **Public** (anyone can join) or **Private** (owner-approved).
- Owners & members.

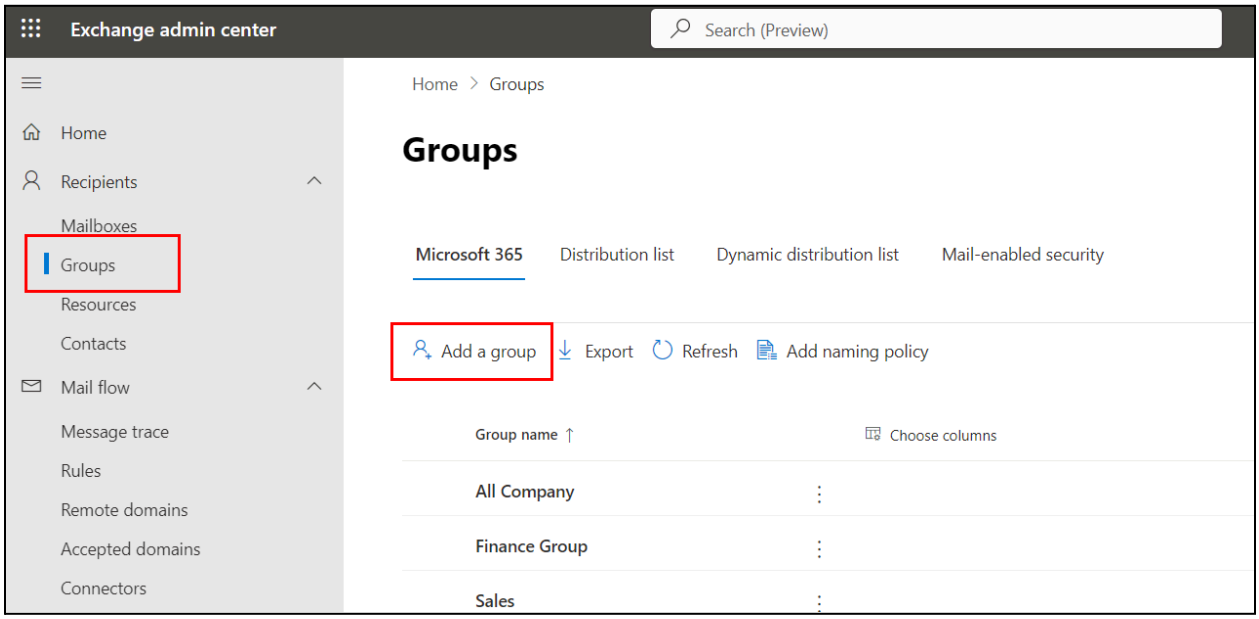
5. Assign licenses (if required for Teams/Planner/SharePoint).
6. Click **Create group**.



Exchange Admin Center (EAC)

1. Go to **https://admin.exchange.microsoft.com**.
2. Navigate → **Recipients** → **Groups** → **Add a group**.
3. Select **Microsoft 365 Group**.
4. Fill in: **Name, Alias, Email, Privacy**, owners, members.

5. Save → Group created.



PowerShell (Exchange Online)

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Create a Microsoft 365 Group

New-UnifiedGroup -DisplayName "Sales Team" -Alias "SalesTeam"
-EmailAddresses "SalesTeam@contoso.com" -AccessType Private -Owners
user1@contoso.com -Members user2@contoso.com,user3@contoso.com


# Add members later

Add-UnifiedGroupLinks -Identity "Sales Team" -LinkType Members -Links
user4@contoso.com


# View group

Get-UnifiedGroup -Identity "Sales Team"
```

✅ **Validation**

- In **Outlook/OWA** → the group appears in the left navigation.
- Test sending an email to group email → should deliver to all members.
- Check shared resources (calendar, files, OneNote).
- Run PowerShell check:

```
Get-UnifiedGroupLinks -Identity "Sales Team" -LinkType Members
```

✅ **Best Practices**

- Use **private groups** for sensitive teams (Finance, HR).
- Use **naming policy** for consistency (e.g., Dept_Project@contoso.com).
- Regularly review group membership with **Access Reviews** in Azure AD.
- Educate users to use the group's **shared mailbox & files** instead of personal storage.

✅ **Use Case**

- A company launches a **new product project**.
- Create a **Microsoft 365 Group: "ProjectPhoenix"** → adds shared mailbox, calendar, Teams, and file storage.
- All project members automatically get access to collaboration tools without manual setup.

---

11. How to Create a Distribution Group

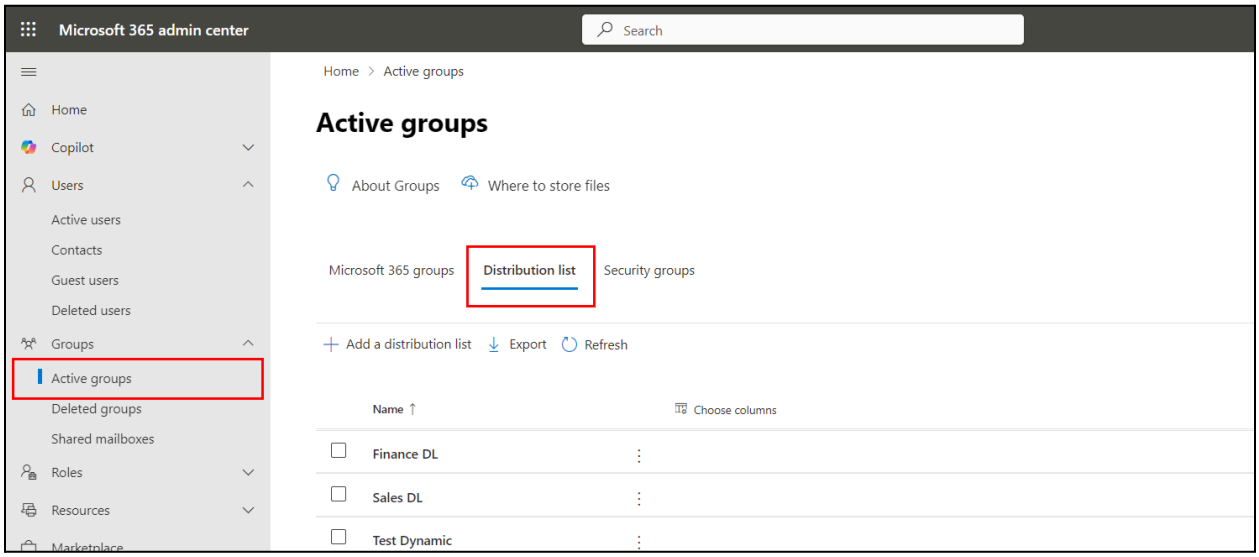
✅ **Purpose**
A Distribution Group (Distribution List) is used to **send emails to multiple recipients** at once.
Key points:

- Simplifies communication for teams, departments, or projects.
- Members receive emails sent to the group email address.
- Does **not** provide collaboration tools like Teams, SharePoint, or Planner.
- Ideal for announcements, newsletters, or internal mailing lists.

✅ Configuration Steps

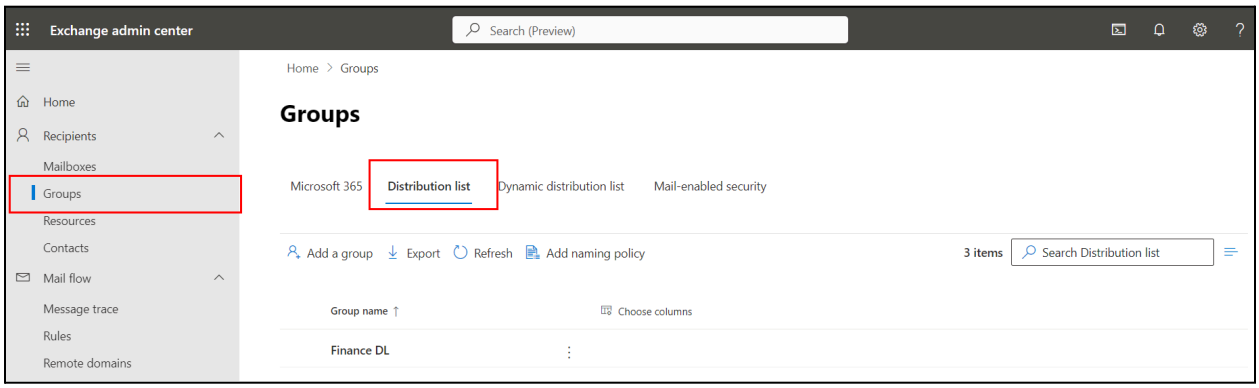
Microsoft 365 Admin Center

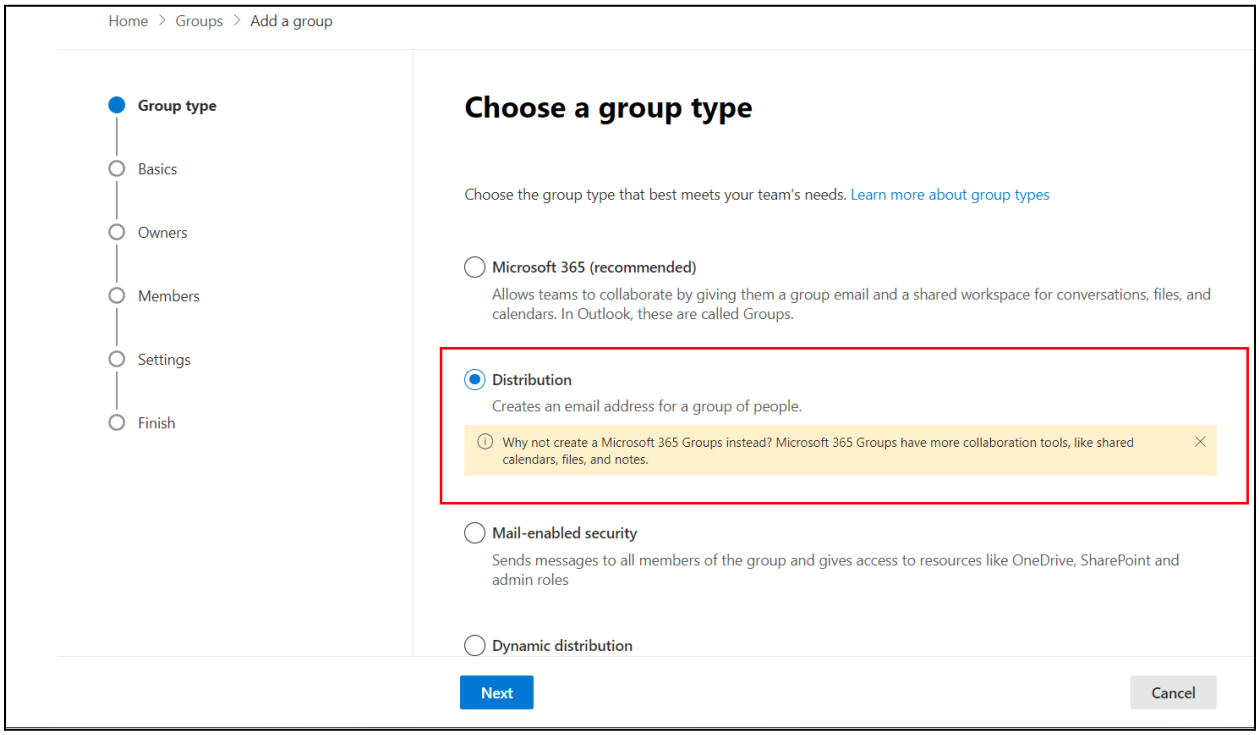
1. Go to https://admin.microsoft.com → Sign in as Global/Exchange Admin.
2. Navigate → **Teams & groups** → **Active teams & groups** → **Add a group**.
3. Select **Distribution** → Next.
4. Configure:
    - **Group name & email address**
    - **Owners & members**
    - Optional: delivery management or restrictions (who can send to this group)
5. Click **Create group**



Exchange Admin Center (EAC)

1. Go to https://admin.exchange.microsoft.com
2. Navigate → **Recipients → Groups → Add a group**
3. Select **Distribution**
4. Fill in: **Name, Alias, Email, Owners, Members**
5. Configure optional settings (delivery management, message approval)
6. Save → Group created





PowerShell (Exchange Online)

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Create a Distribution Group

New-DistributionGroup -Name "MarketingTeam" -Alias "MarketingTeam"
-PrimarySmtpAddress "MarketingTeam@contoso.com" -Members
user1@contoso.com,user2@contoso.com -ManagedBy user3@contoso.com


# Add members later

Add-DistributionGroupMember -Identity "MarketingTeam" -Member
user4@contoso.com


# View group

Get-DistributionGroup -Identity "MarketingTeam"
```

✅ **Validation**

- In Outlook/OWA → the distribution group appears in the address book.
- Test sending an email → all members should receive it.
- Check membership using PowerShell:

```
Get-DistributionGroupMember -Identity "MarketingTeam"
```

✅ **Best Practices**

- Use for **email-only communication**; do not mix with collaboration needs.

- Name groups consistently (e.g., Dept_Function@contoso.com).
- Assign owners for membership management.
- Regularly review members to remove inactive users.
- Restrict who can send to large groups to prevent spam.

✅ **Use Case**
A company wants to send monthly updates to all marketing staff.

- Create a Distribution Group: **MarketingTeam**
- All marketing members automatically receive announcements via email.
- Ensures **consistent communication** without manually selecting recipients.

---

12. How to Convert a Distribution Group

✅ **Purpose**
Converting a Distribution Group to a Microsoft 365 Group allows you to:

- Enable **collaboration features** (Teams, SharePoint, Planner, OneNote) for existing email distribution lists.
- Preserve existing **members and email addresses**.
- Modernize legacy email workflows while retaining group communication.

✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Go to https://admin.exchange.microsoft.com → Sign in as Global/Exchange Admin.
2. Navigate → **Recipients** → **Groups**
3. Select the **Distribution Group** you want to convert.
4. Click **Convert to Microsoft 365 Group**.

5. Configure settings:
    - **Group name & email address** (pre-filled from existing DG)
    - **Privacy**: Public or Private
    - **Owners & members** (existing members are carried over)
6. Click **Convert** → wait for the process to complete

PowerShell (Exchange Online)
Currently, **PowerShell does not directly support DG-to-M365 Group conversion**, but you can:

1. Export members of the Distribution Group:

```
Get-DistributionGroupMember -Identity "MarketingTeam" | Select
PrimarySmtpAddress
```

2. Create a new Microsoft 365 Group and add members:

```
New-UnifiedGroup -DisplayName "MarketingTeam" -Alias "MarketingTeam"
-EmailAddresses "MarketingTeam@contoso.com" -AccessType Private
-Owners user1@contoso.com -Members user2@contoso.com,user3@contoso.com
```

3. Add remaining members from export.

✅ **Validation**

- In Outlook/OWA → the new Microsoft 365 Group appears in the left navigation.
- Test sending an email → should deliver to all existing members.
- Verify access to shared resources: calendar, files, Teams.
- Run PowerShell check:

```
Get-UnifiedGroupLinks -Identity "MarketingTeam" -LinkType Members
```

✅ **Best Practices**

- Notify users about the change, as collaboration tools become available.
- Use private groups for sensitive data.
- Review group membership and owners after conversion.
- Migrate legacy rules, mail flow restrictions, or moderation settings to the new group.
- Test thoroughly before decommissioning the old Distribution Group.

✅ **Use Case**
A company has a legacy **FinanceDept** distribution list for budget approvals.

- Convert **FinanceDept** to a Microsoft 365 Group.
- The finance team now has a shared **mailbox, Teams channel, Planner, and SharePoint library**.
- Existing members continue receiving emails, but collaboration and file sharing are now streamlined.

---

13. How to Create a Dynamic Distribution Group

✅ **Purpose**
A **Dynamic Distribution Group (DDG)** automatically includes recipients based on **criteria or attributes** in Azure AD or Exchange.

- Eliminates manual management of group membership.
- Ideal for large, frequently changing teams (e.g., all users in a department or region).
- Members automatically update when their attributes change (department, location, title, etc.).

- Used primarily for **email communication**; does **not** provide collaboration tools like Teams or SharePoint.

✅ Configuration Steps

Exchange Admin Center (EAC)

1. Go to https://admin.exchange.microsoft.com → Sign in as Global/Exchange Admin.
2. Navigate → **Recipients** → **Groups** → **Add a group**
3. Select **Dynamic distribution** → Next
4. Configure:
    - **Name & Alias**
    - **Owner** (who manages the group)
    - **Recipient filter**: Choose **Users with specific attributes** (Department, Country/Region, Title, etc.)
5. Save → Group created

PowerShell (Exchange Online)

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Create Dynamic Distribution Group based on department

New-DynamicDistributionGroup -Name "HRTeam" -Alias "HRTeam"
-RecipientFilter {Department -eq "HR"}


# Verify the recipient filter

Get-DynamicDistributionGroup -Identity "HRTeam" | Format-List
Name,RecipientFilter
```

```
# Preview members that will be included

Get-Recipient -RecipientPreviewFilter (Get-DynamicDistributionGroup
"HRTeam").RecipientFilter
```

✅ **Validation**

- In Outlook/OWA → the dynamic distribution group appears in the address book.
- Test sending an email → it should deliver to all recipients that match the filter.
- Run PowerShell preview to ensure correct membership:

```
Get-Recipient -RecipientPreviewFilter (Get-DynamicDistributionGroup
"HRTeam").RecipientFilter
```

✅ **Best Practices**

- Use descriptive names that reflect the filter (e.g., HR_AllStaff@contoso.com).
- Keep recipient filters simple for performance efficiency.
- Periodically review and update attributes in Azure AD to ensure correct membership.
- Limit sending permissions to prevent accidental mass emails.
- Communicate with users that membership is **automatic and attribute-based**.

✅ **Use Case**
A company wants to send weekly newsletters to all **Sales Department staff** across multiple regions.

- Create a Dynamic Distribution Group: **SalesTeam**
- Use the filter **Department = Sales**

- Any new employee added to the Sales department automatically receives emails.
- Reduces administrative overhead and ensures accurate communication.

---

14. How to Restore a Deleted Microsoft 365 Group

✅ **Purpose**
Restoring a deleted Microsoft 365 Group allows you to:

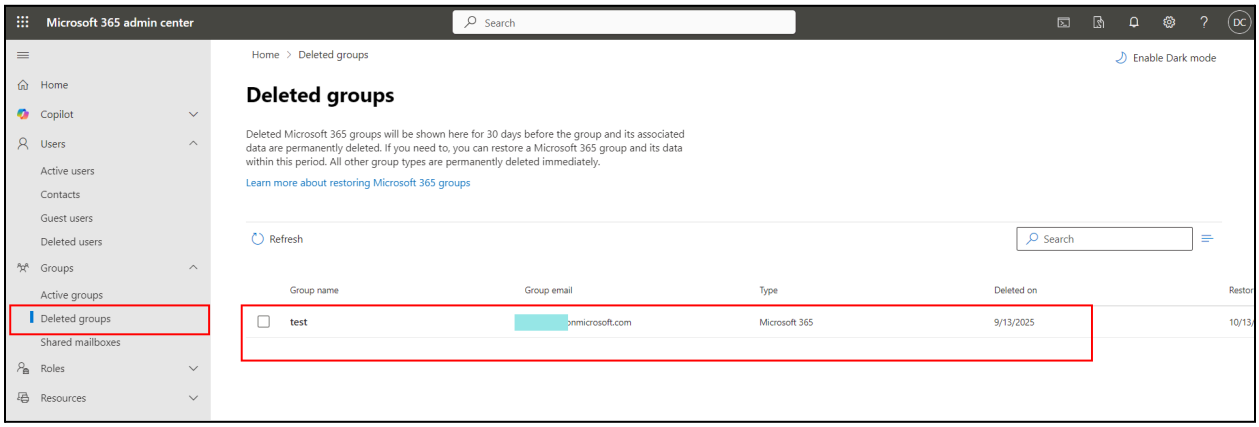
- Recover **group mailbox, files, calendar, and Teams data** within the retention period.
- Prevent loss of important communications and collaboration content.
- Ensure business continuity without recreating the group manually.

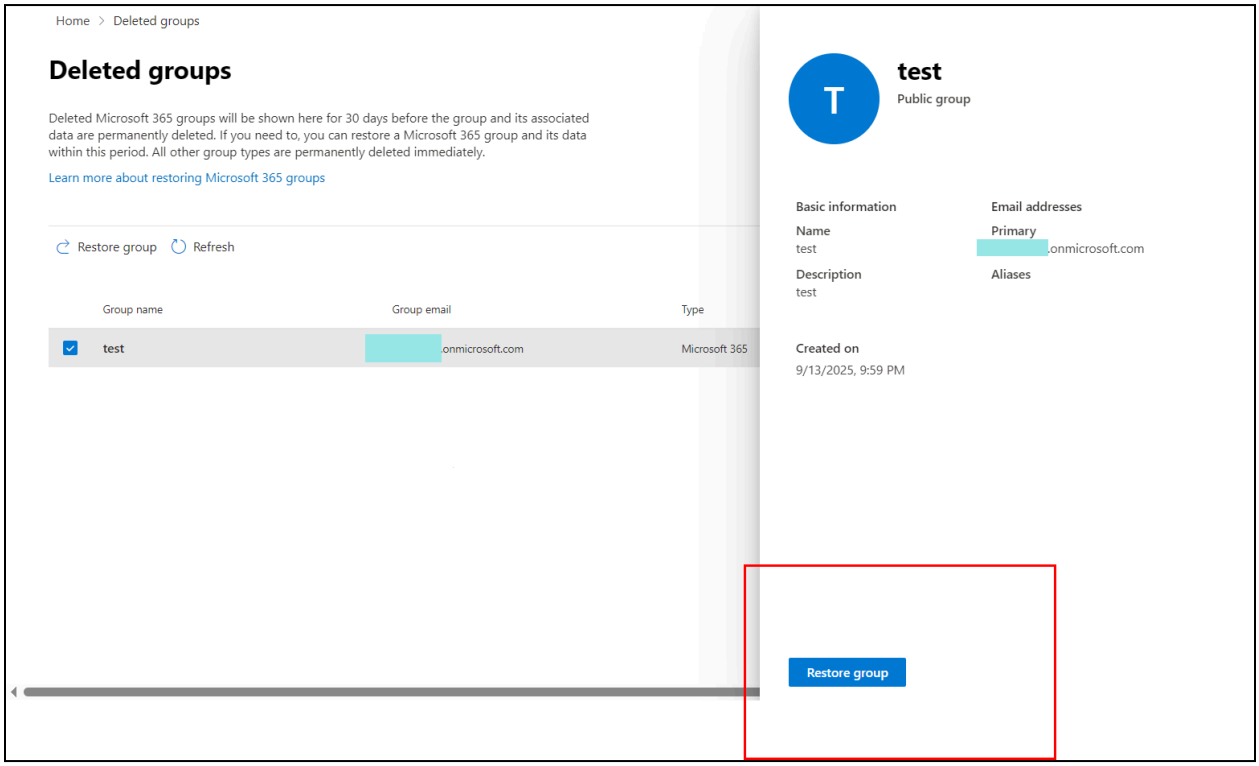
✅ **Configuration Steps**

Microsoft 365 Admin Center

- Go to https://admin.microsoft.com → Sign in as Global/Exchange Admin.
- Navigate → **Teams & groups** → **Deleted groups**
- Select the deleted Microsoft 365 Group you want to restore.
- Click **Restore group** → Confirm

- Wait for the group to be restored (may take a few minutes).





PowerShell (Exchange Online / Azure AD)

```
# Connect to Exchange Online

Connect-ExchangeOnline


# List deleted Microsoft 365 Groups (soft-deleted within 30 days)
```

```
Get-UnifiedGroup -SoftDeletedMailbox


# Restore a deleted group

Restore-UnifiedGroup -Identity "ProjectPhoenix"


# Verify restoration

Get-UnifiedGroup -Identity "ProjectPhoenix"
```

✅ **Validation**

- In Outlook/OWA → the restored group appears in the left navigation.
- Test sending an email → should deliver to all original members.
- Check access to shared resources (calendar, files, Teams).
- Confirm membership:

```
Get-UnifiedGroupLinks -Identity "ProjectPhoenix" -LinkType Members
```

✅ **Best Practices**

- Restore **within 30 days** of deletion (default soft-delete retention period).
- Communicate with users about the restoration to avoid confusion.
- Verify **licenses** are reassigned if needed.
- Regularly backup critical group data using third-party tools or Microsoft 365 retention policies.
- Avoid deleting groups unnecessarily; consider archiving instead.

✅ **Use Case**
A project team accidentally deletes the **ProjectPhoenix** Microsoft 365 Group.

- Admin restores the group within the 30-day retention window.
- All members regain access to emails, shared files, and Teams channels.
- Project work continues seamlessly without data loss.

---

15. How to Create a Mail-Enabled Security Group

✅ **Purpose**
A **Mail-Enabled Security Group** combines **security permissions** with **email communication**.

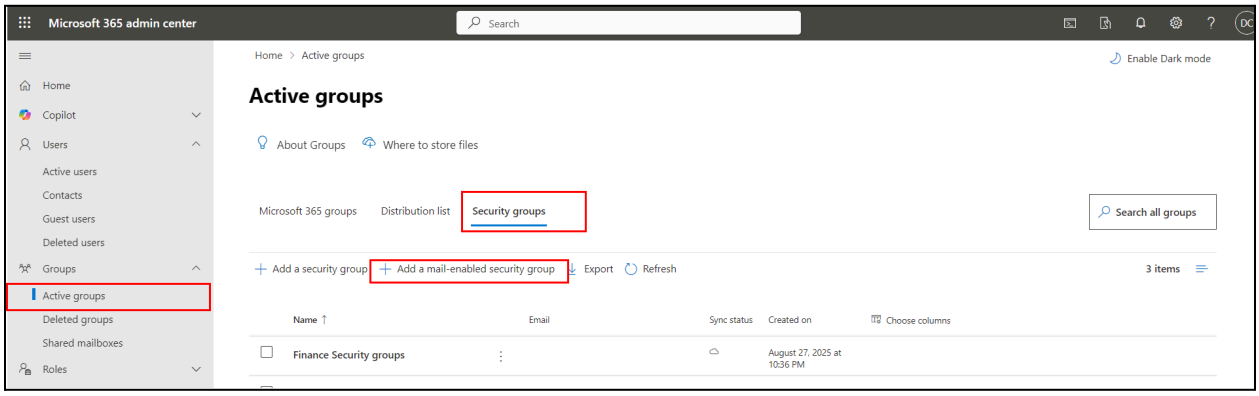
- Can be used to **assign access rights** to resources (SharePoint, file shares, Teams) **and** send emails to all members.
- Ideal for teams needing **both email distribution and access control**.
- Helps streamline both communication and permission management.

✅ **Configuration Steps**

Microsoft 365 Admin Center

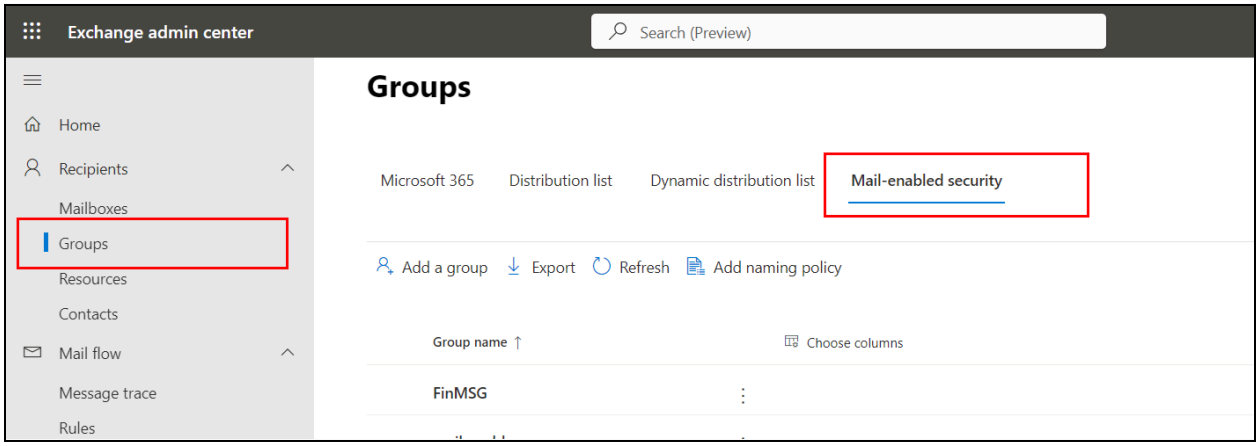
1. Go to https://admin.microsoft.com → Sign in as Global/Exchange Admin.
2. Navigate → **Teams & groups** → **Active teams & groups** → **Add a group**
3. Select **Security** → Enable **Mail-Enabled** option → Next
4. Configure:
    - **Group name & email address**
    - **Owners & members**

5. Click **Create group**



Exchange Admin Center (EAC)

1. Go to https://admin.exchange.microsoft.com
2. Navigate → **Recipients → Groups → Add a group**
3. Select **Mail-Enabled Security**
4. Fill in: **Name, Alias, Email, Owners, Members**
5. Save → Group created



PowerShell (Exchange Online)

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Create Mail-Enabled Security Group
```

```
New-DistributionGroup -Name "FinanceAdmins" -Alias "FinanceAdmins"
-PrimarySmtpAddress "FinanceAdmins@contoso.com" -MemberJoinRestriction
Open -Type Security


# Add members later

Add-DistributionGroupMember -Identity "FinanceAdmins" -Member
user1@contoso.com,user2@contoso.com


# Verify group

Get-DistributionGroup -Identity "FinanceAdmins"
```

✅ **Validation**

- In Outlook/OWA → the group appears in the address book.
- Test sending an email → all members should receive it.
- Verify **security access**: assign permissions to a SharePoint site or file share → members can access.
- Check members using PowerShell:

```
Get-DistributionGroupMember -Identity "FinanceAdmins"
```

✅ **Best Practices**

- Use for teams that need **both email communication and resource access**.
- Assign **responsible owners** to manage membership.
- Limit who can send to large mail-enabled security groups.
- Follow consistent naming conventions (e.g., Dept_Sec@contoso.com).

- Regularly review membership and permissions to maintain security compliance.

✅ **Use Case**
A company needs a group for **Finance Administrators** who manage financial systems.

- Create a Mail-Enabled Security Group: **FinanceAdmins**
- Members can receive important email notifications and have **access permissions** to financial SharePoint sites.
- Combines communication and security in a single group, reducing administrative overhead.

---

16. Create and Manage Mail Contacts in Exchange Online

✅ **Purpose**
Mail contacts represent **external email addresses** in the Exchange Online directory.

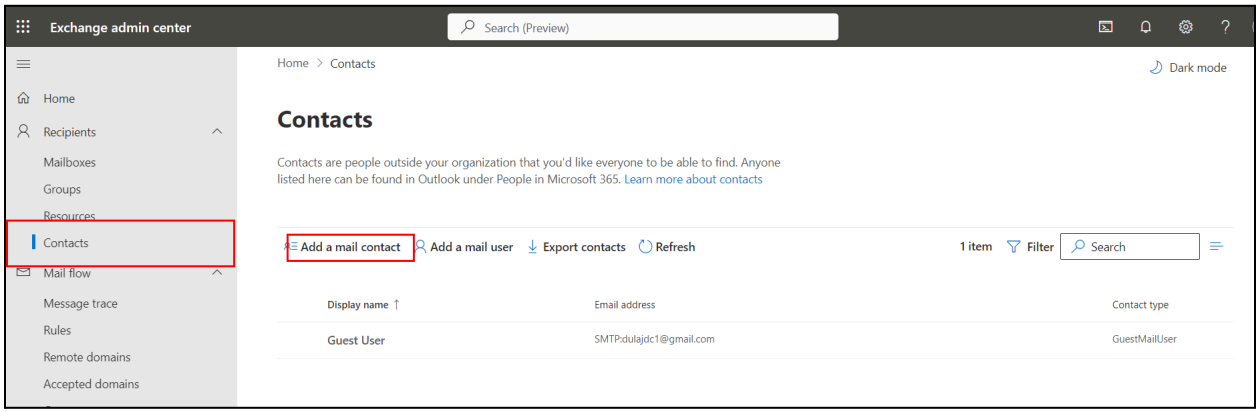
- Useful for sending emails to external partners without creating full Microsoft 365 accounts.
- Can be included in **distribution lists or groups**.

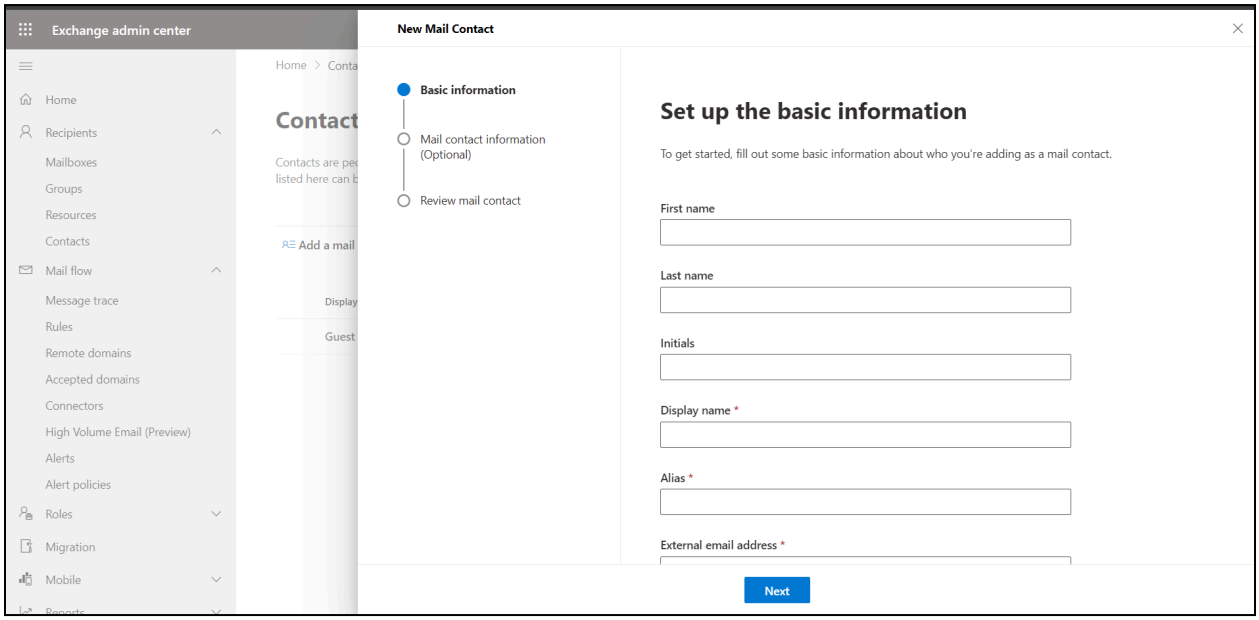
✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Go to https://admin.exchange.microsoft.com.
2. Navigate → **Recipients** → **Contacts** → **Add a contact**.
3. Fill in: **Display Name, External Email Address, Alias**.

4. Save → Contact created.





PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Create a mail contact

New-MailContact -Name "John Doe" -ExternalEmailAddress
"john.doe@example.com" -Alias "JohnDoe"
```

```
# View contact

Get-MailContact -Identity "John Doe"


# Update contact

Set-MailContact -Identity "John Doe" -ExternalEmailAddress
"john.new@example.com"
```

✅ **Validation**

- Appears in the address **book** and can receive emails.
- Can be added to distribution groups.

✅ **Use Case**
Add external vendor contacts for easy inclusion in email communication without creating full accounts.

---

17. Create and Manage Mail Users in Exchange Online

✅ **Purpose**
Mail users have **external email addresses but are represented as user accounts** in Microsoft 365.

- Can **log in** to Microsoft 365 but mail is delivered to an external address.
- Useful for **partners, contractors, or consultants** who need directory presence but not internal mailboxes.

✅ **Configuration Steps**

EAC

1. Navigate → **Recipients** → **Contacts** → **Add mail user**.

2. Fill in: **Display Name, External Email, User Logon, Alias**.

3. Assign password → Save.

PowerShell

```
# Create a mail user

New-MailUser -Name "Jane Smith" -ExternalEmailAddress
"jane.smith@external.com" -UserPrincipalName "jane.smith@contoso.com"
-Password (ConvertTo-SecureString 'Password123!' -AsPlainText -Force)



# View mail user

Get-MailUser -Identity "Jane Smith"
```

✅ **Validation**

- Appears in the address **book**.
- Can receive emails sent to the directory.

✅ **Use Case**
Create accounts for consultants who need access to Teams and Azure AD resources but use external email for messaging.

---

18. Create Room and Equipment Mailbox in Exchange Online

✅ **Purpose**
Room and Equipment Mailboxes are **resource mailboxes** used to schedule rooms or equipment.

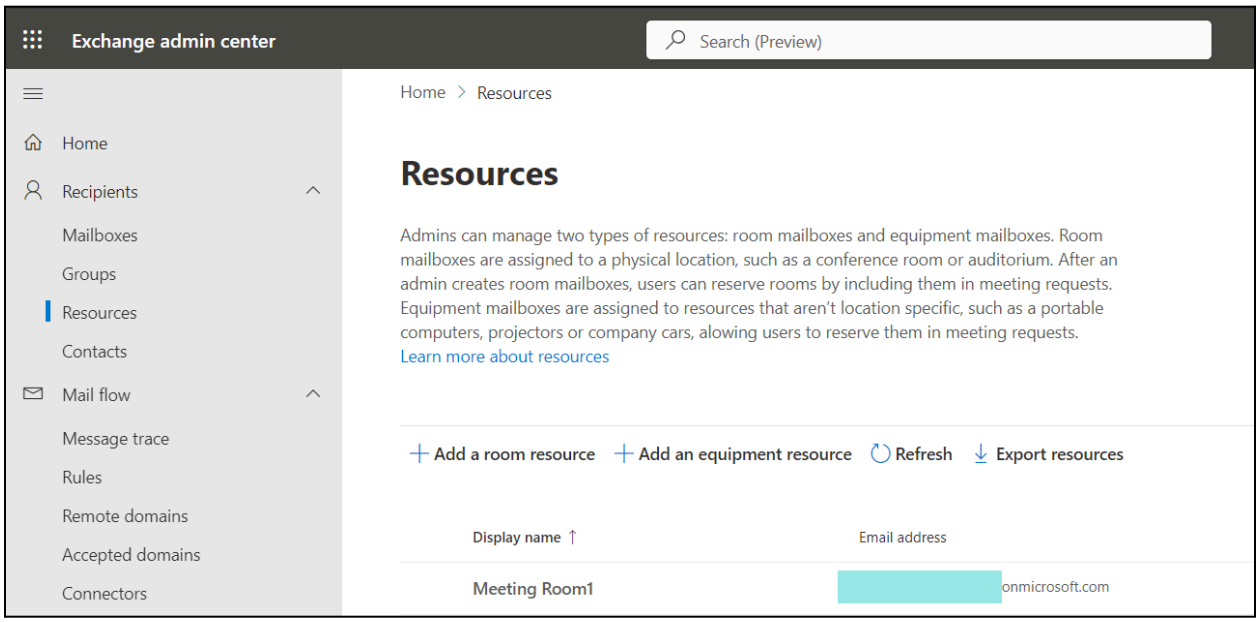
- Room mailbox: physical meeting rooms
- Equipment mailbox: projectors, laptops, shared devices

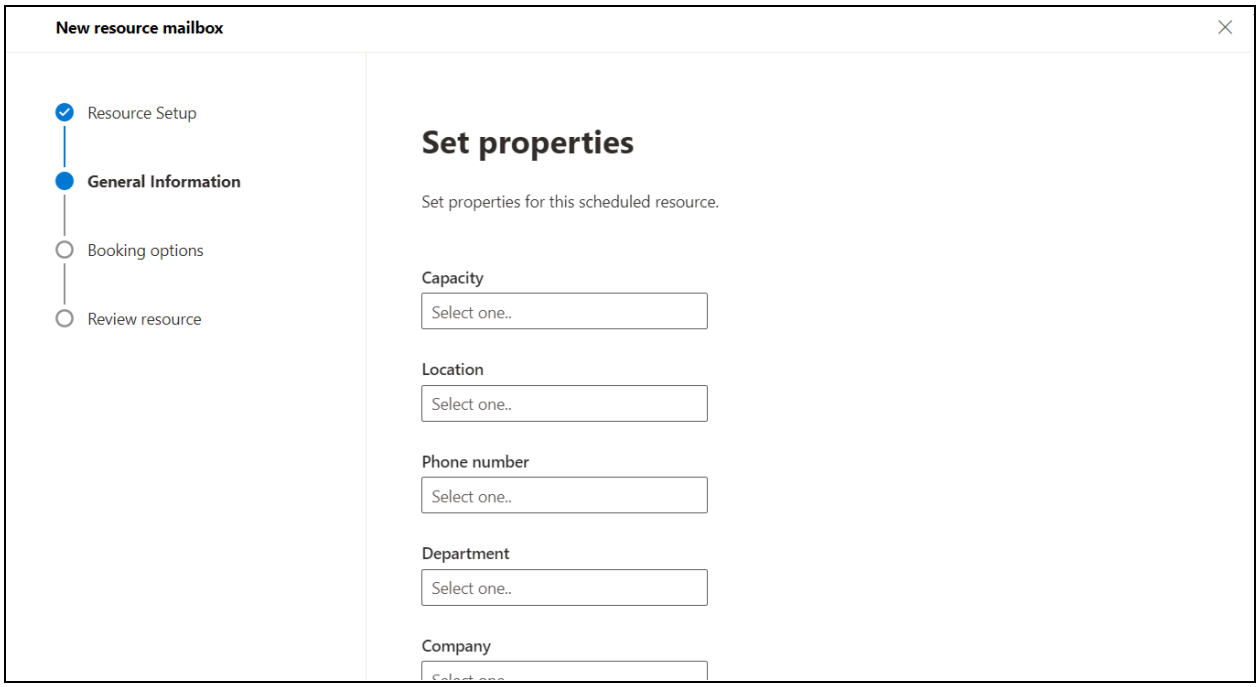
- Enables **calendar-based booking**

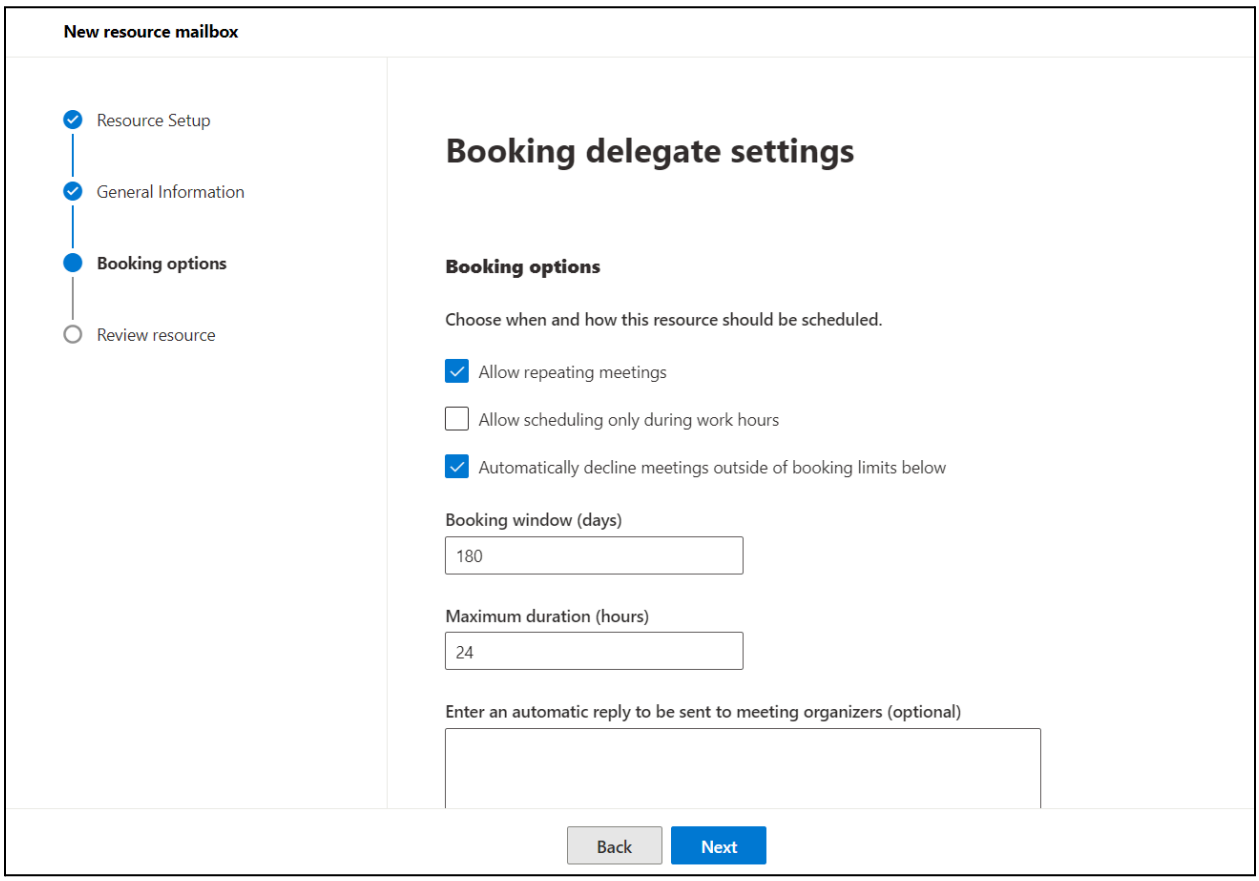
✅ Configuration Steps

EAC

1. Navigate → **Recipients** → **Resources** → **Add a resource**.
2. Choose **Room** or **Equipment**.
3. Fill in: **Name, Email, Capacity (for rooms)**.
4. Save → Mailbox created.







PowerShell

```
# Create a room mailbox
```

```
New-Mailbox -Name "ConfRoom101" -Room


# Create equipment mailbox

New-Mailbox -Name "Projector1" -Equipment


# View resource mailbox

Get-Mailbox -RecipientTypeDetails RoomMailbox

Get-Mailbox -RecipientTypeDetails EquipmentMailbox
```

✅ **Validation**

- Appears in Outlook **Room Finder** when booking meetings.
- Can send calendar invites to test availability.

✅ **Use Case**
Create a room mailbox **ConfRoom101** and an equipment mailbox **Projector1** for meeting scheduling.

---

19. Manage and Book Resource Mailbox in Exchange Online

✅ **Purpose**
Resource mailboxes allow **automated scheduling and booking** with configurable policies.

- Control **booking permissions, delegate approvals, maximum meeting duration, and auto-accept rules**.

✅ **Configuration Steps**

EAC

1. Navigate → **Recipients** → **Resources** → **Select a resource**.

2. Configure:
    - Booking options (AutoAccept, Require Approval)
    - Maximum meeting duration
    - Delegate management
3. Save changes.

PowerShell

```
# Set resource mailbox to auto-accept

Set-CalendarProcessing -Identity "ConfRoom101" -AutomateProcessing
AutoAccept -AllowConflicts $false -MaximumDurationInMinutes 120


# View configuration

Get-CalendarProcessing -Identity "ConfRoom101"
```

✅ **Validation**

- Book a test meeting → auto-accept based on policy.
- Check delegates receive approval requests if configured.

✅ **Use Case**
Automate conference room booking while preventing overlapping reservations and limiting meeting duration.

---

20. Create a Shared Mailbox in Exchange Online

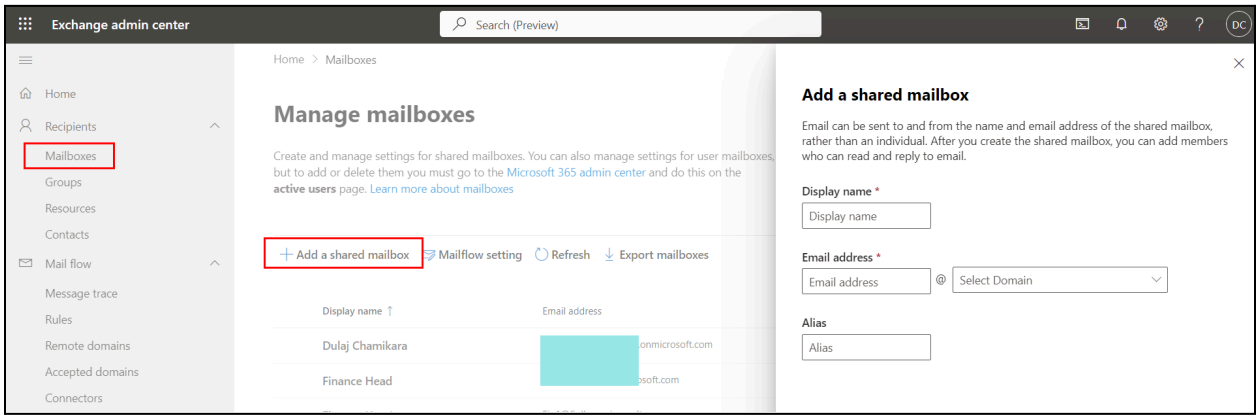
✅ **Purpose**
A Shared Mailbox allows **multiple users to send and receive emails** from a common mailbox.

- Includes shared calendar, contacts, and tasks.
- Users do **not need separate licenses** if under 50GB mailbox size.
- Ideal for **support, info, or sales email addresses**.

✅ Configuration Steps

EAC

1. Navigate → **Recipients** → **mailboxes**→ **Add a shared mailbox**.
2. Fill in: **Name, Email**.
3. Add members who need access.
4. Save → Mailbox created.



PowerShell

```
# Create a shared mailbox

New-Mailbox -Name "SupportTeam" -Shared -PrimarySmtpAddress
"support@contoso.com"


# Add members

Add-MailboxPermission -Identity "SupportTeam" -User user1@contoso.com
-AccessRights FullAccess -InheritanceType All
```

```
Add-RecipientPermission -Identity "SupportTeam" -Trustee
user1@contoso.com -AccessRights SendAs


# Verify

Get-Mailbox -Identity "SupportTeam"
```

✅ **Validation**

- Appears in Outlook → users can send/receive emails.
- Test **Send As** and **Full Access** permissions.

✅ **Use Case**
Create a **support@contoso.com** shared mailbox for the customer support team to handle incoming requests collectively.

---

21. Convert a User Mailbox to a Shared Mailbox in Exchange Online

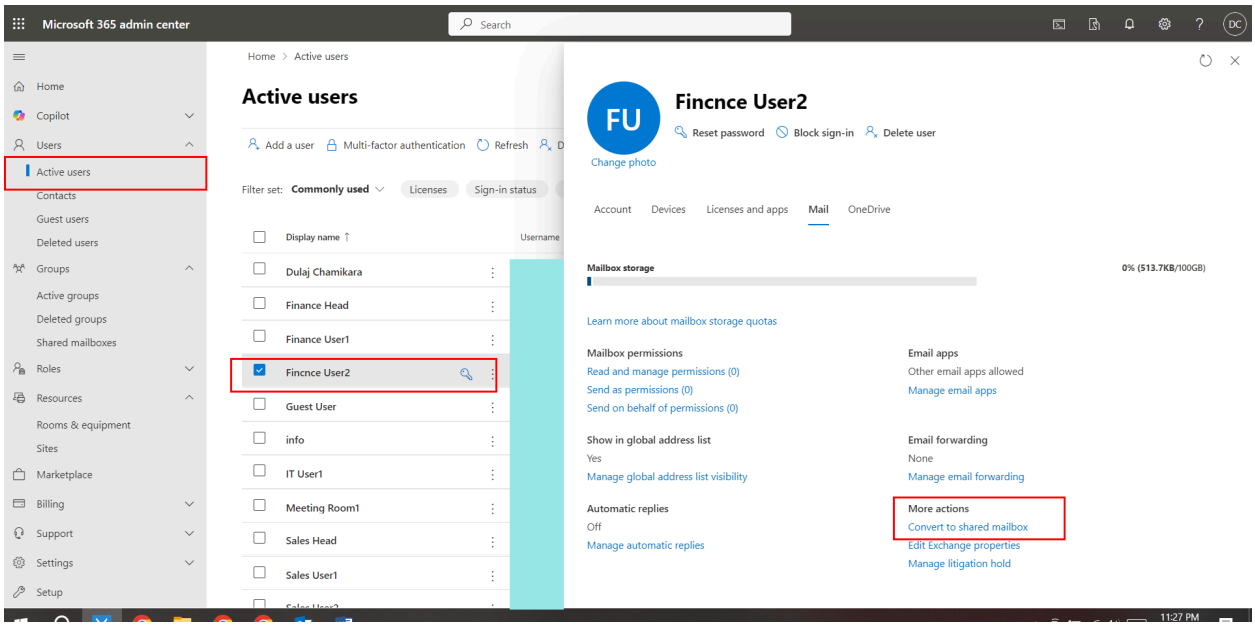
✅ **Purpose**
Converting a user mailbox to a shared mailbox allows:

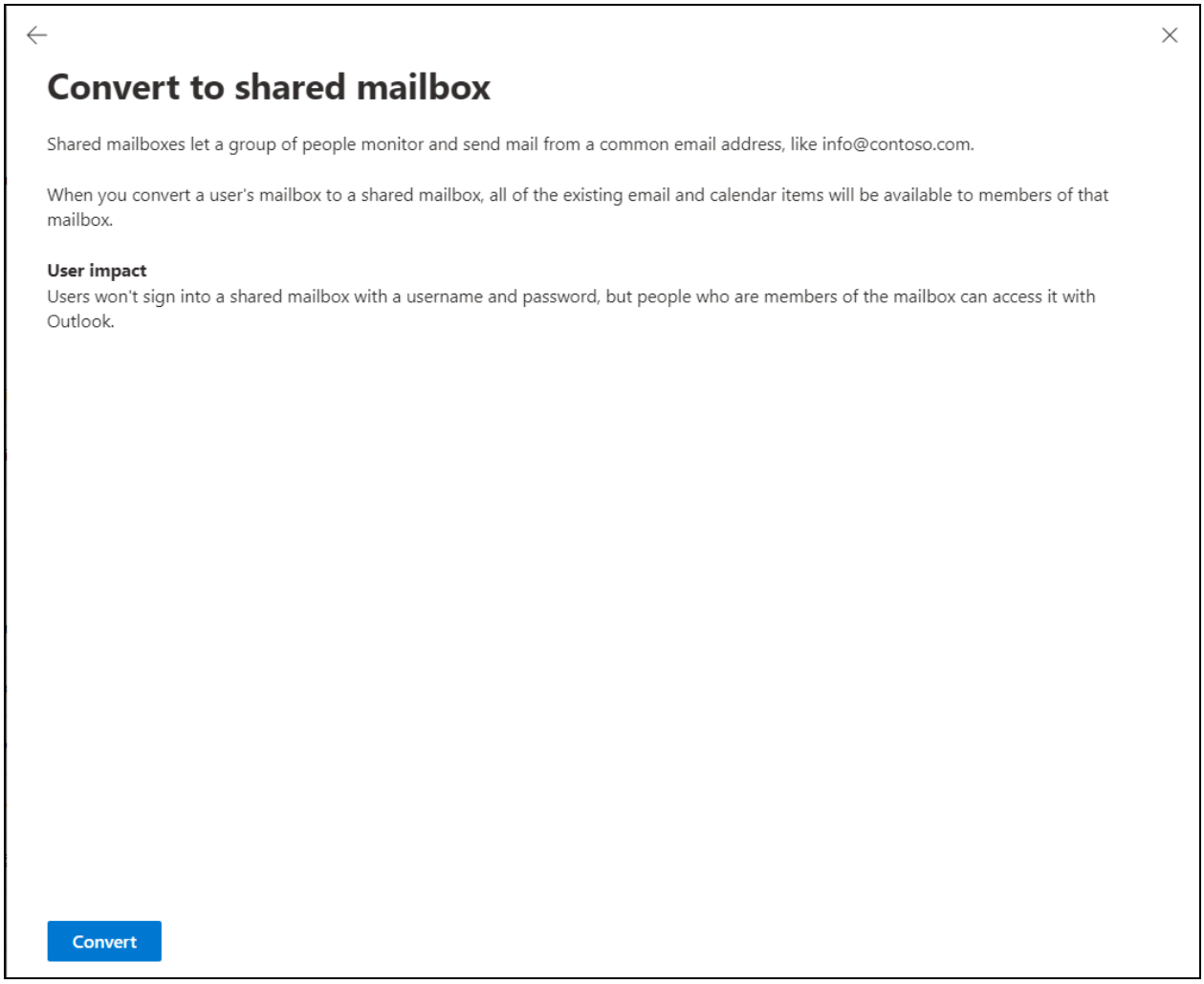
- Multiple users to **access and manage emails collectively** without needing separate licenses (if mailbox is under 50GB).
- Simplified collaboration for teams handling common mailboxes such as support, info, or sales.
- Retention of existing emails, calendar items, and contacts during conversion.

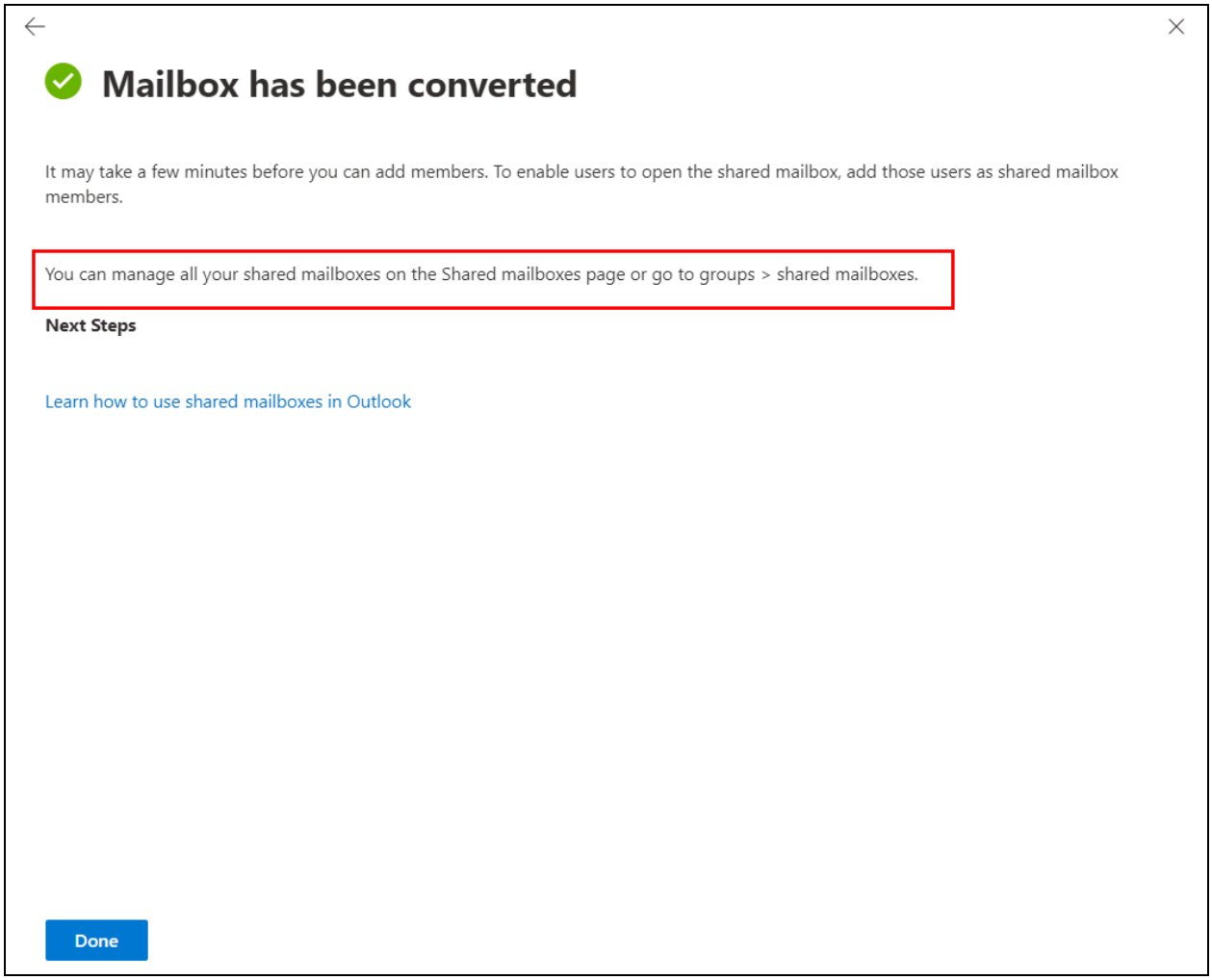
✅ **Configuration Steps**

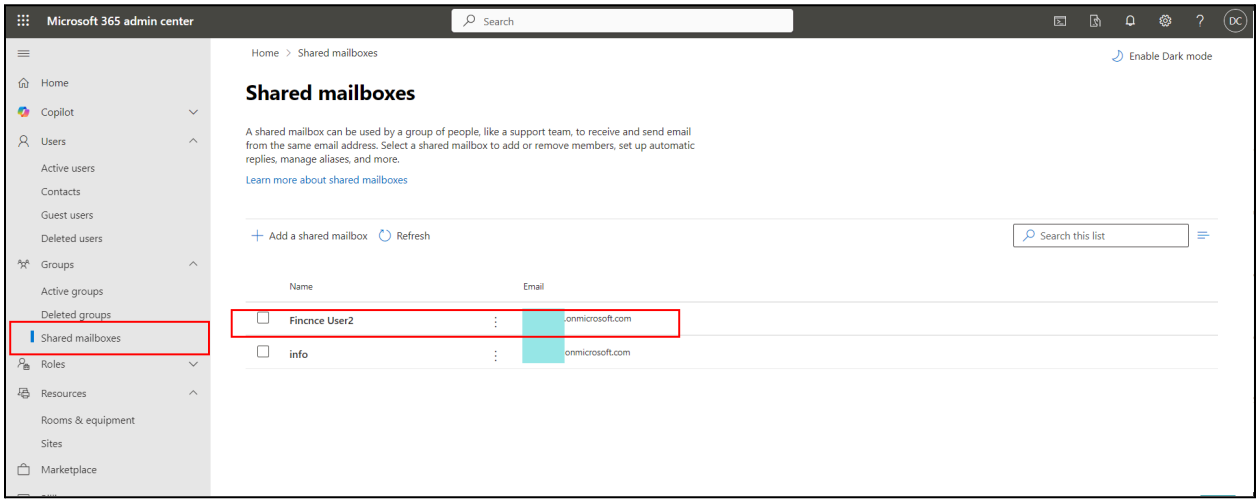
Microsoft 365 Admin Center

1. Go to https://admin.microsoft.com → Sign in as Global/Exchange Admin.
2. Navigate → **Users** → **Active users**
3. Select the user mailbox you want to convert.
4. In the **Mailbox settings** section, click **Convert to shared mailbox**.
5. Confirm → the mailbox is converted.
6. Add members who need access: **Mail** → **Shared mailbox** → **Members** → **Edit** → Add users.




Convert to shared mailbox
Shared mailboxes let a group of people monitor and send mail from a common email address, like info@contoso.com.
When you convert a user's mailbox to a shared mailbox, all of the existing email and calendar items will be available to members of that mailbox.
User impact
Users won't sign into a shared mailbox with a username and password, but people who are members of the mailbox can access it with Outlook.
Convert





PowerShell

```
# Connect to Exchange Online
```

```
Connect-ExchangeOnline


# Convert a user mailbox to a shared mailbox

Set-Mailbox -Identity "John Doe" -Type Shared


# Verify conversion

Get-Mailbox -Identity "John Doe" | Format-Table
DisplayName,RecipientTypeDetails
```

✅ **Validation**

- The mailbox appears in Outlook/OWA under shared mailboxes.
- Users with permissions can **send and receive emails** from the shared mailbox.
- Verify members:

```
Get-MailboxPermission -Identity "John Doe" | Where-Object
{$_.AccessRights -eq "FullAccess"}
```

✅ **Best Practices**

- Convert only mailboxes that are no longer used for individual login.
- Add **all required members** immediately after conversion.
- Monitor mailbox size to ensure it stays under the license-free limit (50GB).
- Communicate with users about the new access and functionality.

✅ **Use Case**
A support team mailbox **support@contoso.com** was previously assigned to one user.

- Convert it to a shared mailbox.
- Assign all support team members as full-access users.
- Team members can now manage emails collectively without additional licenses.

---

22. Configure A Moderated Recipient in Exchange Online

✅ **Purpose**
A moderated recipient ensures that **emails sent to a specific mailbox or distribution group require approval** before delivery.

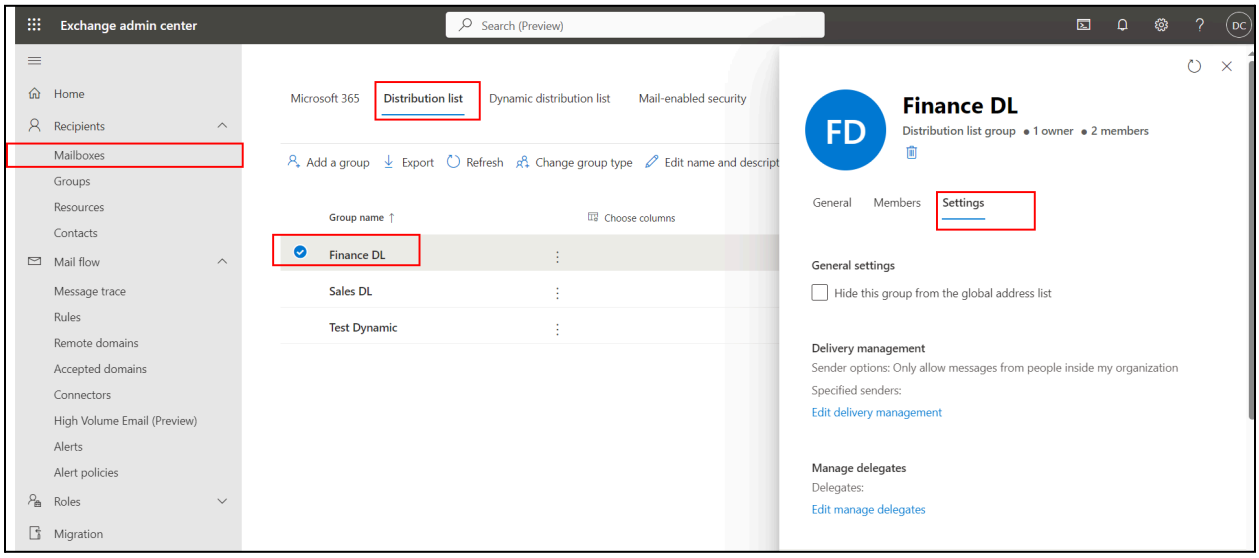
- Helps prevent **unauthorized or accidental emails** to sensitive groups.
- Ideal for departments handling confidential information (Finance, HR, Legal).
- Moderation can be applied to **user mailboxes, distribution groups, or shared mailboxes**.

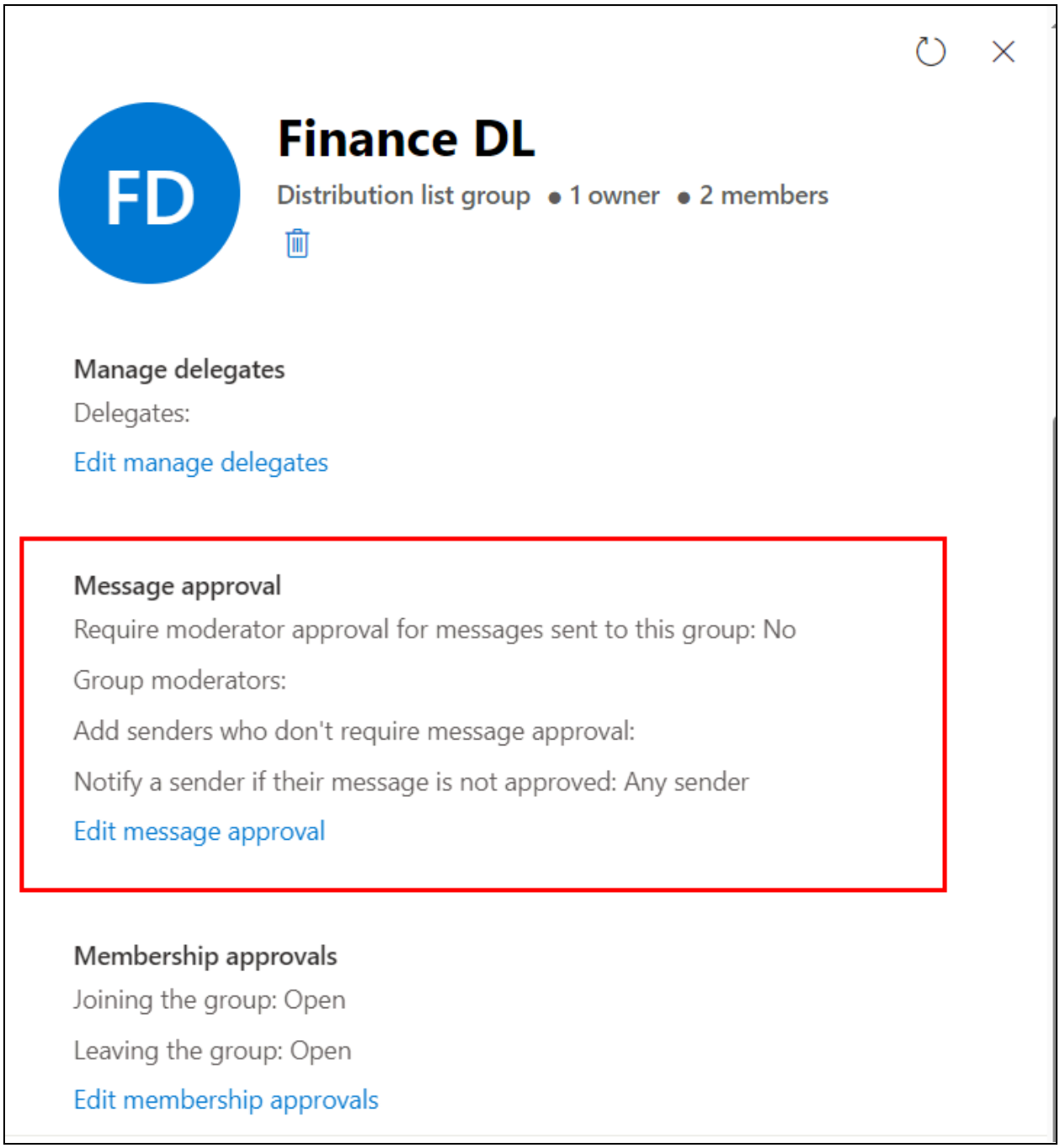
✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Go to https://admin.exchange.microsoft.com → Sign in as Global/Exchange Admin.
2. Navigate → **Recipients** → **Mailboxes or Groups**
3. Select the mailbox/group → **Mail flow settings** → **Message approval**
4. Enable **"Messages sent to this recipient must be approved by a moderator"**.
5. Assign one or more **moderators** who will approve or reject emails.
6. Configure notification settings (send notifications to sender upon approval/rejection).

7. Save changes.





PowerShell

```
# Connect to Exchange Online
```

```
Connect-ExchangeOnline


# Enable moderation for a distribution group

Set-DistributionGroup -Identity "FinanceDept" -ModerationEnabled $true
-ModeratedBy user1@contoso.com -SendModerationNotifications True


# Verify moderation settings

Get-DistributionGroup -Identity "FinanceDept" | Format-Table
DisplayName,ModerationEnabled,ModeratedBy
```

✅ **Validation**

- Send a test email to the moderated recipient.
- Moderator receives an approval request.
- Email is delivered to members **only after approval**.
- Check moderation logs or PowerShell to confirm approvals.

✅ **Best Practices**

- Assign **responsible and available moderators** to prevent delayed email delivery.
- Use moderation for **sensitive or high-volume mailboxes** only.
- Regularly review moderation settings and assigned moderators.
- Communicate with senders about moderated recipients to reduce confusion.

✅ **Use Case**

The Finance department wants to control emails sent to **FinanceDept@contoso.com**.

- Admin configures moderation with the department head as the moderator.

- All emails to the finance group are **approved by the head** before delivery, preventing accidental leaks of sensitive data.

---

23. Assign Full Access Permission on Other Mailboxes in Exchange Online

✅ **Purpose**
Full Access permission allows a user to **open and manage another mailbox** in Exchange Online.

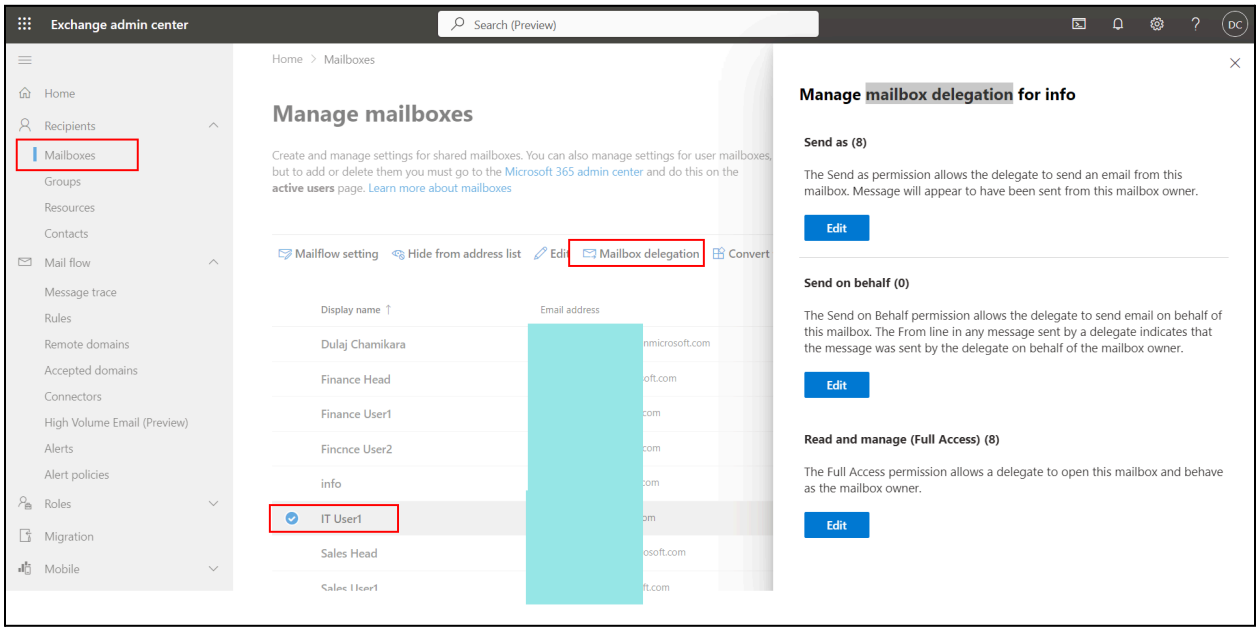
- Users can **read, reply, and organize emails** in the mailbox.
- Does **not** allow sending emails as the mailbox unless **Send As** or **Send on Behalf** permissions are granted.
- Useful for team members, assistants, or shared mail scenarios.

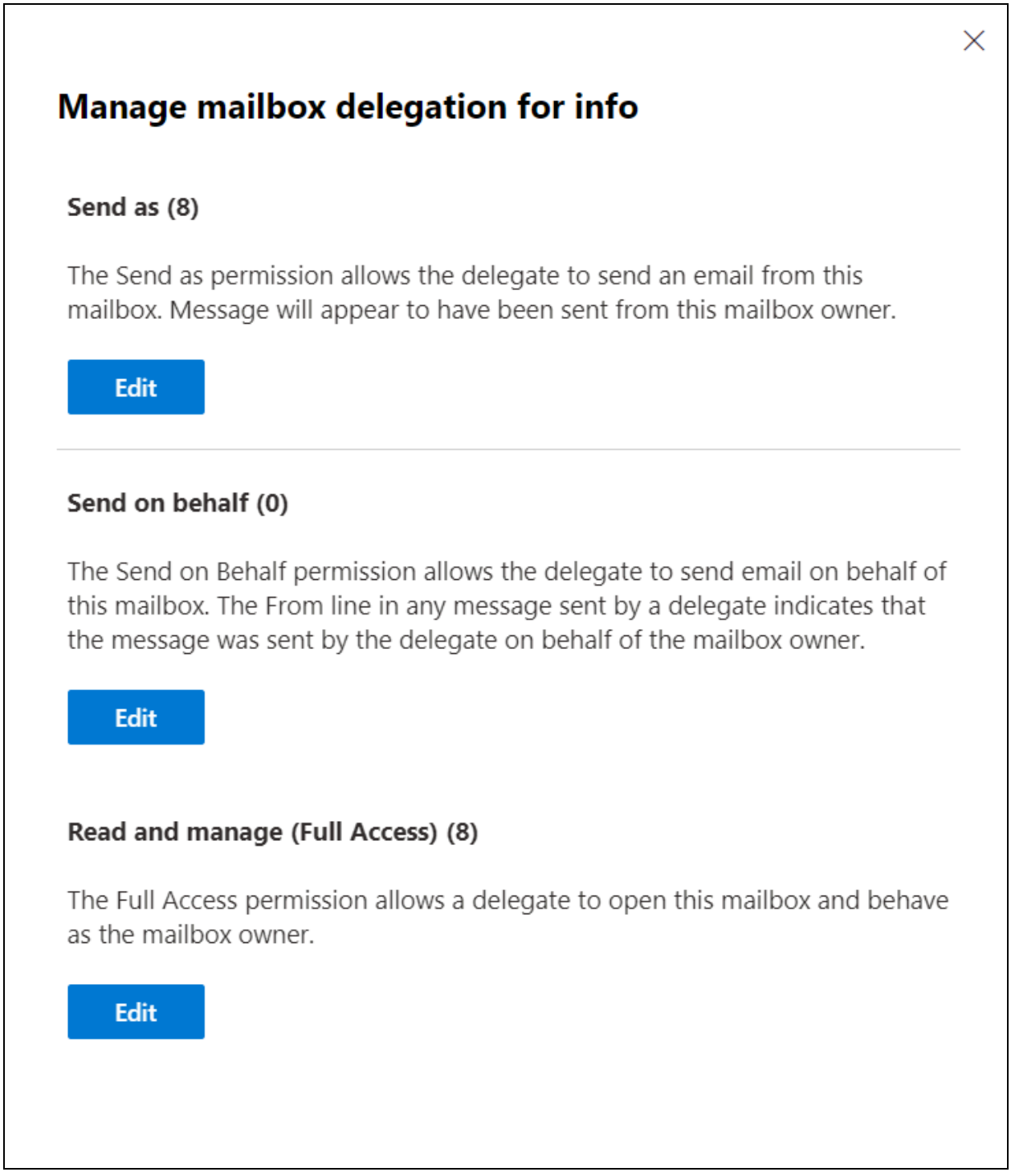
✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Go to https://admin.exchange.microsoft.com → Sign in as Global/Exchange Admin.
2. Navigate → **Recipients** → **Mailboxes**
3. Select the mailbox → **mailbox delegation** → **Full Access** → **Edit**

4. Add users who need Full Access permission → Save changes





PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline
```

```
# Assign Full Access permission

Add-MailboxPermission -Identity "SupportTeam" -User user1@contoso.com
-AccessRights FullAccess -InheritanceType All


# Verify permissions

Get-MailboxPermission -Identity "SupportTeam" | Where-Object {$_.User
-like "user1*"}
```

✅ **Validation**

- The assigned user can open the mailbox in Outlook or OWA.
- Test by reading and moving emails in the target mailbox.
- Verify using PowerShell to ensure proper permission assignment.

✅ **Best Practices**

- Assign Full Access **only to required users** to maintain security.
- Combine with **Send As** or **Send on Behalf** if the user needs to send emails from the mailbox.
- Regularly review mailbox permissions for inactive or departed users.
- Document permission changes for compliance purposes.

✅ **Use Case**

A support team mailbox **SupportTeam@contoso.com** needs to be managed by multiple staff members.

- Assign Full Access permission to all support agents.
- Agents can collectively handle incoming emails without requiring individual licenses for the mailbox.

---

24. Grant Send As Permission on Mailbox in Exchange Online

✅ Purpose

Send As permission allows a user to **send emails that appear as if they are sent directly from another mailbox**.

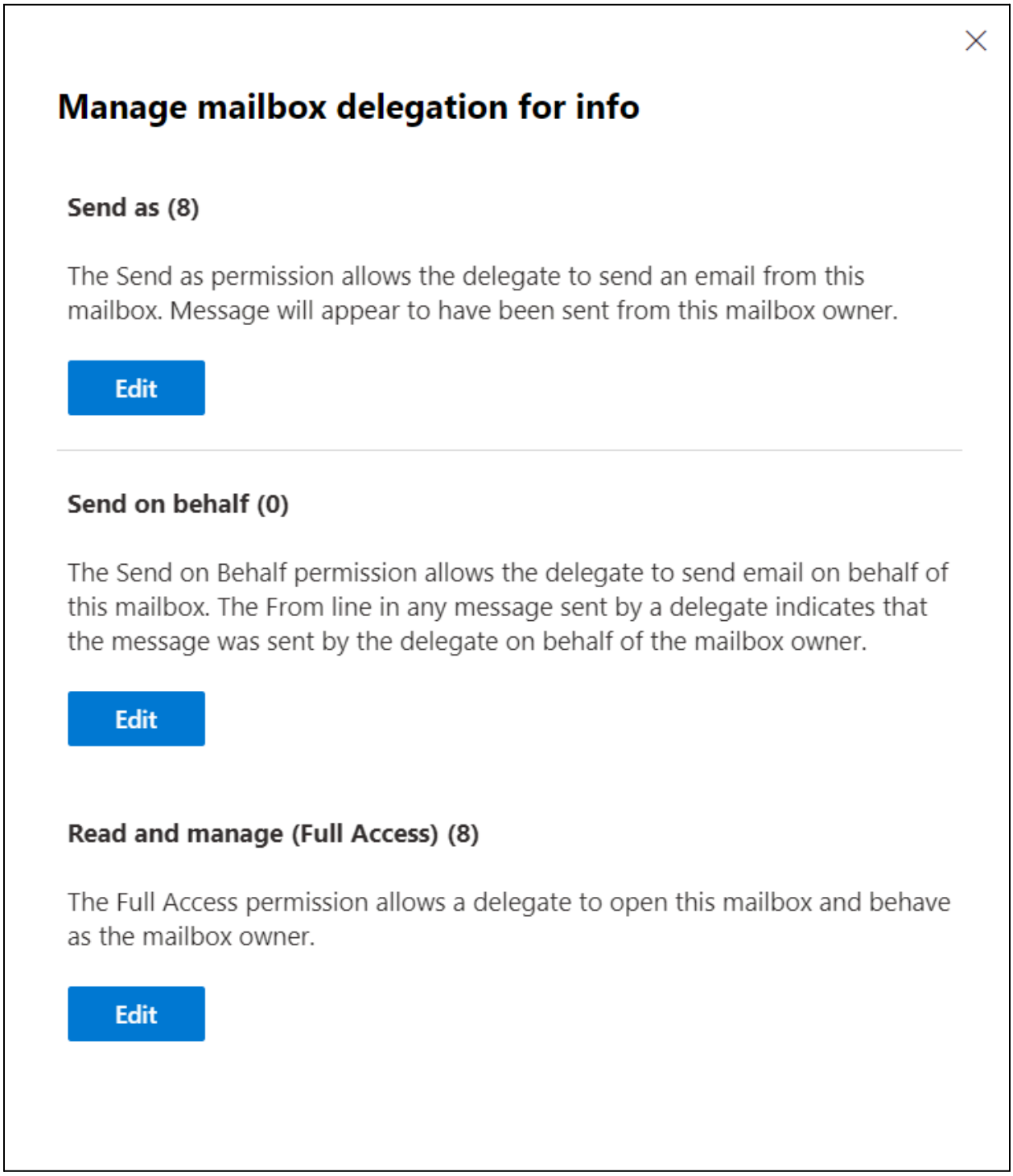
- The recipient sees the email **from the mailbox itself**, not from the delegator.
- Useful for **shared mailboxes, departmental mailboxes, or executive assistants**.
- Requires careful assignment to prevent misuse.

✅ Configuration Steps

Exchange Admin Center (EAC)

1. Go to https://admin.exchange.microsoft.com → Sign in as Global/Exchange Admin.
2. Navigate → **Recipients** → **Mailboxes**
3. Select the mailbox → **Mailbox permissions** → **Send As** → **Edit**

4. Add the user(s) who require **Send As** permissions → Save changes



PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline
```

```
# Grant Send As permission

Add-RecipientPermission -Identity "SupportTeam" -Trustee
user1@contoso.com -AccessRights SendAs


# Verify permission

Get-RecipientPermission -Identity "SupportTeam" | Where-Object
{$_.Trustee -like "user1*"}
```

✅ **Validation**

- Assigned user sends a test email → appears **from SupportTeam@contoso.com**.
- Verify in Outlook or OWA that the email **does not show the delegator's name**.
- Check permissions with PowerShell to confirm correct assignment.

✅ **Best Practices**

- Assign **only to trusted users**.
- Document who has Send As permission for auditing and compliance.
- Combine with Full Access permission if users need mailbox management.
- Periodically review Send As permissions to remove inactive or departed users.

✅ **Use Case**
A support team uses **SupportTeam@contoso.com**.

- Grant Send As permission to all agents.
- Agents can respond to customer emails directly as **SupportTeam**, maintaining a professional, unified communication identity.

---

25. Assign Send on Behalf Permission in Exchange Online

✅ **Purpose**

Send on Behalf permission allows a user to **send emails on behalf of another mailbox**.

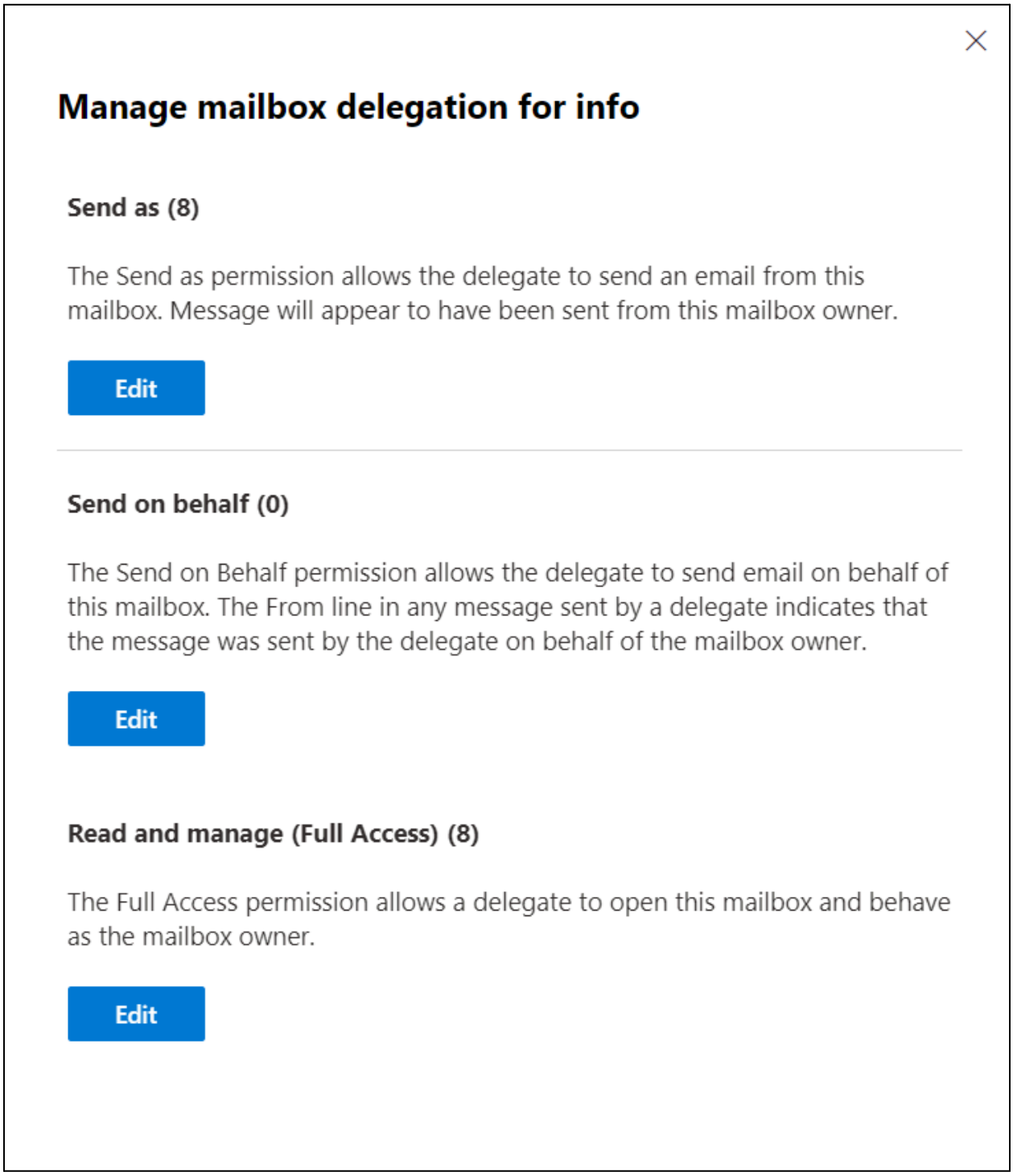
- The recipient sees the email as **"From: User on behalf of Mailbox"**.
- Useful for **assistants, team members, or delegated mail handling**.
- Unlike Send As, it clearly indicates **who sent the email**.

✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Go to https://admin.exchange.microsoft.com → Sign in as Global/Exchange Admin.
2. Navigate → **Recipients** → **Mailboxes**
3. Select the mailbox → **Mailbox delegation** → **Send on behalf** → **Edit**

4. Add the user(s) who should send on behalf → Save changes



PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline
```

```
# Assign Send on Behalf permission

Set-Mailbox -Identity "SupportTeam" -GrantSendOnBehalfTo
user1@contoso.com


# Verify permission

Get-Mailbox -Identity "SupportTeam" | Format-Table
DisplayName,GrantSendOnBehalfTo
```

✅ **Validation**

- Assigned user sends a test email → appears **From: user1 on behalf of SupportTeam**.
- Verify in Outlook or OWA that the delegation is applied correctly.
- Use PowerShell to confirm the delegated user list.

✅ **Best Practices**

- Assign **only to trusted delegates**.
- Document Send on Behalf assignments for compliance purposes.
- Use in scenarios where the recipient **must know the actual sender**.
- Combine with Full Access if the delegate also needs to manage mailbox content.

✅ **Use Case**

An executive assistant sends emails on behalf of the CEO from **CEO@contoso.com**.

- Recipient sees **“From: Assistant on behalf of CEO”**, maintaining transparency while delegating communication.

---

26. Add Recovery Email Address and Phone Number for Office 365 Admin

✅ Purpose

Adding recovery information ensures **account security and recovery options** for Office 365 admins.

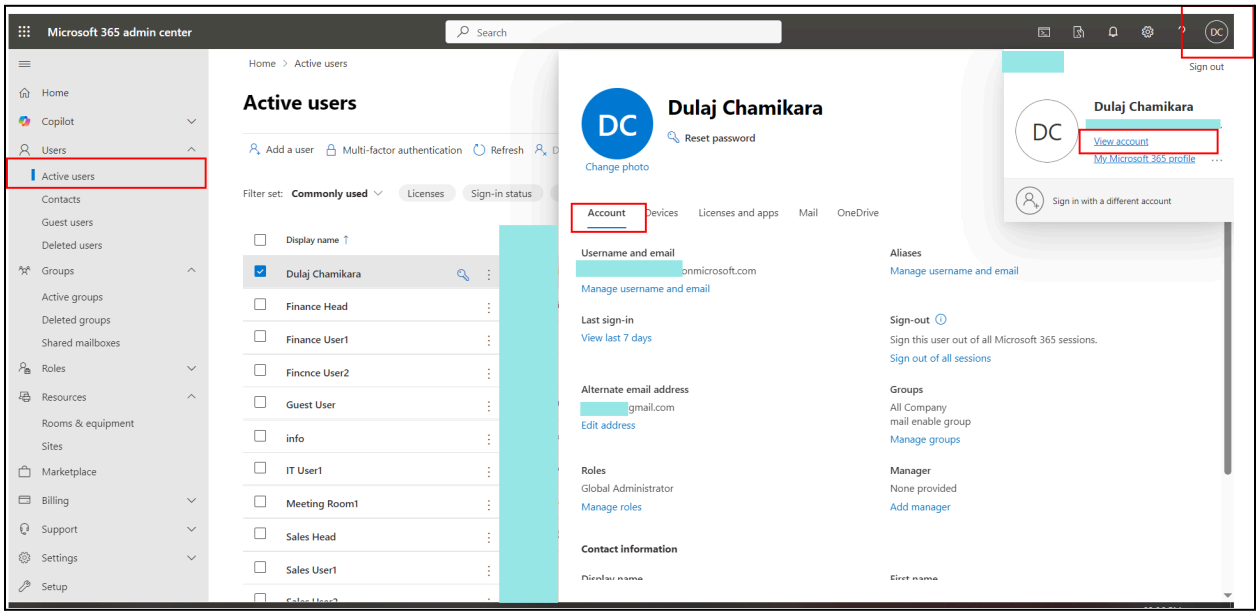
- Allows admins to **reset passwords** or recover accounts in case of lockout or multi-factor authentication (MFA) issues.
- Helps maintain **business continuity** and prevents downtime due to inaccessible admin accounts.

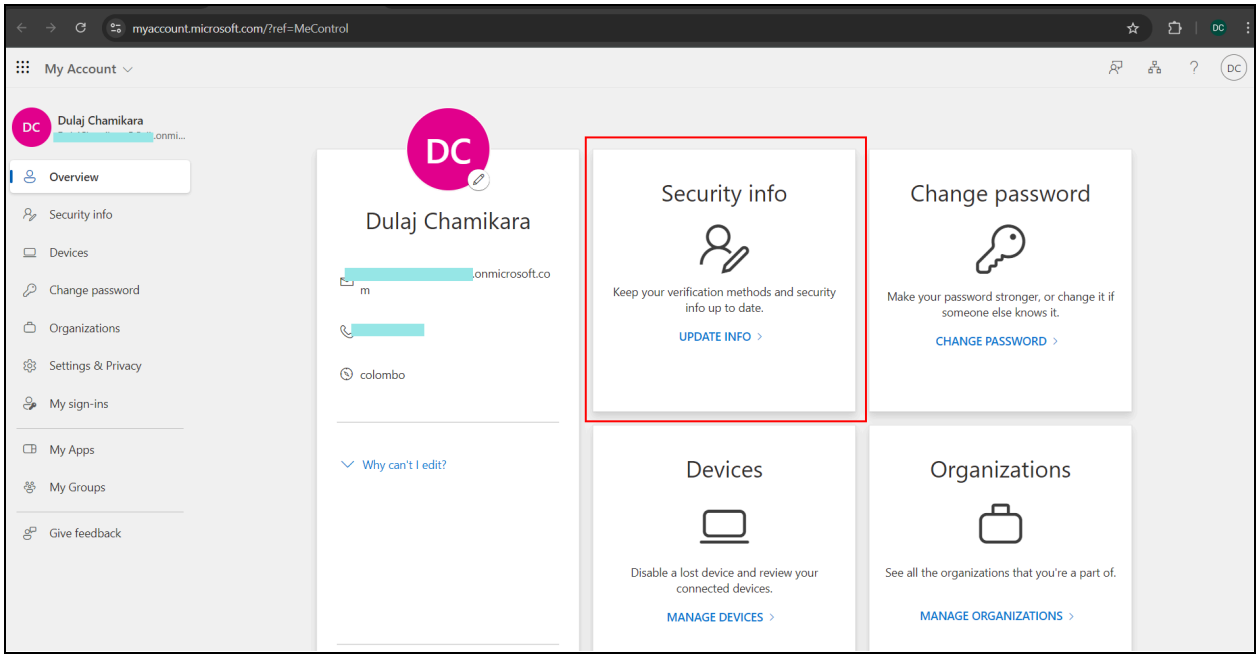
✅ Configuration Steps

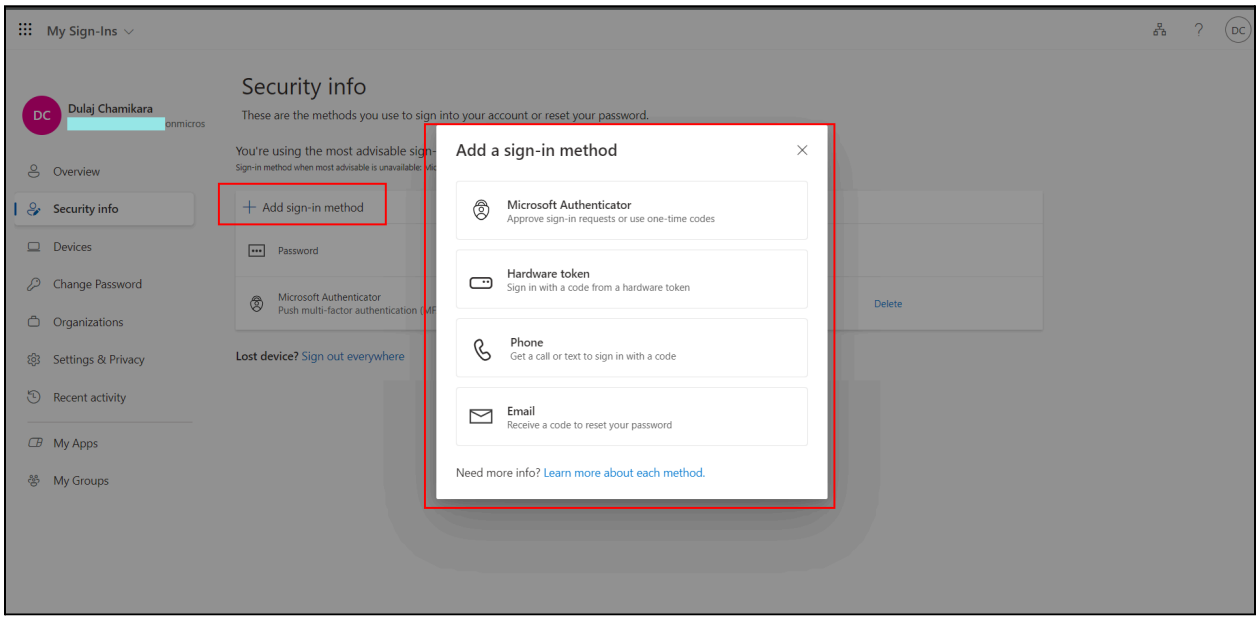
Microsoft 365 Admin Center

1. Sign in to https://admin.microsoft.com using your admin credentials.
2. Click on your **profile picture** → **View Account** → **Security info**.
3. Click **Add method** → **Choose Email or Phone**.
4. Enter the **recovery email address or phone number**.
5. Verify the method by entering the code sent to your email or phone.

6. Save changes.

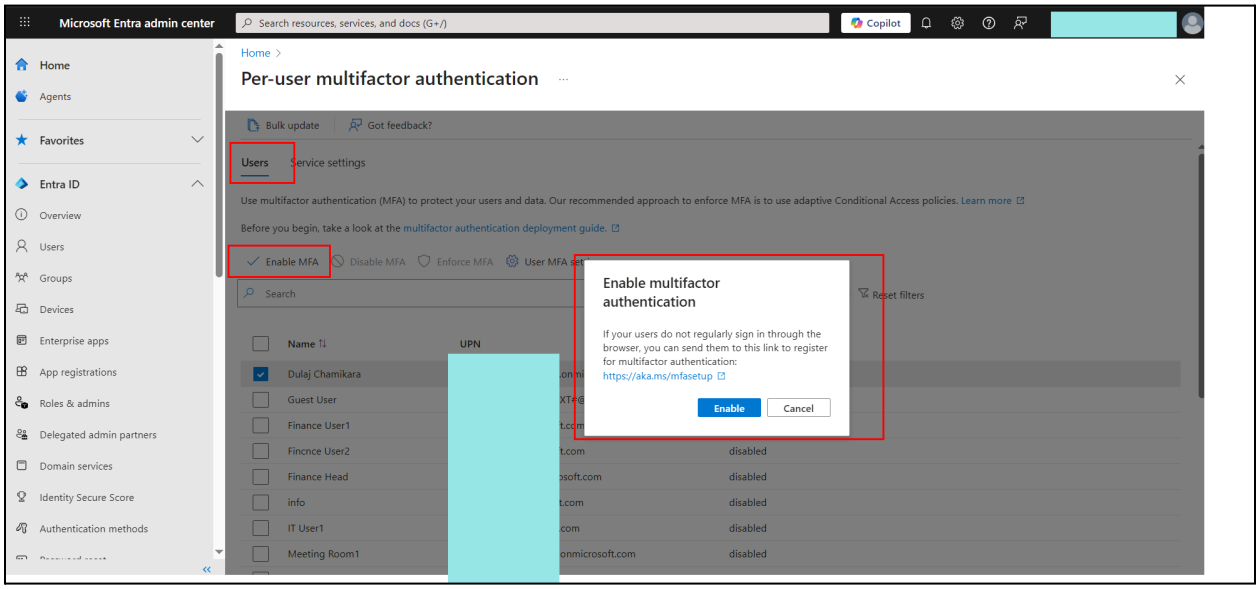






Azure AD (Alternative via PowerShell / Portal)

- Admins can also manage recovery info using the **Azure Active Directory portal → Users → Security info**.



✅ Validation

- Sign out and attempt password recovery → the recovery email or phone should receive a verification code.
- Verify the recovery info appears in the **Security info** section of the admin account.

✅ Best Practices

- Use a **personal email/phone** separate from corporate accounts for recovery.
- Keep recovery methods **up-to-date** for current contact info.
- Enable **multi-factor authentication (MFA)** for all admin accounts in addition to recovery info.
- Review recovery info periodically to ensure accuracy.

✅ Use Case

The Office 365 global admin account is locked out due to MFA issues.

- Recovery phone and email allow immediate account recovery without contacting Microsoft Support.

- Ensures continuity of administrative tasks such as user management and license assignment.

---

27. Set up Multi-factor Authentication (MFA) for Office 365 Users

✅ Purpose

Multi-factor authentication (MFA) adds an **extra layer of security** by requiring users to provide **two or more verification methods**.

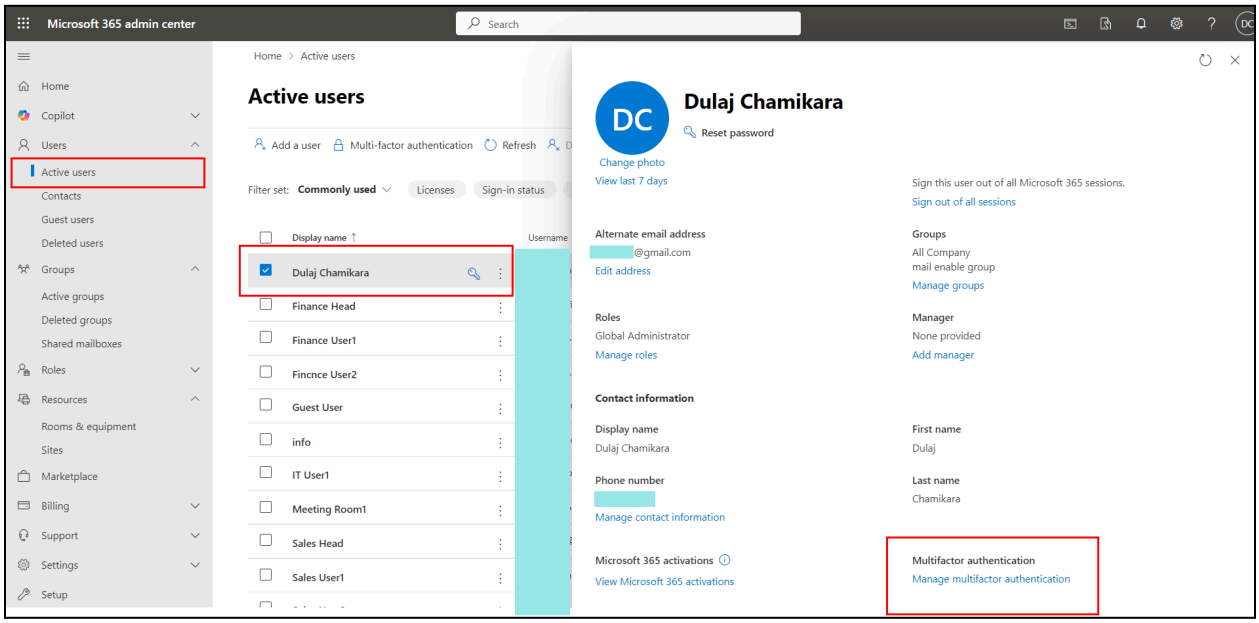
- Protects accounts from unauthorized access even if passwords are compromised.
- Recommended for all users, especially admins and employees with sensitive data access.
- Helps organizations meet **security and compliance requirements**.

✅ Configuration Steps

Microsoft 365 Admin Center

1. Sign in to https://admin.microsoft.com as a Global Admin.
2. Navigate → **Users** → **Active users**.
3. Click **Multi-factor authentication** under **More settings**.
4. Select users to enable MFA → Click **Enable** → Confirm.

5. Users receive a prompt to configure MFA the next time they sign in.



User Setup Steps (for end users)

1. Sign in to https://aka.ms/mfasetup.
2. Choose a verification method:
    - Authentication app (Microsoft Authenticator)
    - Phone call
    - SMS text message
3. Follow prompts to verify and complete setup.

PowerShell (Optional)

```
# Connect to MSOnline

Connect-MsolService


# View MFA status for users
```

```
Get-MsolUser | Select
DisplayName,UserPrincipalName,StrongAuthenticationRequirements


# Enable MFA for a specific user

Set-MsolUser -UserPrincipalName user1@contoso.com
-StrongAuthenticationRequirements
@(@{RelyingParty="*";State="Enabled"})
```

✅ **Validation**

- Users are prompted for a second verification method at the next login.
- Test login with MFA to ensure verification is required.
- Check the admin portal to confirm status as **Enabled** or **Enforced**.

✅ **Best Practices**

- Enforce MFA for **all admins and sensitive roles**.
- Encourage use of the **Microsoft Authenticator app** for convenience and security.
- Educate users about **phishing attacks** and safe MFA practices.
- Combine with recovery email/phone for account recovery.
- Regularly review MFA status for compliance and security auditing.

✅ **Use Case**
A company secures all Office 365 accounts with MFA.

- Even if a user's password is stolen, unauthorized access is prevented.
- Admin accounts have additional protection, reducing the risk of data breaches.

---

28. Setup a Litigation Hold on a Mailbox in Exchange Online

✅ Purpose

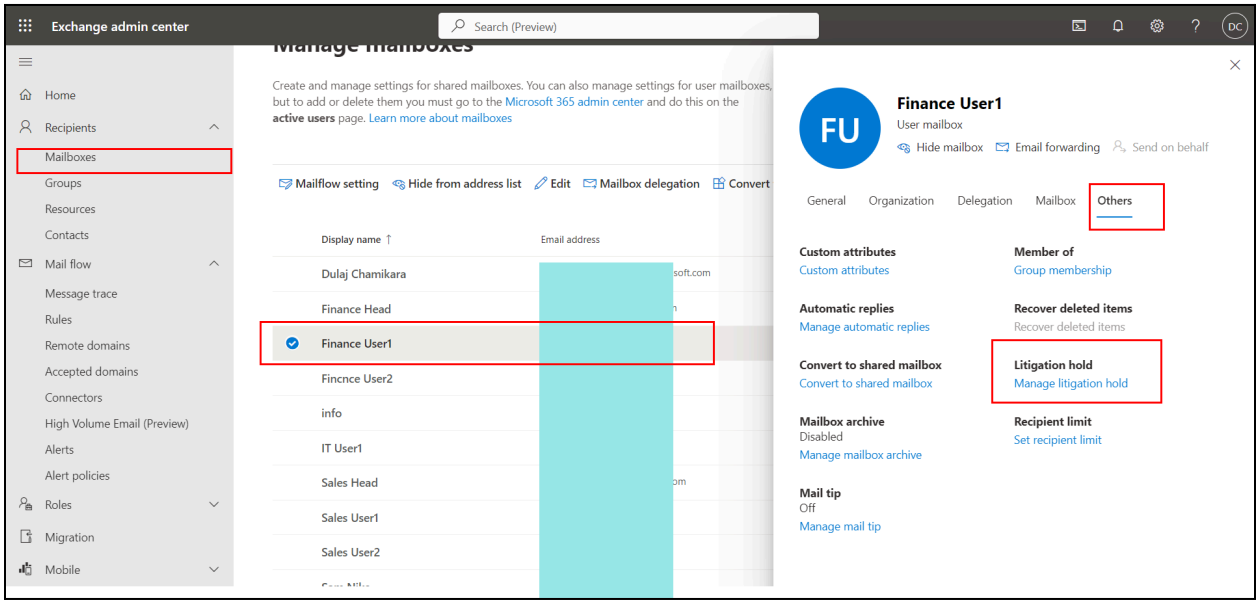
A **Litigation Hold** preserves all mailbox content to meet **legal or compliance requirements**.

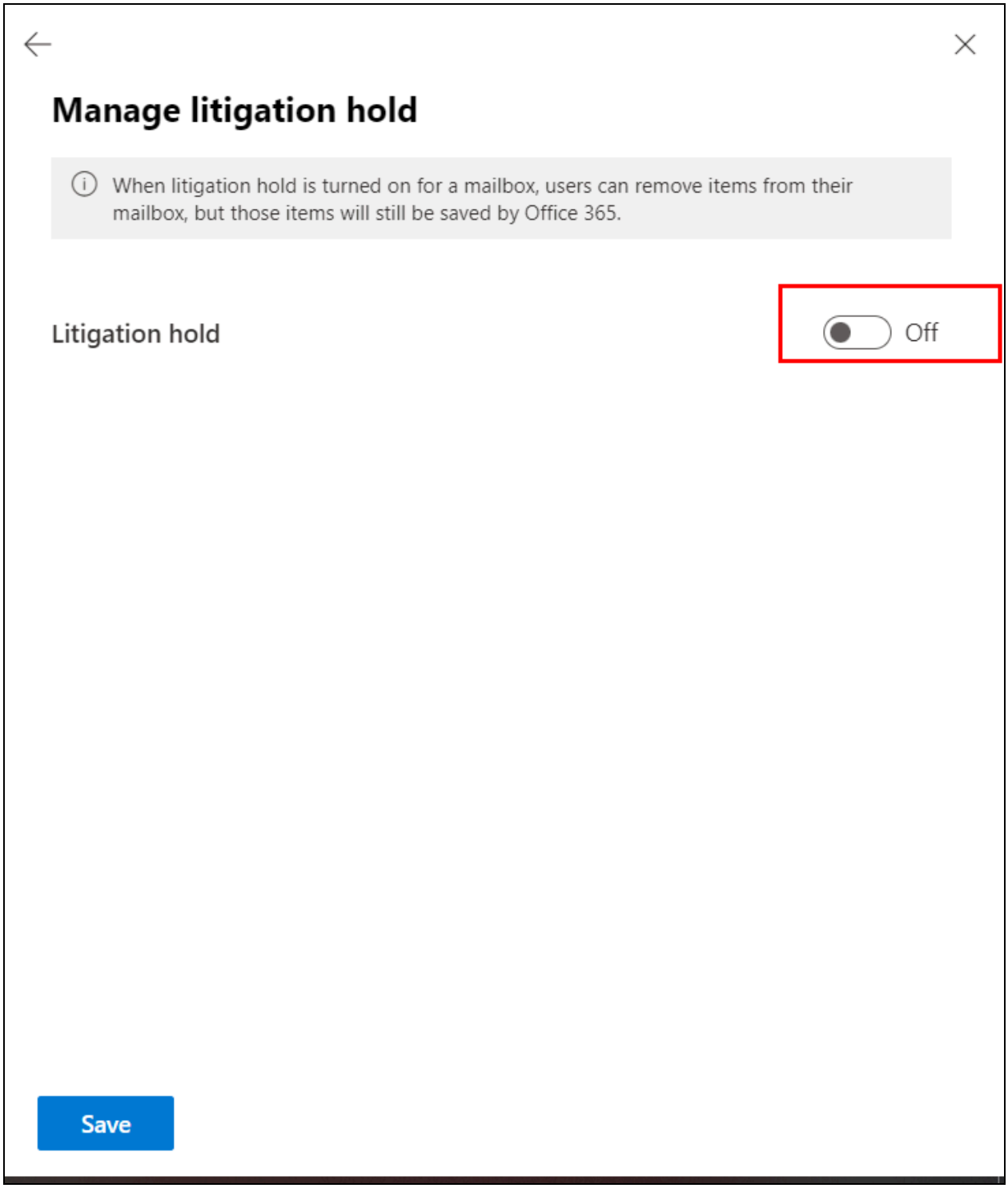
- Ensures that emails, calendar items, and other mailbox data **cannot be permanently deleted** by the user.
- Critical for **legal investigations, audits, or regulatory compliance**.
- Can be applied to **user mailboxes or shared mailboxes**.

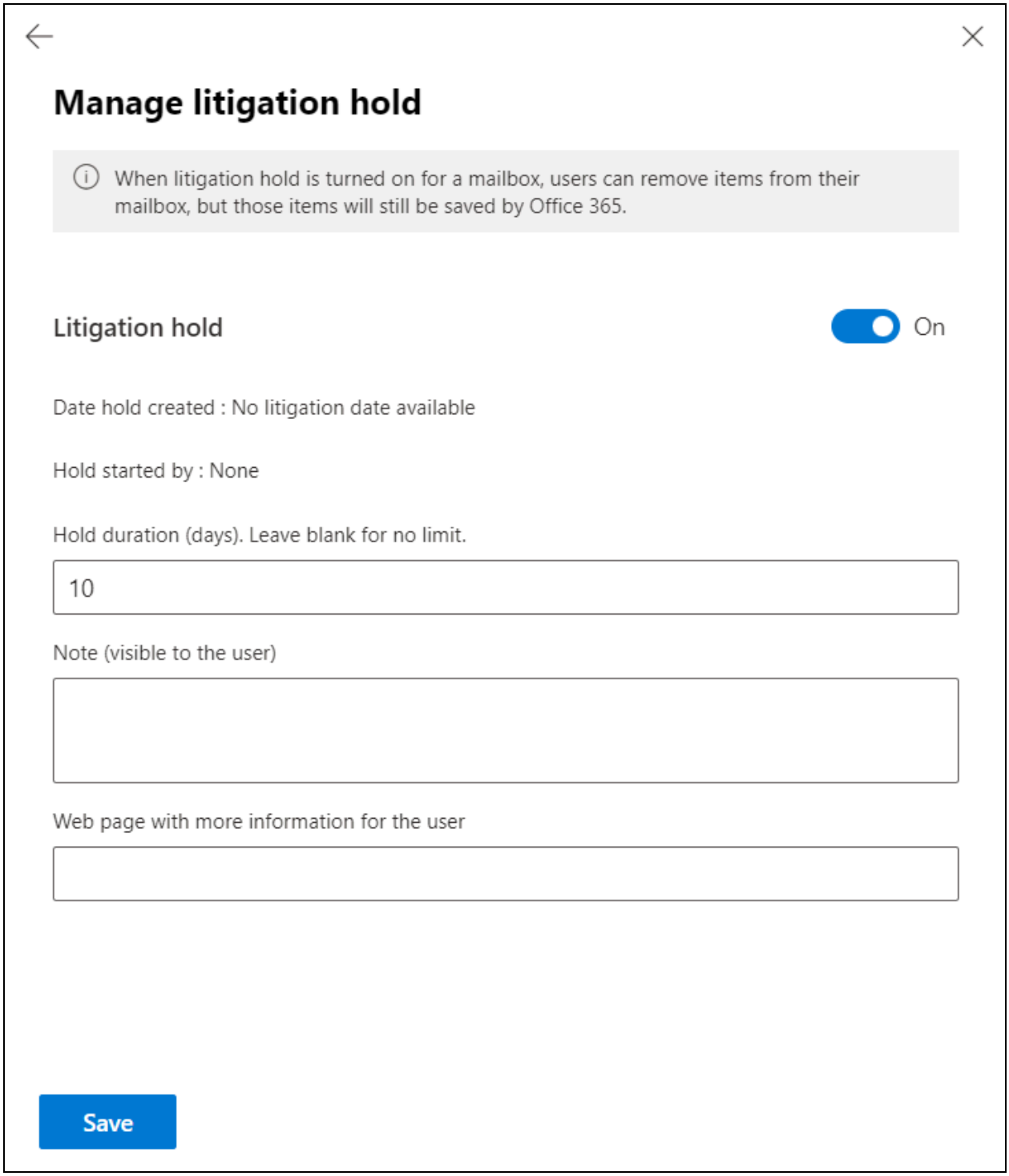
✅ Configuration Steps

Microsoft Exchange Admin Center (EAC)

1. Sign in to https://admin.exchange.microsoft.com as Global/Exchange Admin.
2. Navigate → **Recipients** → **Mailboxes**
3. Select the mailbox → **Others** → **Litigation hold**
4. Enable **Litigation hold**.
5. Specify optional **hold duration** (in days) or leave blank for indefinite retention.
6. Save changes.




Manage litigation hold
When litigation hold is turned on for a mailbox, users can remove items from their mailbox, but those items will still be saved by Office 365.
Litigation hold
Off
Save



PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline
```

```
# Enable Litigation Hold on a mailbox for 365 days

Set-Mailbox -Identity "John Doe" -LitigationHoldEnabled $true
-LitigationHoldDuration 365


# Verify status

Get-Mailbox -Identity "John Doe" | Format-Table
DisplayName,LitigationHoldEnabled,LitigationHoldDuration
```

✅ **Validation**

- Mailbox shows **LitigationHoldEnabled = True**.
- Test by attempting to delete items → items are preserved.
- Ensure that all mailbox content remains accessible to **compliance officers or administrators**.

✅ **Best Practices**

- Apply Litigation Hold only to **mailboxes under legal or compliance requirements** to manage storage efficiently.
- Document holds policies and durations for audit purposes.
- Combine with **archiving and retention policies** for comprehensive compliance management.
- Monitor mailbox size; holds may increase storage requirements.

✅ **Use Case**

An executive mailbox **John.Doe@contoso.com** is under investigation.

- Admin places a Litigation Hold for 365 days.

- All emails, calendar events, and deleted items are preserved.
- Ensures compliance and legal requirements without affecting normal mailbox usage.

---

29. How to Setup Archiving for a Mailbox in Exchange Online

✅ **Purpose**
Mailbox archiving allows users to **store older or less frequently accessed emails** in a separate archive mailbox.

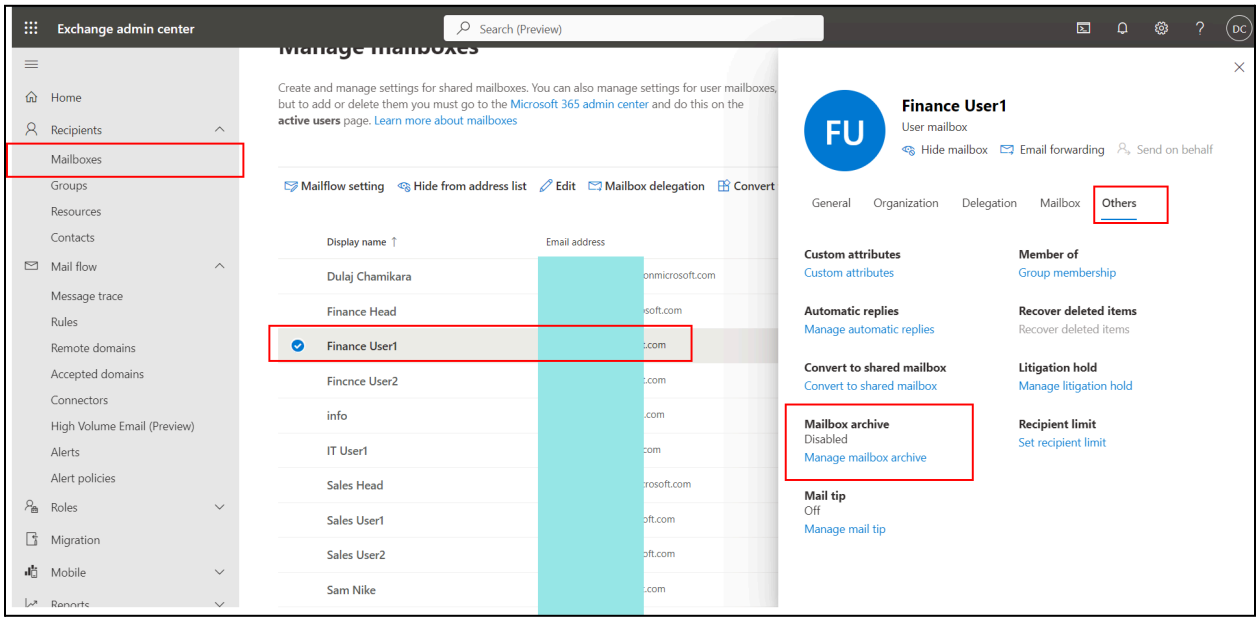
- Helps **reduce primary mailbox size** and maintain performance.
- Retains emails for **compliance or organizational policies**.
- Can be combined with **retention policies** to automatically move emails to archive.

✅ **Configuration Steps**

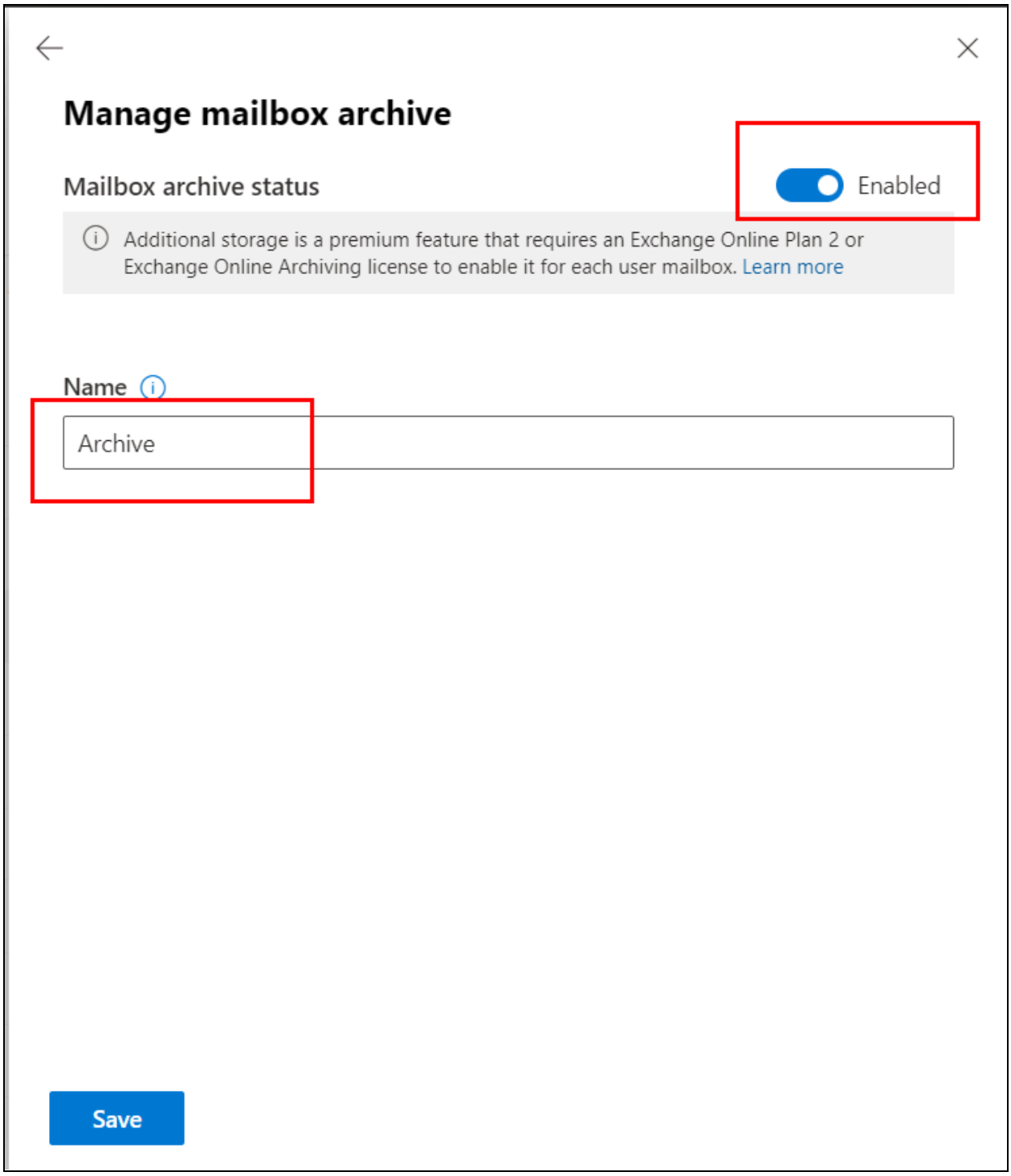
Microsoft 365 Admin Center (EAC)

1. Sign in to https://admin.exchange.microsoft.com as Global/Exchange Admin.
2. Navigate → **Recipients** → **Mailboxes**
3. Select the mailbox → **Mailbox features** → **Archive** → **Enable**

4. Save changes → Archive mailbox is created.




Manage mailbox archive
Mailbox archive status
Disabled
Save



PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline
```

```
# Enable archive mailbox for a user

Enable-Mailbox -Identity "John Doe" -Archive


# Verify archive status

Get-Mailbox -Identity "John Doe" | Format-Table
DisplayName,ArchiveStatus
```

✅ **Validation**

- The archive mailbox appears in **Outlook** and **OWA** under the user's mailbox.
- Test by moving an email to the archive → email appears in the archive folder.
- Verify with PowerShell:

```
Get-Mailbox -Identity "John Doe" | Select DisplayName,ArchiveStatus
```

✅ **Best Practices**

- Enable archive for **users with large mailboxes** or compliance requirements.
- Combine with **retention policies** to automate email movement.
- Communicate to users about archive mailbox usage.
- Monitor archive mailbox size and growth.

✅ **Use Case**
A finance employee's mailbox is nearing its storage limit.

- Admin enables archive mailbox for **John.Doe@contoso.com**.

- Older emails are moved to archive → primary mailbox performance improves while retaining historical emails.

---

30. Create and Publish Retention Labels in Exchange Online

✅ **Purpose**
Retention labels help **classify, retain, or delete emails and documents** based on organizational or compliance policies.

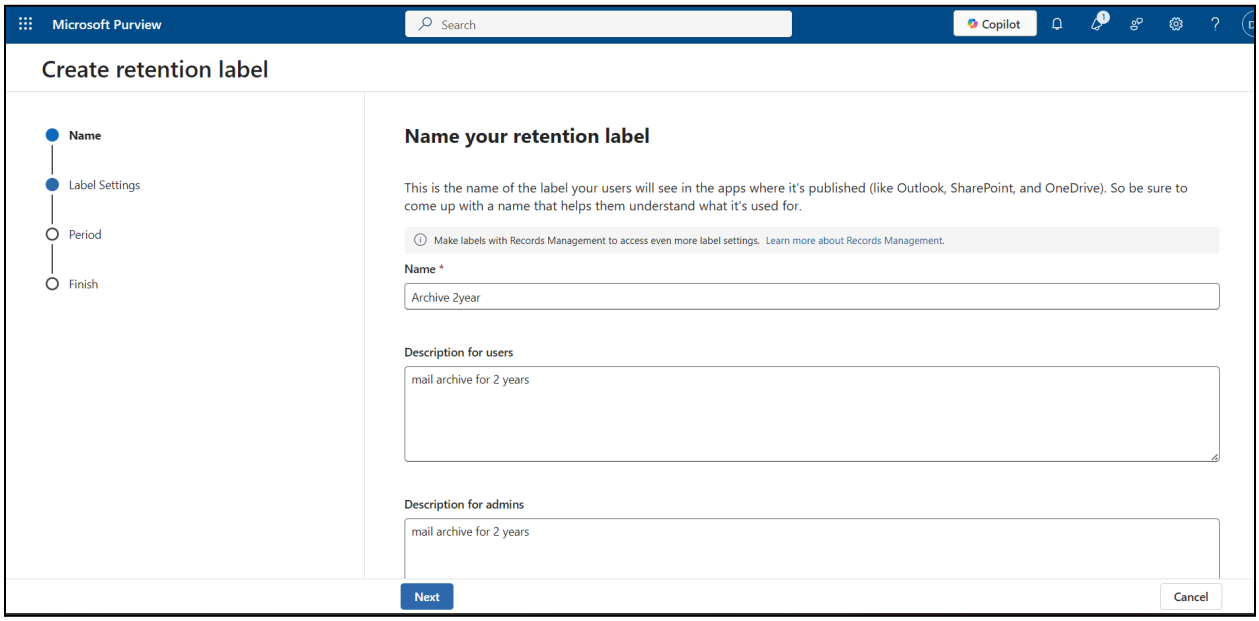
- Supports **information governance** and regulatory compliance.
- Automates **retention or deletion** of content across mailboxes, SharePoint, and Teams.
- Can be applied **manually by users** or **automatically via policies**.

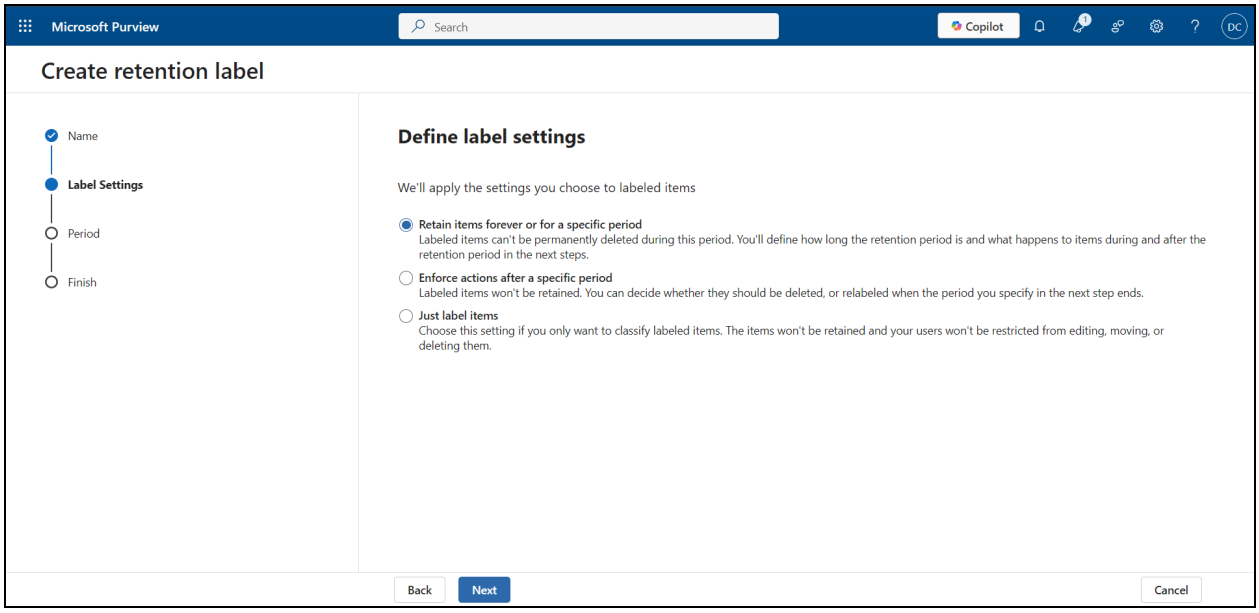
✅ **Configuration Steps**

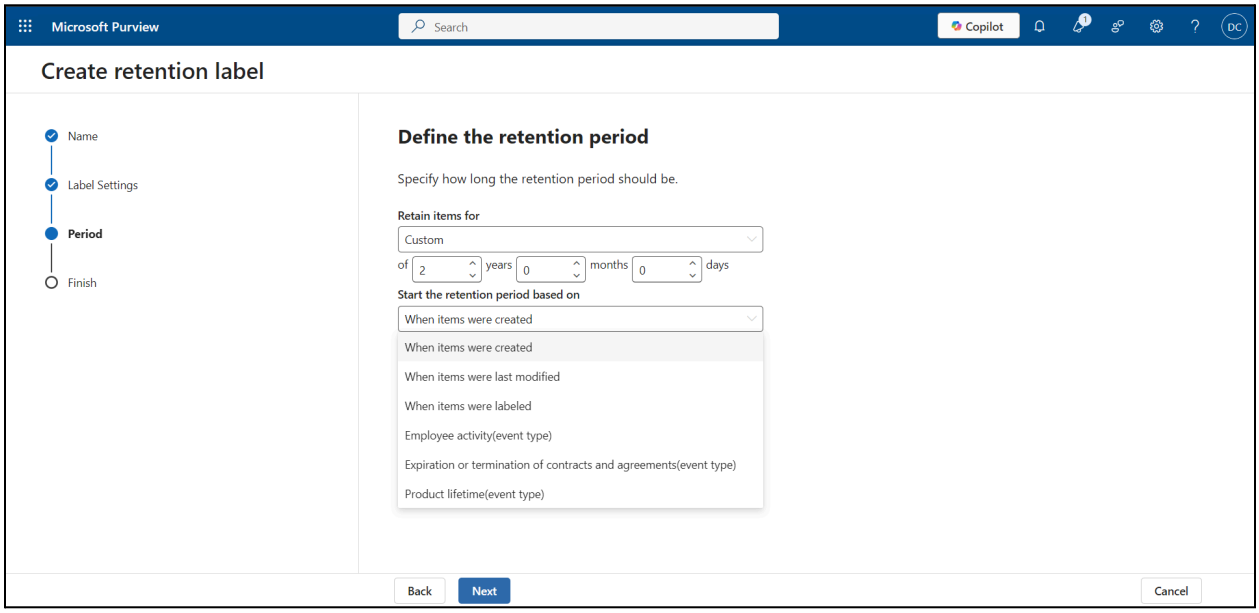
Microsoft Purview Compliance Center

1. Sign in to https://compliance.microsoft.com as Compliance Admin.
2. Navigate → **Data governance →Data LifecycleManagement→ Retention Labels → Create label**
3. Configure label settings:
    - **Name** and description
    - **Retention action**: retain, delete, or trigger a review
    - **Retention period**: number of days, months, or years

4. Save the label.







Publish the Retention Label

1. Navigate → **Label policies → Publish labels**
2. Select the label(s) to publish.
3. Choose **users, groups, or sites** where the label applies.
4. Save and publish → Users can now apply the label to content.

PowerShell (Optional)

```
# Connect to Security & Compliance Center

Connect-IPPSSession


# Create a retention label

New-RetentionCompliancePolicy -Name "Finance 7-Year Retention"
-SharePointLocation All -ExchangeLocation All -RetentionDuration 2555
-RetentionAction Delete


# Publish the policy

Start-RetentionCompliancePolicyRun -Identity "Finance 7-Year
Retention"
```

✅ **Validation**

- Users can see the label in **Outlook, SharePoint, or Teams**.
- Apply label to an email/document → verify retention or deletion behavior.
- Check **compliance reports** for labeled items.

✅ **Best Practices**

- Use clear, descriptive **label names** for easy identification.
- Align retention periods with **legal and organizational requirements**.
- Combine labels with **retention policies** for automated enforcement.
- Regularly review and update labels as policies change.
- Educate users on the purpose and usage of labels to ensure compliance.

✅ **Use Case**
Finance department emails must be retained for **7 years**.

- Admin creates a retention label **“Finance 7-Year Retention”**.
- Label is published to finance users → applied automatically or manually.
- Emails older than 7 years are automatically deleted, ensuring compliance with retention regulations.

---

31. Disable POP and IMAP for All Mailboxes in Exchange Online

✅ **Purpose**
Disabling POP and IMAP enhances **email security** and ensures users access mail via **modern protocols** (Exchange Online, Outlook, or OWA).

- POP and IMAP are older protocols with **limited security features**.
- Prevents users from bypassing **Exchange Online policies** and MFA.
- Helps enforce **organization-wide security compliance**.

✅ **Configuration Steps**

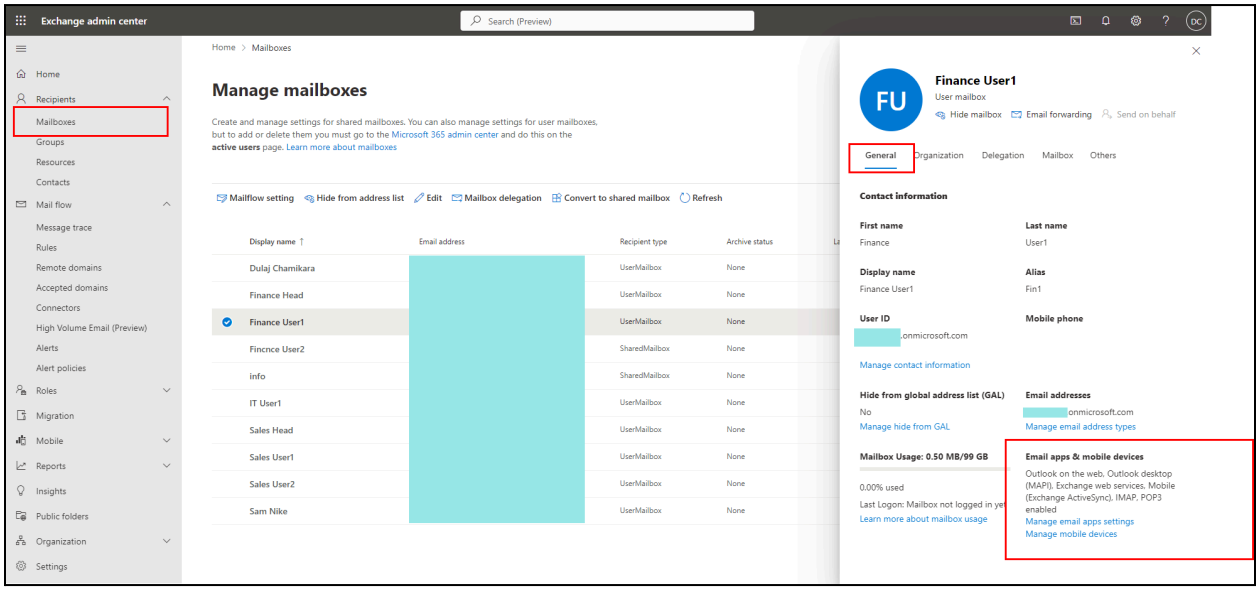
PowerShell (Recommended for bulk changes)

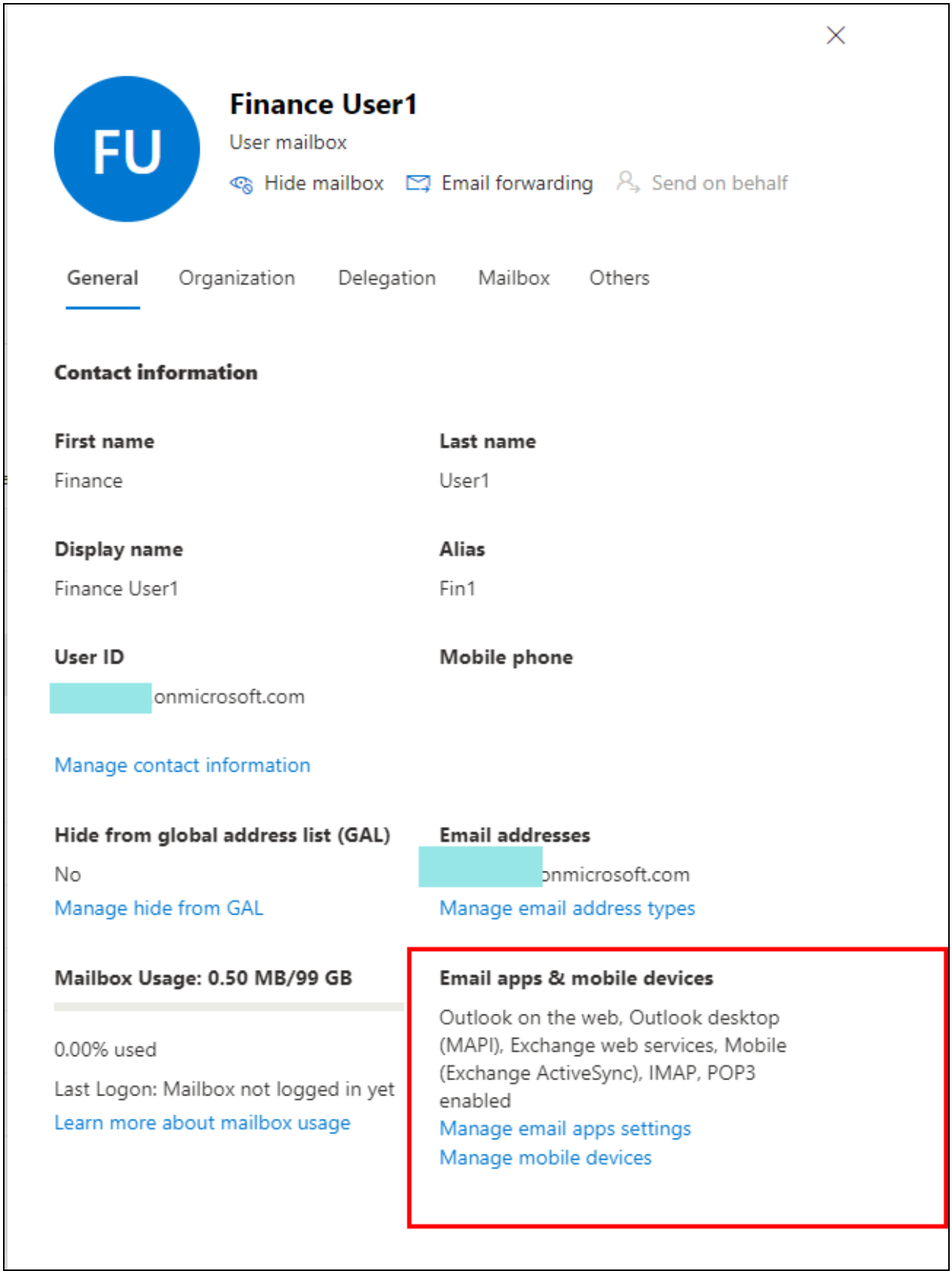
```
# Connect to Exchange Online

Connect-ExchangeOnline


# Disable POP for all mailboxes

Get-CASMailbox -ResultSize Unlimited | Set-CASMailbox -PopEnabled
$false


# Disable IMAP for all mailboxes

Get-CASMailbox -ResultSize Unlimited | Set-CASMailbox -ImapEnabled
$false
```

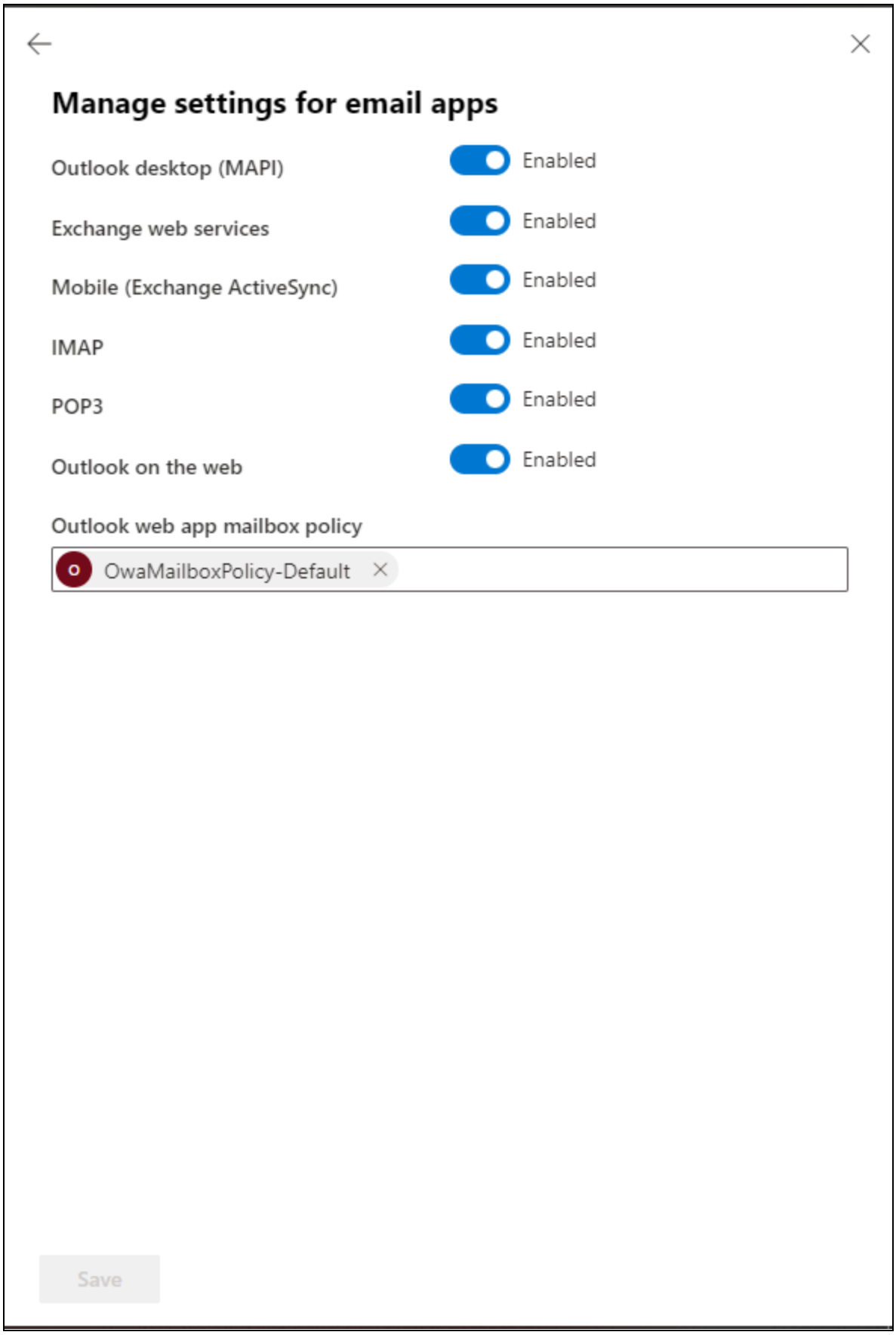
```
# Verify settings for a mailbox

Get-CASMailbox -Identity "user1@contoso.com" | Format-Table
Name,PopEnabled,ImapEnabled
```

Exchange Admin Center (EAC) – Individual Mailbox

1. Sign in to https://admin.exchange.microsoft.com as Global/Exchange Admin.
2. Navigate → **Recipients** → **Mailboxes**
3. Select a mailbox → **Mailbox features** → **POP/IMAP**
4. Toggle **POP and IMAP to Disabled** → Save changes.




FU
Finance User1
User mailbox
Hide mailbox
Email forwarding
Send on behalf
General
Organization
Delegation
Mailbox
Others
Contact information
First name
Finance
Last name
User1
Display name
Finance User1
Alias
Fin1
User ID
onmicrosoft.com
Mobile phone
Manage contact information
Hide from global address list (GAL)
No
Manage hide from GAL
Email addresses
onmicrosoft.com
Manage email address types
Mailbox Usage: 0.50 MB/99 GB
0.00% used
Last Logon: Mailbox not logged in yet
Learn more about mailbox usage
Email apps & mobile devices
Outlook on the web, Outlook desktop (MAPI), Exchange web services, Mobile (Exchange ActiveSync), IMAP, POP3 enabled
Manage email apps settings
Manage mobile devices


Manage settings for email apps
Outlook desktop (MAPI)
Enabled
Exchange web services
Enabled
Mobile (Exchange ActiveSync)
Enabled
IMAP
Enabled
POP3
Enabled
Outlook on the web
Enabled
Outlook web app mailbox policy
OwaMailboxPolicy-Default
Save

✅ **Validation**

- Attempt to connect via POP/IMAP → connection should fail.
- Use PowerShell to verify that `PopEnabled` and `ImapEnabled` are **False** for all mailboxes.
- Test mail access via Outlook, OWA, or mobile apps to ensure continued connectivity.

✅ **Best Practices**

- Disable POP and IMAP organization-wide to enforce modern authentication.
- Inform users about the change and provide guidance for Outlook or OWA access.
- Combine with **MFA** and **Conditional Access policies** for enhanced security.
- Regularly review mailbox protocol settings to prevent unauthorized access.

✅ **Use Case**
An organization wants to **prevent unsecured email access**.

- Admin disables POP and IMAP for all mailboxes.
- Users are required to access mail through Outlook or OWA, ensuring **MFA and security policies** are enforced.

---

32. How to Setup Password Expiration Policy in Microsoft 365

✅ **Purpose**
A password expiration policy enforces **regular password changes** to enhance account security.

- Helps reduce the risk of **compromised credentials**.
- Supports **compliance requirements** for sensitive systems.

- Can be applied to all users or specific groups in Microsoft 365.

✅ Configuration Steps

Microsoft 365 Admin Center (Modern Method via Azure AD)

1. Sign in to https://portal.azure.com as Global Admin.
2. Navigate → **Azure Active Directory** → **Security** → **Authentication methods** → **Password protection**.
3. Configure **password expiration policy**:
    - **Days before password expires** (default: 90 days)
    - **Notification period** before expiration (default: 14 days)
4. Save settings → Policy applies to selected users or all users.

PowerShell (MSOnline Module)

```
# Connect to Microsoft 365

Connect-MsolService


# Enable password expiration

Set-MsolUser -UserPrincipalName user1@contoso.com
-PasswordNeverExpires $false


# Set organization-wide password expiration policy

Set-MsolPasswordPolicy -ValidityPeriod 90 -NotificationDays 14
-DomainName contoso.com


# Verify policy
```

```
Get-MsolPasswordPolicy -DomainName contoso.com
```

✅ **Validation**

- Users receive **password expiration notifications** X days before expiry.
- Test by setting a short expiration period for a test user → verify notification is received.
- Check Azure AD or PowerShell to ensure policy is applied.

✅ **Best Practices**

- Enforce a reasonable password rotation period (e.g., 60–90 days).
- Combine with **multi-factor authentication (MFA)** to strengthen security.
- Educate users on creating **strong, unique passwords**.
- Review password policies periodically for compliance with organizational standards.

✅ **Use Case**
An organization requires employees to **update passwords every 90 days**.

- Admin sets up a password expiration policy in Azure AD.
- Employees are notified 14 days prior → new passwords required upon next login.
- Ensures accounts remain secure and meets internal compliance requirements.

---

33. How to Create a Shared Calendar in Microsoft 365

✅ **Purpose**
A shared calendar enables **collaborative scheduling and visibility** across teams or departments.

- Allows team members to **view, edit, and manage events** in a common calendar.

- Reduces scheduling conflicts and improves **team coordination**.
- Can be shared with **internal users, external users, or specific groups**.

✅ Configuration Steps

Outlook on Web (OWA)

1. Sign in to https://outlook.office.com.
2. Navigate → **Calendar** → **Add calendar** → **Create new calendar**.
3. Enter **calendar name** (e.g., Team Meetings).
4. Click **Share** → Add users or groups → Assign permissions:
    - **Can view all details**
    - **Can edit**
5. Save changes → Shared calendar appears in all members' Outlook calendars.

Outlook Desktop App

1. Open Outlook → **Calendar view**.
2. Click **Home** → **Open Calendar** → **Create New Blank Calendar**.
3. Name the calendar → Right-click → **Share** → **Share Calendar**.
4. Enter users or groups → Assign permission level → Send invitation.

PowerShell (Optional – Mailbox Calendar Sharing)

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Grant calendar sharing permissions
```

```
Set-MailboxFolderPermission -Identity "JohnDoe@contoso.com:\Calendar"
-User "TeamMember@contoso.com" -AccessRights Editor


# Verify permissions

Get-MailboxFolderPermission -Identity "JohnDoe@contoso.com:\Calendar"
```

✅ **Validation**

- Shared calendar appears in members' Outlook/OWA.
- Test creating an event → verify all assigned members can see or edit it.
- Confirm permissions using PowerShell for accuracy.

✅ **Best Practices**

- Use **descriptive calendar names** to avoid confusion.
- Assign **appropriate permission levels** based on user roles.
- Regularly review calendar sharing to remove inactive users.
- Encourage users to **check availability before scheduling** to reduce conflicts.

✅ **Use Case**
A project team creates a shared calendar **ProjectPhoenix Meetings**.

- Team members have edit permissions → can schedule and update meetings.
- Improves visibility of project deadlines and reduces double-booking.

---

34. How to Configure Email Disclaimer in Exchange Online

✅ **Purpose**
Email disclaimers automatically append **legal or informational text** to outgoing emails.

- Helps organizations comply with **legal, regulatory, or corporate policies**.
- Can include confidentiality statements, company branding, or disclaimers for external communications.
- Applied to **all or selected users** based on policies.

✅ Configuration Steps

Exchange Admin Center (EAC)

1. Sign in to https://admin.exchange.microsoft.com as Global/Exchange Admin.
2. Navigate → **Mail flow** → **Rules** → **+ (Create a new rule)**
3. Select **Apply disclaimers** → **Enter rule name**
4. Configure rule settings:
    - **Apply to:** All messages or specific recipients
    - **Mode:** Append disclaimer or prepend disclaimer
    - **Disclaimer text:** Enter legal statement or HTML formatted content
    - **Fallback action:** Wrap, ignore, or reject if disclaimer cannot be applied
5. Save the rule → It takes effect immediately.

PowerShell (Exchange Online)

```
# Connect to Exchange Online

Connect-ExchangeOnline



# Create a transport rule with disclaimer

New-TransportRule -Name "Company Disclaimer" -ApplyHtmlDisclaimerText
"This email is confidential and intended for the recipient only."
-ApplyHtmlDisclaimerFallbackAction Wrap -SentToScope NotInOrganization
```

```
# Verify rule

Get-TransportRule | Format-Table Name,Enabled
```

✅ **Validation**

- Send a test email → disclaimer should appear at the bottom or top as configured.
- Check for proper formatting in Outlook, OWA, and mobile clients.
- The confirm rule is enabled and applies to intended recipients using EAC or PowerShell.

✅ **Best Practices**

- Use **clear and concise language** in disclaimers.
- Test formatting on multiple email clients to ensure readability.
- Apply disclaimers **only to external emails** if internal emails do not require them.
- Document and review disclaimers regularly for legal compliance updates.

✅ **Use Case**
All outgoing emails from **@contoso.com** append a confidentiality statement for external recipients:

> "This email is confidential and intended solely for the recipient. Any unauthorized use is prohibited."

- Ensures compliance with legal and corporate policies.

---

35. How to Block User Access to Microsoft 365 | Block User Sign-in

✅ **Purpose**
Blocking a user prevents them from **signing in to Microsoft 365 services** without deleting their account.

- Useful for **terminated employees**, **suspended accounts**, or **temporary access restrictions**.
- Preserves **mailbox data, OneDrive files, and SharePoint access** for compliance or recovery.
- Ensures security by **preventing unauthorized access**.

✅ **Configuration Steps**

Microsoft 365 Admin Center

1. Sign in to https://admin.microsoft.com as Global Admin.
2. Navigate → **Users** → **Active users**.
3. Select the user to block.
4. In the **Account** section → Toggle **Block sign-in** → **On**.
5. Save changes → User is now blocked from signing in.

PowerShell

```
# Connect to Microsoft 365

Connect-MsolService



# Block user sign-in

Set-MsolUser -UserPrincipalName user1@contoso.com -BlockCredential
$true



# Verify status
```

```
Get-MsolUser -UserPrincipalName user1@contoso.com | Select
DisplayName,BlockCredential
```

✅ **Validation**

- Attempt to sign in with the blocked user account → access is denied.
- Check **BlockCredential = True** via PowerShell.
- Confirm that mailbox and OneDrive files are **still intact**.

✅ **Best Practices**

- Block accounts immediately when **employees leave the organization**.
- Avoid deleting accounts until data retention policies are addressed.
- Use **audit logs** to monitor blocked accounts and sign-in attempts.
- Document reasons for blocking accounts for compliance.

✅ **Use Case**
An employee leaves the company.

- Admin blocks sign-in for **john.doe@contoso.com**.
- The mailbox and OneDrive remain accessible to HR or compliance for data retention purposes, while the user cannot access any Microsoft 365 service.

---

36. How to Restore a Deleted Microsoft 365 User | User Mailboxes

✅ **Purpose**
Restoring a deleted user allows recovery of **user accounts, mailboxes, and associated data** within the **retention period**.

- Useful when a user is **accidentally deleted** or **rejoins the organization**.

- Preserves mailbox content, OneDrive files, and Teams data.
- The retention period for restoration is typically **30 days** by default.

✅ Configuration Steps

Microsoft 365 Admin Center

1. Sign in to https://admin.microsoft.com as Global Admin.
2. Navigate → **Users** → **Deleted users**.
3. Select the user to restore → Click **Restore user**.
4. Assign **licenses** if needed → Update user information as required.
5. Complete restoration → The user mailbox and account are reactivated.

PowerShell

```
# Connect to Microsoft 365

Connect-MsolService


# List deleted users

Get-MsolUser -ReturnDeletedUsers


# Restore a deleted user

Restore-MsolUser -UserPrincipalName user1@contoso.com


# Verify restoration

Get-MsolUser -UserPrincipalName user1@contoso.com
```

✅ **Validation**

- User appears in **Active users** list after restoration.
- Test mailbox access via Outlook or OWA.
- Verify license assignment and associated data (OneDrive, Teams, SharePoint).

✅ **Best Practices**

- Restore users **within the retention period** to avoid permanent data loss.
- Assign licenses immediately after restoration.
- Inform the user of changes and updated credentials.
- Document restoration for compliance and auditing purposes.

✅ **Use Case**
An employee account **jane.doe@contoso.com** was accidentally deleted.

- Admin restores the user within 10 days.
- The mailbox and OneDrive files are preserved → Jane resumes work without data loss.

---

37. Converting the Mailbox of Deleted User in Microsoft 365 Exchange Online

✅ **Purpose**
When a user is deleted, their mailbox can be **retained, converted, or assigned as a shared mailbox**.

- Preserves **emails and associated data** for compliance or operational needs.
- Useful for **departed employees** whose mail needs to be accessible to other team members.
- Allows organizations to **maintain continuity of communication** without consuming a full license (if converted to shared mailbox).

✅ Configuration Steps

Microsoft 365 Admin Center

1. Sign in to https://admin.microsoft.com as Global Admin.
2. Navigate → **Users** → **Deleted users**.
3. Select the deleted user → Click **Restore user** (if mailbox not restored already).
4. Convert mailbox to **Shared Mailbox**:
    - Navigate → **Exchange Admin Center** → **Recipients** → **Mailboxes**
    - Select the restored user mailbox → **Convert to shared mailbox** → Save.

PowerShell (Exchange Online)

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Convert user mailbox to shared mailbox

Set-Mailbox -Identity "DeletedUser@contoso.com" -Type Shared


# Verify conversion

Get-Mailbox -Identity "DeletedUser@contoso.com" | Format-Table
DisplayName,RecipientTypeDetails
```

✅ Validation

- Shared mailbox appears in **Outlook/OWA** for assigned users.
- Users with permissions can **access, send, and receive emails** from the mailbox.

- Confirm conversion using PowerShell: `RecipientTypeDetails` should show **SharedMailbox**.

✅ **Best Practices**

- Assign **Full Access** and/or **Send As** permissions to relevant team members.
- Retain mailbox only as long as needed to **meet compliance or operational requirements**.
- Document mailbox conversion and assigned permissions for auditing.

✅ **Use Case**
An employee **john.doe@contoso.com** leaves the organization.

- Admin restores the mailbox and converts it to a shared mailbox.
- Team members have access to emails → ongoing project communication is preserved without assigning a new license.

---

38. How to Give Access to OneDrive to Another User in Microsoft 365

✅ **Purpose**
Granting access to a user's OneDrive allows another person to **manage or access files** in cases of absence, account transfer, or administrative needs.

- Useful when an employee **leaves the organization** or is **on extended leave**.
- Ensures **continuity of work** and access to important documents.
- Maintains **data security** while enabling controlled access.

✅ **Configuration Steps**

Microsoft 365 Admin Center

1. Sign in to https://admin.microsoft.com as Global Admin.

2. Navigate → **Users** → **Active users** → Select the user whose OneDrive you want to access.

3. Click **OneDrive** → **Access files** → **Create link to access files**.

4. Copy the link and provide it to another user (or directly assign access via permissions).

PowerShell (SharePoint Online / OneDrive Admin)

```
# Connect to SharePoint Online

Connect-SPOService -Url https://contoso-admin.sharepoint.com



# Grant admin access to another user

Set-SPOUser -Site
https://contoso-my.sharepoint.com/personal/user1_contoso_com
-LoginName user2@contoso.com -IsSiteCollectionAdmin $true
```

✅ **Validation**

- Assigned users can access the OneDrive site via **link or admin access**.
- Verify that files, folders, and permissions are accessible.
- Ensure only intended access is granted to prevent unauthorized data exposure.

✅ **Best Practices**

- Grant access **only to necessary personnel**.
- Remove access immediately when no longer required.
- Prefer **view or edit permissions** over full control unless absolutely needed.
- Document access assignments for auditing and compliance purposes.

✅ **Use Case**
An employee **leaves the company** with critical project files in OneDrive.

- Admin grants the project manager **Site Collection Admin access**.
- Managers can retrieve, edit, or transfer files to other team members without disrupting project progress.

---

39. Create and Manage Inactive Mailbox in Microsoft 365 Exchange Online

✅ **Purpose**
An **Inactive Mailbox** preserves mailbox content of **deleted or former users** while disabling access to the account.

- Useful for **compliance, legal, or regulatory retention requirements**.
- Ensures **email content is preserved** even after a user account is deleted.
- Supports scenarios where a mailbox is required for **audit or eDiscovery purposes**.

✅ **Configuration Steps**

Prerequisites

- The mailbox must have a **litigation hold or retention policy** applied **before deletion**.

Microsoft 365 / Exchange Online

1. Delete the user account in Microsoft 365 → Mailbox becomes **inactive** due to the applied hold.
2. Navigate → **Exchange Admin Center → Compliance → eDiscovery or Content Search** to manage the inactive mailbox.
3. Assign access to **compliance officers or legal teams** for content search and retrieval.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Check if mailbox is inactive

Get-Mailbox -InactiveMailboxOnly | Format-Table
DisplayName,ExchangeGuid,ArchiveStatus


# Assign eDiscovery access

Add-MailboxPermission -Identity "InactiveUser@contoso.com" -User
complianceuser@contoso.com -AccessRights FullAccess
```

✅ **Validation**

- Confirm mailbox appears in **inactive mailboxes list** in Exchange Admin Center.
- Verify assigned users can access mailbox content via **eDiscovery or compliance tools**.
- Attempt login → should fail, confirming the mailbox is inactive.

✅ **Best Practices**

- Apply **litigation hold or retention policy** before deleting the user to ensure data preservation.
- Grant access only to **authorized compliance or legal personnel**.
- Regularly review inactive mailboxes to ensure **retention policies are applied**.
- Document mailbox status and assigned permissions for compliance audits.

✅ **Use Case**
An employee **John Doe** leaves the company.

- Admin deletes the user account, and because a litigation hold was applied, the mailbox becomes **inactive**.
- The legal team can access emails for audit purposes without restoring the account or consuming a license.

---

40. Create a Content Search in Microsoft 365 Compliance Center with Permission

✅ **Purpose**
Content Search allows admins and compliance officers to **search across Microsoft 365 data** for emails, documents, Teams messages, and other content.

- Useful for **legal investigations, audits, and compliance reviews**.
- Helps locate content **without restoring or accessing individual mailboxes**.
- Can be used to **export search results** for review or legal purposes.

✅ **Configuration Steps**

Assign Permissions

1. Sign in to https://compliance.microsoft.com as **Global Admin or Compliance Admin**.
2. Navigate → **Permissions** → **Compliance roles** → **eDiscovery Manager**.
3. Assign users as **eDiscovery Managers** to allow content search creation and export.

Create a Content Search

1. Navigate → **Content search** → **+ New search**.
2. Enter **search name and description** (e.g., “ProjectPhoenix Audit Search”).
3. Configure search criteria:

    - Locations: Exchange mailboxes, SharePoint sites, OneDrive accounts, Teams channels
    - Keywords, date ranges, or conditions
4. Review settings → Save and run the search.
5. Once search completes, select the search → **Preview results** → **Export results** if needed.

PowerShell (Optional)

```
# Connect to Security & Compliance Center

Connect-IPPSSession


# Create a content search

New-ComplianceSearch -Name "ProjectPhoenixSearch" -ExchangeLocation
all -ContentMatchQuery 'subject:"ProjectPhoenix" AND sent>=01/01/2025'


# Start the search

Start-ComplianceSearch -Identity "ProjectPhoenixSearch"


# Verify search status

Get-ComplianceSearch -Identity "ProjectPhoenixSearch"
```

✅ **Validation**

- Search status shows **Completed** in the Compliance Center.
- Preview shows emails, documents, or Teams messages matching the query.

- Users with assigned **eDiscovery permissions** can view/export search results.

✅ **Best Practices**

- Grant **eDiscovery Manager role** only to authorized personnel.
- Use **specific keywords and date ranges** to narrow search scope.
- Document searches and results for **audit and compliance purposes**.
- Schedule or repeat searches for ongoing investigations or regulatory requirements.

✅ **Use Case**
A compliance officer needs all emails and documents related to **ProjectPhoenix**.

- Creates a content search in the Compliance Center with keywords and project dates.
- Exports the results for review → ensures regulatory compliance without disturbing user mailboxes.

---

41. How to Disable Automatic Forwarding in Exchange Online Microsoft 365

✅ **Purpose**
Disabling automatic forwarding prevents users from **automatically sending emails to external recipients**, which can pose **security and data leakage risks**.

- Protects sensitive or confidential organizational data.
- Helps enforce **data compliance policies**.
- Ensures all emails remain **within Microsoft 365** unless explicitly shared.

✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Sign in to https://admin.exchange.microsoft.com as Global/Exchange Admin.
2. Navigate → **Mail flow** → **Rules** → **+ (Create a new rule)**.
3. Select **"Apply disclaimers or restrictions"** → **"More options"**.
4. Configure rule:
    - Apply to **All messages sent outside the organization**
    - Action → **Block the message** → **Notify sender with explanation**
5. Name the rule (e.g., "Disable Automatic Forwarding") → Save.

PowerShell (Recommended for bulk enforcement)

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Disable automatic forwarding for all users

Get-Mailbox -ResultSize Unlimited | Set-Mailbox -ForwardingSmtpAddress
$null -DeliverToMailboxAndForward $false


# Verify settings for a mailbox

Get-Mailbox -Identity "user1@contoso.com" | Format-Table
DisplayName,ForwardingSmtpAddress,DeliverToMailboxAndForward
```

✅ **Validation**

- Test by attempting to create a mailbox rule to forward emails externally → should fail or no emails delivered externally.
- Confirm PowerShell shows `ForwardingSmtpAddress = null` and `DeliverToMailboxAndForward = False`.

- Check EAC rule enforcement by sending test emails to external accounts.

✅ **Best Practices**

- Apply **organization-wide** to prevent accidental data leaks.
- Exceptions can be granted to **specific users or groups** with documented approval.
- Monitor **forwarding attempts and audit logs** for compliance.
- Educate users on **secure alternatives** for sharing data externally (OneDrive, SharePoint links).

✅ **Use Case**
An organization wants to **prevent employees from auto-forwarding corporate emails to personal accounts**.

- Admin disables automatic forwarding via PowerShell and EAC rules.
- All emails remain within Microsoft 365 → reduces risk of sensitive information leakage.

---

42. Create Email Rules to Prevent Ransomware Using File Extension

✅ **Purpose**
Email rules targeting file extensions help **prevent ransomware and malicious files** from reaching users' mailboxes.

- Blocks suspicious attachments like `.exe`, `.js`, `.vbs`, and other risky files.
- Protects **end users and corporate data** from malware infections.
- Supports compliance with **security policies** and best practices for email hygiene.

✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Sign in to https://admin.exchange.microsoft.com as Global/Exchange Admin.

2. Navigate → **Mail flow** → **Rules** → **+ (Create a new rule)**.
3. Select **“Block messages”** → **More options**.
4. Configure rule:
    - Apply to **All messages** or specific recipients/groups.
    - Condition → **Any attachment’s file extension matches** → Enter risky extensions (e.g., `.exe, .js, .vbs`).
    - Action → **Reject the message with explanation** or **Quarantine the message**.
5. Name the rule (e.g., “Block Suspicious File Extensions”) → Save.

PowerShell (Optional)

```
# Connect to Exchange Online

Connect-ExchangeOnline



# Create a transport rule to block risky attachments

New-TransportRule -Name "Block Suspicious Files"
-AttachmentExtensionMatchesWords "exe","js","vbs"
-RejectMessageReasonText "Attachments with this file type are blocked
for security reasons." -RejectMessageEnhancedStatusCode 5.7.1



# Verify rule

Get-TransportRule | Format-Table Name,Enabled,Priority
```

✅ **Validation**

- Send test emails with blocked file extensions → emails should be **rejected or quarantined**.

- Review **message trace logs** to ensure the rule is applied correctly.
- Confirm users cannot receive blocked attachments in Outlook or OWA.

✅ **Best Practices**

- Maintain an **updated list of high-risk file extensions**.
- Combine rules with **Anti-Malware policies in Microsoft 365 Defender**.
- Inform users about **safe alternatives for sharing files** (OneDrive, SharePoint links).
- Monitor **rule effectiveness and false positives** regularly.

✅ **Use Case**
An organization wants to prevent ransomware attacks via email.

- Admin creates a transport rule blocking `.exe`, `.js`, `.vbs`, and other high-risk files.
- Emails containing these attachments are rejected → users remain protected from potential malware infections.

---

43. Change a User Name and Email Address in Exchange Online Microsoft 365

✅ **Purpose**
Updating a user's name and email address ensures that **organizational directories, email routing, and communication** remain accurate.

- Supports **employee name changes, mergers, or standardization of email addresses**.
- Maintains **delivery of emails** to the updated address.
- Ensures **consistency across Microsoft 365 services** (Exchange Online, Teams, OneDrive).

✅ **Configuration Steps**

Microsoft 365 Admin Center

1. Sign in to https://admin.microsoft.com as Global Admin.
2. Navigate → **Users** → **Active users** → Select the user.
3. Click **Manage username and email**.
4. Update the **Display name** and **User principal name (UPN)** / **primary email address**.
5. Save changes → Microsoft 365 automatically updates the email address.
6. Optionally, add **email aliases** to ensure old addresses continue to receive emails.

Exchange Admin Center (Optional for Alias Management)

1. Navigate → **Recipients** → **Mailboxes** → **Select user**.
2. Go to **Email addresses** → **Add alias or update primary SMTP**.
3. Save changes → Propagate updates across Exchange Online.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Change display name

Set-Mailbox -Identity "user1@contoso.com" -DisplayName "John Smith"


# Change primary email address (UPN/SMTP)

Set-Mailbox -Identity "user1@contoso.com" -PrimarySmtpAddress
"john.smith@contoso.com"
```

```
# Add previous email as alias

Set-Mailbox -Identity "john.smith@contoso.com" -EmailAddresses
@{add="user1@contoso.com"}


# Verify changes

Get-Mailbox -Identity "john.smith@contoso.com" | Format-Table
DisplayName,PrimarySmtpAddress,EmailAddresses
```

✅ **Validation**

- Send test emails to both **new and old addresses** → ensure delivery works.
- Verify the **display name** reflects changes in Outlook, Teams, and address book.
- Check aliases and primary SMTP addresses using PowerShell or EAC.

✅ **Best Practices**

- Notify users of the **updated email address** to prevent confusion.
- Maintain old email addresses as **aliases** for at least 90 days to ensure email continuity.
- Update email signatures, Teams profiles, and SharePoint permissions if necessary.
- Document changes for auditing and compliance.

✅ **Use Case**
An employee **changes their last name** after marriage.

- Admin updates display name and primary email to **John Smith (john.smith@contoso.com)**.
- Old address **user1@contoso.com** remains as an alias → emails still delivered → seamless transition for colleagues and clients.

---

44. Assign or Remove Licenses for Users (Organization-wide / Bulk Management)

✅ **Purpose**
Licenses control access to Microsoft 365 services like Exchange, Teams, SharePoint, and OneDrive.

- Assigning licenses enables users to **use Microsoft 365 apps**.
- Removing licenses **frees up subscription resources** and ensures compliance.
- Bulk management simplifies administration for large organizations.

✅ **Configuration Steps**

Microsoft 365 Admin Center

1. Sign in to https://admin.microsoft.com as Global Admin.
2. Navigate → **Users** → **Active Users**.
3. Select one or multiple users → **Licenses and Apps**.
4. Toggle licenses **on or off** → Save changes.

PowerShell (Bulk Assignment/Removal)

```
# Connect to Microsoft 365

Connect-MsolService


# Assign license to a user

Set-MsolUserLicense -UserPrincipalName user1@contoso.com -AddLicenses
"contoso:ENTERPRISEPACK"


# Remove license from a user
```

```
Set-MsolUserLicense -UserPrincipalName user2@contoso.com
-RemoveLicenses "contoso:ENTERPRISEPACK"


# Bulk assignment from CSV

Import-Csv "C:\UsersList.csv" | ForEach-Object {

    Set-MsolUserLicense -UserPrincipalName $_.UserPrincipalName
-AddLicenses "contoso:ENTERPRISEPACK"

}
```

✅ **Validation**

- Verify licenses via **Admin Center** → user's "Licenses" column.
- Use PowerShell: `Get-MsolUser -UserPrincipalName user1@contoso.com | Select DisplayName,Licenses`.

✅ **Best Practices**

- Maintain a **naming and license assignment standard** for consistency.
- Review licenses regularly → remove unused licenses.
- Document changes for auditing.

✅ **Use Case**
Onboarding 50 new employees → assign Exchange Online, Teams, and OneDrive licenses via bulk CSV using PowerShell.

---

45. Delete a User Mailbox Permanently

✅ **Purpose**
Deleting a mailbox permanently removes the account and frees up licenses.

- Required when employees **leave the organization**.
- Can be combined with **archiving or inactive mailbox retention** for compliance.

✅ Configuration Steps

Microsoft 365 Admin Center

1. Navigate → **Users** → **Active Users** → **Select User** → **Delete User**.
2. Confirm deletion → mailbox moves to **Deleted Users** for 30 days by default.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Remove a mailbox permanently

Remove-Mailbox -Identity "user1@contoso.com" -Permanent $true


# Verify deletion

Get-Mailbox -Identity "user1@contoso.com"
```

✅ Validation

- Users no longer appear in **Active Users**.
- Mailbox removed from Exchange Online → no access.

✅ Best Practices

- Backup important emails if required → export PST or convert to shared mailbox.

- Delete users **only after compliance requirements** are satisfied.

✅ **Use Case**
Employee John Doe leaves → mailbox deleted permanently after archiving project emails.

---

46. Convert a Shared Mailbox to a User Mailbox

✅ **Purpose**
Converting allows a shared mailbox to be **assigned a license** and used as a **full user mailbox**.

✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Navigate → **Recipients** → **Shared Mailboxes** → **Select mailbox**.
2. Click **Convert to Regular Mailbox** → **Assign License** → Save.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Convert shared mailbox to user mailbox

Set-Mailbox -Identity "sharedmailbox@contoso.com" -Type Regular


# Assign license in Microsoft 365 Admin Center
```

✅ **Validation**

- Mailbox appears in the Active **Users** list.

- Users can login directly with credentials.

✅ **Best Practices**

- Convert only if the mailbox needs **full user access**.
- Ensure license assignment after conversion.

✅ **Use Case**
A shared mailbox for a contractor is converted to a user mailbox when they join full-time → can send/receive emails individually.

---

47. Restore a Deleted Shared Mailbox

✅ **Purpose**
Restoring a deleted shared mailbox recovers **emails and shared resources** within the retention period.

✅ **Configuration Steps**

Microsoft 365 Admin Center

1. Navigate → **Users** → **Deleted Users** → **Select Shared Mailbox** → Restore.
2. Assign **permissions** and verify mailbox access.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Restore deleted mailbox

Undo-SoftDeletedMailbox -Identity "sharedmailbox@contoso.com"


# Verify
```

```
Get-Mailbox -SoftDeletedMailbox
```

✅ **Validation**

- Mailbox reappears in the Shared **Mailboxes** list.
- Assigned users can access emails and calendars.

✅ **Best Practices**

- Restore **within 30 days** of deletion.
- Reassign permissions as required.

✅ **Use Case**
Accidentally deleted shared mailbox for project team → restored within 10 days → no data lost.

---

48. Manage Mailbox Quotas & Storage Limits

✅ **Purpose**
Mailbox quotas ensure **storage usage is controlled** and maintain system performance.

✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Navigate → **Recipients** → **Mailboxes** → **Select User** → **Mailbox Usage / Properties**.
2. Adjust:
    - Issue warning at X MB
    - Prohibit send at Y MB
    - Prohibit send and receive at Z MB → Save

PowerShell

```
# Connect to Exchange Online
```

```
Connect-ExchangeOnline


# Set mailbox quota

Set-Mailbox -Identity "user1@contoso.com" -ProhibitSendQuota 4GB
-ProhibitSendReceiveQuota 5GB -IssueWarningQuota 3.5GB


# Verify quota

Get-Mailbox -Identity "user1@contoso.com" | Format-Table
DisplayName,ProhibitSendQuota,ProhibitSendReceiveQuota,IssueWarningQuo
ta
```

✅ **Validation**

- The user receives a warning when the mailbox reaches the warning quota.
- Cannot send messages after reaching the prohibited send quota.
- Cannot send or receive after prohibiting send and receive quota.

✅ **Best Practices**

- Set quotas based on **business needs and mailbox usage patterns**.
- Monitor storage regularly → adjust quotas if needed.
- Inform users of limits → encourage archiving old emails.

✅ **Use Case**
The finance team user has large mailbox → set warning at 3.5 GB, prohibit send at 4 GB, prohibit send/receive at 5 GB → prevents mailbox bloat.

---

49. Configure Conditional Access Policies (Restrict Access by Device/Location)

✅ Purpose

Conditional Access (CA) allows admins to **control how, when, and from where users can access Microsoft 365 services**.

- Enhance security by enforcing **multi-factor authentication (MFA)**, device compliance, or location restrictions.
- Prevent unauthorized access from **untrusted devices or networks**.
- Supports **Zero Trust security models**.

✅ Configuration Steps

Microsoft 365 / Azure AD

1. Sign in to https://portal.azure.com as Global Admin.
2. Navigate → **Azure Active Directory** → **Security** → **Conditional Access** → **+ New Policy**.
3. Configure:
    - **Assignments**: Select users/groups and cloud apps (e.g., Exchange Online, SharePoint).
    - **Conditions**: Device platform, location, sign-in risk, client app.
    - **Access Controls**: Require MFA, block access, require compliant device.
4. Enable policy → Save and monitor results.

✅ Validation

- Test login from allowed vs. blocked devices/locations.
- Review **Sign-in logs** in Azure AD for enforcement results.

✅ Best Practices

- Apply **pilot policies** to a small group before org-wide deployment.
- Combine CA with **MFA and Intune compliance** for maximum security.
- Document policies and exceptions for auditing.

✅ **Use Case**
Restrict Exchange Online access → only from corporate network and compliant devices → unauthorized access attempts from public Wi-Fi blocked.

---

50. Setup Data Loss Prevention (DLP) Policies

✅ **Purpose**
DLP policies **protect sensitive data** from being shared externally via email or Teams.

- Detect content like **credit card numbers, social security numbers, or confidential documents**.
- Prevent accidental or intentional data leakage.

✅ **Configuration Steps**

Microsoft 365 Compliance Center

1. Sign in → https://compliance.microsoft.com.
2. Navigate → **Data loss prevention** → **+ Create policy**.
3. Choose **templates** (e.g., Financial, GDPR, HIPAA).
4. Define **locations** (Exchange, OneDrive, SharePoint, Teams).
5. Configure **rules and actions**: Block sharing, notify user, report incident.
6. Test and enable policy.

✅ **Validation**

- Send a test email with sensitive data → ensure DLP triggers action (block/warning).

- Monitor **DLP reports** in Compliance Center.

✅ **Best Practices**

- Start with **audit mode** to monitor impact before enforcing.
- Use **clear notifications** to educate users on policy violations.
- Regularly review sensitive data types and adjust policies.

✅ **Use Case**
Finance sends payroll info via email → DLP blocks sensitive attachments from leaving the organization → prevents data breach.

---

51. Enable Litigation Hold / In-Place Hold for Compliance

✅ **Purpose**
Litigation Hold preserves mailbox content **indefinitely or for a defined period** for compliance or legal reasons.

- Protects **emails, calendar items, and deleted content** from permanent deletion.
- Useful for **legal investigations, audits, or regulatory compliance**.

✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Navigate → **Recipients** → **Mailboxes** → **Select User**.
2. Go to **Mailbox Features** → **Enable Litigation Hold**.
3. Specify **hold duration** (optional) → Save.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline
```

```
# Enable Litigation Hold

Set-Mailbox -Identity "user1@contoso.com" -LitigationHoldEnabled $true
-LitigationHoldDuration 365


# Verify

Get-Mailbox -Identity "user1@contoso.com" | Select
DisplayName,LitigationHoldEnabled,LitigationHoldDuration
```

✅ **Validation**

- Deleted items remain in the Recoverable **Items folder**.
- Hold status visible in **Mailbox Features** or via PowerShell.

✅ **Best Practices**

- Only apply to **users requiring compliance or legal retention**.
- The document holds rationale and duration.
- Monitor mailbox size → may grow due to preserved items.

✅ **Use Case**
Employee leaves company → mailbox placed on 2-year litigation hold for ongoing legal case → all emails preserved.

---

52. Configure eDiscovery Cases & Content Searches

✅ **Purpose**
eDiscovery allows admins to **search, export, and preserve content** across Exchange, SharePoint, OneDrive, and Teams.

- Essential for **legal investigations, audits, and regulatory compliance**.
- Reduces need to restore mailboxes individually.

✅ Configuration Steps

Microsoft 365 Compliance Center

1. Navigate → **eDiscovery** → **Core** → + New Case.
2. Add **members** (compliance officers).
3. Within case → **Content search** → **New Search**.
4. Define **locations, keywords, date ranges**.
5. Run search → preview → export results if required.

PowerShell

```
# Connect to Security & Compliance Center

Connect-IPPSSession


# Create a new content search

New-ComplianceSearch -Name "ProjectXSearch" -ExchangeLocation all
-ContentMatchQuery 'subject:"ProjectX"'


# Start search

Start-ComplianceSearch -Identity "ProjectXSearch"


# Verify status

Get-ComplianceSearch -Identity "ProjectXSearch"
```

✅ **Validation**

- Search shows results matching criteria.
- Exported content accessible only to assigned eDiscovery members.

✅ **Best Practices**

- Assign **case members carefully** for compliance.
- Narrow searches with **keywords and dates** to reduce volume.
- Document search purpose and results for auditing.

✅ **Use Case**
Legal team needs emails and documents related to **ProjectX** → creates eDiscovery case → exports content for review.

---

53. Manage Retention Policies and Labels

✅ **Purpose**
Retention policies and labels **control the lifecycle of emails and documents**.

- Automates **deletion, archiving, or retention** for compliance.
- Applies to **Exchange, SharePoint, OneDrive, Teams**.

✅ **Configuration Steps**

Microsoft 365 Compliance Center

1. Navigate → **Information governance** → **Retention policies / labels** → **+ Create**.
2. Define **retention settings**: Retain for X days/years, delete after, or trigger actions.
3. Assign to **users, groups, or sites**.
4. Publish labels if needed → Users can manually apply them.

✅ **Validation**

- Retention policies visible in the Compliance **Center**.
- Test by sending emails or creating documents → ensure retention rules apply.

✅ **Best Practices**

- Apply default retention policies to all mailboxes for compliance baseline.
- Educate users about manual labels and proper usage.
- Monitor **policy conflicts** and resolve overlaps.

✅ **Use Case**
HR mails need to be retained for 7 years → retention policy applied → automatic archiving and eventual deletion ensures compliance.

---

54. Configure Audit Logging & Reports

✅ **Purpose**
Audit logging tracks **user and admin actions** in Microsoft 365.

- Essential for **security monitoring, compliance audits, and forensic investigations**.
- Logs include **sign-ins, mailbox changes, file access, and admin activities**.

✅ **Configuration Steps**

Microsoft 365 Compliance Center

1. Navigate → **Audit** → **Start recording user/admin activities** (if not enabled).
2. Use **Search** to filter by user, activity, date range, or service.
3. Export results for compliance reporting.

PowerShell

```
# Connect to Security & Compliance Center
```

```
Connect-IPPSSession


# Search audit log

Search-UnifiedAuditLog -StartDate "2025-01-01" -EndDate "2025-01-31"
-Operations SendOnBehalf, SendAs -ResultSize 1000


# Export to CSV

Search-UnifiedAuditLog ... | Export-Csv "C:\AuditLog.csv"
-NoTypeInformation
```

✅ **Validation**

- Audit logs populated with user/admin actions.
- Cross-check logs for suspicious or unauthorized activity.

✅ **Best Practices**

- Enable audit logging **organization-wide**.
- Review logs **regularly** for compliance or security issues.
- Retain logs as per **organizational retention policies**.

✅ **Use Case**
Admin wants to review all **Send As** actions in January → runs audit search → exports CSV for review → ensures no unauthorized activity occurred.

---

55. Create Transport Rules (Mail Flow Rules)

✅ **Purpose**
Transport rules allow admins to **control email flow** in Exchange Online based on conditions, actions, and exceptions.

- Can **block, redirect, or append disclaimers**.
- Enforce **organizational policies** such as sensitive data handling or compliance.

✅ Configuration Steps

Exchange Admin Center (EAC)

1. Sign in → https://admin.exchange.microsoft.com.
2. Navigate → **Mail flow** → **Rules** → **+ (Create a new rule)**.
3. Configure rule:
    - Name: e.g., “Block External Payroll Emails”.
    - Apply conditions (sender, recipient, subject, keywords).
    - Choose action (block, redirect, notify, quarantine).
4. Set exceptions if needed → Save → Test.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline



# Create a transport rule to block external emails with "confidential"
in subject

New-TransportRule -Name "Block Confidential External"
-SubjectContainsWords "confidential" -SentToScope NotInOrganization
-RejectMessageReasonText "External forwarding of confidential emails
is blocked."
```

✅ Validation

- Send test emails matching the condition → ensure rule triggers action.
- Monitor **Mail Flow** → **Message Trace** for enforcement.

✅ **Best Practices**

- Start with **audit-only mode** to avoid unintentional disruptions.
- Document rules → avoid conflicts or overlapping conditions.
- Review periodically to remove outdated rules.

✅ **Use Case**
Finance department emails with “Payroll” in subject blocked from going externally → prevents data leaks.

---

56. Configure Email Disclaimer (Advanced)

✅ **Purpose**
Email disclaimers automatically **append legal or informational text** to all outgoing emails.

- Ensures compliance with **legal, regulatory, or corporate policies**.
- Can include **confidentiality notices or GDPR statements**.

✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Navigate → **Mail flow** → **Rules** → **+ (Apply disclaimers)**.
2. Configure rule:
    - Apply to all outgoing messages or specific recipients.
    - Append disclaimer text → HTML formatting supported.
    - Set exceptions (internal emails, certain domains).

3. Save → Test by sending email externally.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Create disclaimer rule

New-TransportRule -Name "Company Disclaimer" -SentToScope
NotInOrganization -ApplyHtmlDisclaimerText "<b>Confidential: For
authorized recipients only.</b>" -ApplyHtmlDisclaimerFallbackAction
Wrap
```

✅ **Validation**

- Send test emails → disclaimer appears in the email body.
- Ensure formatting preserved in Outlook and OWA.

✅ **Best Practices**

- Maintain **consistent format and branding**.
- Avoid overly long disclaimers → may affect readability.
- Use transport rules instead of client-side signatures for **consistency**.

✅ **Use Case**
The legal team requires all outgoing emails to carry a confidentiality notice → implemented via transport rule → automatic appending for all external recipients.

---

57. Block External Forwarding for Security

✅ **Purpose**
Prevent users from automatically forwarding emails outside the organization → protects **sensitive information**.

✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Navigate → **Mail flow** → **Rules** → **+ (Create new rule)**.
2. Condition: Apply to messages sent externally.
3. Action: **Reject message or notify sender**.
4. Save → Test.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline



# Disable automatic forwarding for all mailboxes

Get-Mailbox -ResultSize Unlimited | Set-Mailbox -ForwardingSmtpAddress
$null -DeliverToMailboxAndForward $false
```

✅ **Validation**

- Test auto-forwarding → message blocked or fails.
- Check mailbox settings to ensure forwarding addresses cleared.

✅ **Best Practices**

- Allow exceptions for approved business scenarios.
- Monitor compliance via **message trace**.

✅ **Use Case**
Users are blocked from forwarding internal financial emails to personal accounts → prevents data leakage.

---

58. Configure Anti-Malware / Anti-Phishing Policies

✅ **Purpose**
Protects organizations from **malware, phishing, and spam** in emails.

✅ **Configuration Steps**

Microsoft 365 Security & Compliance Center

1. Navigate → **Threat management** → **Policy** → **Anti-spam / Anti-malware**.
2. Configure policies:
    - Block or quarantine malicious emails.
    - Set actions for high-confidence phishing.
    - Customize safe sender/blocked sender lists.
3. Apply to all users or groups → Save.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Create a custom anti-malware policy

New-MalwareFilterPolicy -Name "Custom AntiMalware" -Action
DeleteMessage -NotifyAdmin $true
```

✅ **Validation**

- Send test malware/phishing simulation emails → ensure detection and quarantine.
- Monitor **Security & Compliance reports**.

✅ **Best Practices**

- Combine with **Safe Links and Safe Attachments** in Microsoft Defender.
- Update policies regularly → adapt to new threats.
- Educate users about phishing attacks.

✅ **Use Case**
Organization blocks all emails containing suspicious attachments → reduces risk of ransomware infections.

---

59. Manage Safe Sender / Blocked Sender Lists

✅ **Purpose**
Control email delivery by specifying **trusted and blocked senders**.

- Improves **spam filtering** efficiency.
- Ensures **critical emails are delivered** and malicious emails blocked.

✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Navigate → **Protection** → **Spam filter** → **Edit policy**.
2. Add email addresses or domains to **Allowed senders (Safe)** or **Blocked senders**.
3. Save → Apply to all users or specific groups.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline
```

```
# Add blocked sender domain

Set-HostedContentFilterPolicy -Identity "Default"
-BlockedSendersAndDomains @{Add="malicious.com"}


# Add safe sender

Set-HostedContentFilterPolicy -Identity "Default"
-AllowedSendersAndDomains @{Add="trustedpartner.com"}
```

✅ **Validation**

- Emails from blocked senders go to spam/quarantine.
- Emails from safe senders delivered to the inbox.

✅ **Best Practices**

- Maintain updated **trusted and blocked sender lists**.
- Avoid overly broad blocks → may impact legitimate emails.
- Periodically review lists for accuracy.

✅ **Use Case**
Trusted vendors added to the safe sender list → ensure their invoices are delivered.
Spammy domains blocked → reduces unwanted email clutter.

---

60. Create Microsoft 365 Groups & Teams (Advanced Settings & Membership)

✅ **Purpose**
Microsoft 365 Groups provide a **collaborative workspace** with shared mailbox, calendar, SharePoint, OneNote, and Teams integration.

- Supports **team collaboration, project management, and departmental communication**.
- Advanced settings control **privacy, membership, and external access**.

✅ Configuration Steps

Microsoft 365 Admin Center

1. Navigate → **Teams & Groups** → **Active Teams & Groups** → **+ Add a group**.
2. Select **Microsoft 365 Group** → **Next**.
3. Configure:
    - Name, email alias, description.
    - Privacy: **Public** or **Private**.
    - Owners & members → optional external users.
4. Advanced settings:
    - Allow/deny external sharing.
    - Enable Teams, Planner, SharePoint site.
5. Save → Group created.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Create M365 Group

New-UnifiedGroup -DisplayName "ProjectPhoenix" -Alias "ProjectPhoenix"
-EmailAddresses "ProjectPhoenix@contoso.com" -AccessType Private
-Owners "admin@contoso.com" -Members
"user1@contoso.com","user2@contoso.com"
```

✅ **Validation**

- The Verify group appears in **Outlook / Teams**.
- Test sending emails and accessing shared resources.

✅ **Best Practices**

- Use **naming conventions** for consistency (Dept_Project).
- Use private groups for **sensitive teams**.
- Review membership regularly.

✅ **Use Case**
A new product project requires collaboration → M365 Group created → shared mailbox, Teams, and files available automatically.

---

61. Manage Shared Mailboxes (Permissions, Quotas, Access)

✅ **Purpose**
Shared mailboxes allow multiple users to **send/receive emails from a common mailbox** without individual licenses.

✅ **Configuration Steps**

EAC / Admin Center

1. Navigate → **Recipients** → **Shared Mailboxes** → **+ Add**.
2. Assign **owners** (users who can manage mailboxes).
3. Assign **permissions**:
    - Full Access: read and send from mailbox.
    - Send As: send as mailbox identity.
    - Send on Behalf: send using mailbox with “on behalf” label.

4. Configure **mailbox quota** and archive settings.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Create shared mailbox

New-Mailbox -Shared -Name "Support" -DisplayName "Support Team" -Alias
"Support"


# Assign Full Access

Add-MailboxPermission -Identity "Support" -User "user1@contoso.com"
-AccessRights FullAccess


# Assign Send As

Add-RecipientPermission -Identity "Support" -Trustee
"user1@contoso.com" -AccessRights SendAs
```

✅ **Validation**

- Users can open mailboxes in Outlook / OWA.
- Send/receive emails as mailbox identity.

✅ **Best Practices**

- Use shared mailboxes for **team email handling**.
- Avoid assigning a large number of users → manage via groups.

- Monitor mailbox size → adjust quotas as needed.

✅ **Use Case**
The support team uses a shared mailbox → multiple agents access and reply without personal licenses.

---

62. Room & Equipment Mailbox Policies

✅ **Purpose**
Room and equipment mailboxes manage **resources like meeting rooms, projectors, or laptops**.

✅ **Configuration Steps**

EAC

1. Navigate → **Recipients** → **Resources** → **+ Add Resource**.
2. Select type: **Room or Equipment**.
3. Configure:
    - Name, email alias.
    - Booking options: allow conflicts, auto-accept requests, schedule limits.
4. Assign **permissions**: who can book directly or require approval.

PowerShell

```
# Create room mailbox

New-Mailbox -Room -Name "ConferenceRoom1" -DisplayName "Conference
Room 1" -Alias "ConfRoom1"



# Set booking options

Set-CalendarProcessing -Identity "ConfRoom1" -AutomateProcessing
AutoAccept -AllowConflicts $false -BookingWindowInDays 180
```

✅ **Validation**

- Test booking via Outlook → auto-accept or request approval.
- Check scheduling restrictions.

✅ **Best Practices**

- Automate acceptance for frequently used rooms.
- Limit booking window → avoid long-term conflicts.
- Regularly audit resource usage.

✅ **Use Case**
Conference Room 1 auto-accepts meeting requests → prevents double bookings → team efficiency improved.

---

63. Configure Shared Calendars & Scheduling Permissions

✅ **Purpose**
Shared calendars enable teams to **coordinate schedules, meetings, and resource bookings**.

✅ **Configuration Steps**

Outlook / OWA

1. Open user calendar → **Share Calendar**.
2. Assign **permissions**: View Only, Edit, Delegate.
3. Optionally, add a shared **mailbox calendar** for team schedules.

PowerShell

```
# Grant calendar access
```

```
Add-MailboxFolderPermission -Identity "user1@contoso.com:\Calendar"
-User "user2@contoso.com" -AccessRights Editor
```

✅ **Validation**

- Test shared calendar access → view/edit as assigned.
- Schedule meeting → verify attendees can see updates.

✅ **Best Practices**

- Use **calendar permissions** carefully to protect sensitive events.
- Encourage using **shared mailboxes** for team scheduling.

✅ **Use Case**
The project team shares a calendar → members can see deadlines, meetings, and resource availability.

---

64. OneDrive & SharePoint Access Management

✅ **Purpose**
Controls **user access to files and sites**, ensuring security and collaboration.

✅ **Configuration Steps**

Microsoft 365 Admin Center

1. Navigate → **SharePoint Admin Center / OneDrive**.
2. Assign **site permissions**: Owner, Member, Visitor.
3. Configure **sharing settings**: internal only, external sharing allowed, expiration.

PowerShell

```
# Connect to SharePoint Online

Connect-SPOService -Url "https://contoso-admin.sharepoint.com"
```

```
# Grant user access to site

Set-SPOUser -Site "https://contoso.sharepoint.com/sites/projectX"
-LoginName "user1@contoso.com" -IsSiteCollectionAdmin $false
```

✅ **Validation**

- Users can access assigned files/sites.
- External sharing restrictions enforced.

✅ **Best Practices**

- Enforce **least privilege principle**.
- Review access regularly → remove inactive users.
- Use **sensitivity labels** for confidential content.

✅ **Use Case**
ProjectX SharePoint site → only project team has access → sensitive documents protected.

---

65. Disable Legacy Protocols (POP/IMAP/EWS Basic Auth)

✅ **Purpose**
Legacy protocols are **less secure** → disabling reduces risk of compromised credentials.

✅ **Configuration Steps**

Exchange Admin Center / PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Disable POP/IMAP for all users
```

```
Get-CASMailbox -ResultSize Unlimited | Set-CASMailbox -PopEnabled
$false -ImapEnabled $false


# Disable basic authentication for EWS

Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
```

✅ **Validation**

- Legacy email clients cannot connect using POP/IMAP.
- Users redirected to modern authentication.

✅ **Best Practices**

- Notify users before disabling.
- Monitor for legacy client usage → migrate to modern clients.

✅ **Use Case**
Organization disables POP/IMAP → reduces phishing risk and enforces modern auth.

---

66. Configure Outlook Web Access (OWA) Policies

✅ **Purpose**
OWA policies control **features and access in web-based Outlook**.

✅ **Configuration Steps**

Exchange Admin Center

1. Navigate → **Permissions** → **Outlook Web App Policies** → **+ Add**.
2. Configure settings:
    - Disable forwarding, calendar sharing, instant messaging.

    - Enable/disable mobile device sync.

3. Assign policy to users → Save.

✅ **Validation**

- Users access Outlook Web App → verify policy restrictions applied.

✅ **Best Practices**

- Use OWA policies to **restrict sensitive data exposure**.
- Combine with Conditional Access for enhanced security.

✅ **Use Case**
Restrict OWA features for the finance team → cannot forward emails externally → protects sensitive info.

---

67. Mobile Device Access / Conditional Access for Devices

✅ **Purpose**
Controls **which mobile devices can access Microsoft 365** based on compliance, encryption, and policies.

✅ **Configuration Steps**

Intune / Azure AD

1. Navigate → **Endpoint security** → **Conditional Access** → **+ New Policy**.
2. Assign users/groups → select apps (Exchange, Teams).
3. Require **compliant devices** or **encryption**, block non-compliant devices.

✅ **Validation**

- Test sign-in from compliant and non-compliant devices.
- Non-compliant devices blocked from Exchange/Teams.

✅ **Best Practices**

- Enforce **MFA and device compliance**.
- Monitor mobile device inventory regularly.

✅ **Use Case**
Only Intune-enrolled devices can access Exchange → prevents untrusted devices from syncing emails.

---

68. Automatic Forwarding & Mailbox Rules Security

✅ **Purpose**
Automatic forwarding can be **used by attackers to exfiltrate data** → controlling it reduces risk.

✅ **Configuration Steps**

Exchange Admin Center / PowerShell

```
# Disable automatic forwarding for all users

Get-Mailbox -ResultSize Unlimited | Set-Mailbox -ForwardingSmtpAddress $null -DeliverToMailboxAndForward $false
```

✅ **Validation**

- Attempted auto-forwarding fails.
- Check mailbox forwarding settings → cleared.

✅ **Best Practices**

- Allow exceptions for business-critical scenarios only.
- Monitor **message trace** for suspicious activity.

✅ **Use Case**
Users blocked from forwarding emails to external accounts → reduces potential for data leaks.

---

69. Message Trace & Email Tracking

✅ **Purpose**
Message trace helps **track email delivery status** in Exchange Online.

- Useful for **investigating delivery issues, spam, or suspicious emails**.
- Provides **detailed email route and status information**.

✅ **Configuration Steps**

Exchange Admin Center (EAC)

1. Navigate → **Mail flow** → **Message trace** → **Start a trace**.
2. Select: Sender, Recipient, Date range, Status.
3. Run trace → view results (Delivered, Pending, Failed, Quarantined).

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline



# Trace messages

Get-MessageTrace -StartDate "2025-08-01" -EndDate "2025-08-29"
-SenderAddress "user1@contoso.com"



# View detailed message trace

Get-MessageTraceDetail -MessageTraceId <MessageTraceId>
-RecipientAddress "user2@contoso.com"
```

✅ **Validation**

- Confirm messages delivered, delayed, or blocked.
- Verify routing details match intended path.

✅ **Best Practices**

- Use message trace to **investigate incidents**.
- Export results for **auditing or troubleshooting**.

✅ **Use Case**
User reports not receiving emails → message trace confirms external emails quarantined → resolves delivery issue.

---

70. Usage Reports (Mailbox, Teams, OneDrive)

✅ **Purpose**
Usage reports provide insights on **adoption, activity, and storage usage** across Microsoft 365 services.

✅ **Configuration Steps**

Microsoft 365 Admin Center

1. Navigate → **Reports** → **Usage**.
2. Select service: Exchange, Teams, OneDrive, SharePoint.
3. Review metrics: Active users, Mailbox size, File storage, Collaboration activity.
4. Export CSV for further analysis.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline
```

```
# Get mailbox usage report

Get-MailboxStatistics -Database "DB01" | Select
DisplayName,ItemCount,TotalItemSize
```

✅ **Validation**

- Verify data accuracy by comparing reported activity to actual usage.

✅ **Best Practices**

- Monitor adoption trends → adjust licenses and training accordingly.
- Review storage utilization → plan for archiving or quota adjustments.

✅ **Use Case**
Monthly report shows Team usage growing → organization invests in training for underutilized features.

---

71. Audit Logging for Compliance & Investigations

✅ **Purpose**
Audit logging tracks **user and admin activities** for compliance, security, and forensic investigations.

✅ **Configuration Steps**

Microsoft 365 Compliance Center

1. Navigate → **Audit** → **Start recording user/admin activities**.
2. Search logs by user, activity, or date range.
3. Export results for investigations.

PowerShell

```
# Connect to Security & Compliance Center
```

```
Connect-IPPSSession


# Search audit log

Search-UnifiedAuditLog -StartDate "2025-08-01" -EndDate "2025-08-29"
-Operations SendOnBehalf, SendAs -ResultSize 500 | Export-Csv
"C:\AuditLog.csv" -NoTypeInformation
```

✅ **Validation**

- Confirm activities logged for specified users/actions.
- Check logs for anomalies or policy violations.

✅ **Best Practices**

- Enable audit logging organization-wide.
- Retain logs per compliance policy.
- Regularly review audit logs for suspicious activity.

✅ **Use Case**
Legal audit requires reviewing “Send As” actions → audit logs provide exact timestamps and users involved.

---

72. Dynamic Distribution Groups (Attribute-based Membership)

✅ **Purpose**
Dynamic distribution groups automatically include users based on **attributes** (department, location, title).

✅ **Configuration Steps**

EAC

1. Navigate → **Recipients → Groups → + Add → Dynamic Distribution Group**.
2. Configure:
    - Name, Alias.
    - Membership rules: department, state, title, or custom attributes.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Create dynamic distribution group

New-DynamicDistributionGroup -Name "SalesTeam" -RecipientFilter
"(Department -eq 'Sales')"
```

✅ **Validation**

- Send test email → only users matching criteria receive it.
- Membership updates automatically with attribute changes.

✅ **Best Practices**

- Use AD attributes consistently → ensures correct membership.
- Review membership rules periodically.

✅ **Use Case**
All users in “Marketing” department automatically added to marketing announcement emails.

---

73. Mail-Enabled Security Groups

✅ **Purpose**
Mail-enabled security groups **combine security permissions with email distribution**.

✅ **Configuration Steps**

EAC

1. Navigate → **Recipients** → **Groups** → **+ Add** → **Mail-enabled security group**.
2. Assign members → configure email address.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Create mail-enabled security group

New-DistributionGroup -Name "FinanceAdmins" -Type Security -Members
"user1@contoso.com","user2@contoso.com"
```

✅ **Validation**

- Users receive emails sent to the group.
- Group can be assigned permissions in SharePoint or Teams.

✅ **Best Practices**

- Document group purpose → avoid overlap with distribution groups.
- Review members periodically.

✅ **Use Case**
Finance Admin group receives system alerts and has access to sensitive SharePoint libraries.

---

74. Convert Distribution Group in Microsoft 365 Group

✅ **Purpose**
Upgrade legacy distribution lists → Microsoft 365 Groups for **modern collaboration tools**.

✅ **Configuration Steps**

EAC / PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Convert distribution group

Set-DistributionGroup -Identity "OldDL" -Microsoft365Group $true
```

✅ **Validation**

- Group now appears in Outlook → shared mailbox, calendar, Teams, and SharePoint accessible.

✅ **Best Practices**

- Backup DL content before conversion.
- Communicate change to users → may affect membership and access.

✅ **Use Case**
Old departmental DL converted to M365 Group → adds Teams and SharePoint integration.

---

75. Inactive Mailboxes & Compliance Archiving

✅ **Purpose**
Inactive mailboxes retain data for **compliance and legal retention** after a user is deleted.

✅ **Configuration Steps**

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Convert deleted mailbox to inactive

Set-Mailbox -Identity "user1@contoso.com" -InactiveMailbox $true


# Verify

Get-Mailbox -SoftDeletedMailbox
```

✅ **Validation**

- Mailbox retained → accessible to compliance admins.
- Emails preserved per retention policy.

✅ **Best Practices**

- Retain only required mailboxes → reduces storage costs.
- Apply retention policies consistently.

✅ **Use Case**
Employee leaves → mailbox made inactive → preserves emails for legal investigation.

---

76. Advanced Content Search & eDiscovery Export

✅ **Purpose**
Search and export emails, Teams, SharePoint, OneDrive content for **legal, compliance, or audit purposes**.

✅ **Configuration Steps**

Compliance Center

1. Navigate → **eDiscovery** → **Content Search** → **New Search**.
2. Define locations, keywords, date ranges.
3. Run search → preview → export with **PST or CSV**.

PowerShell

```
# Connect to Security & Compliance Center

Connect-IPPSSession


# Create and start content search

New-ComplianceSearch -Name "ProjectXSearch" -ExchangeLocation all
-ContentMatchQuery 'subject:"ProjectX"'

Start-ComplianceSearch -Identity "ProjectXSearch"
```

✅ **Validation**

- Preview and export content → confirm relevant results captured.

✅ **Best Practices**

- Document search parameters for compliance.
- Limit access to eDiscovery members.

✅ **Use Case**
Legal team exports emails for ProjectX → needed for contract review.

---

77. Block Ransomware & Malicious Attachments

✅ **Purpose**
Protect organizations from **malware, ransomware, and phishing emails**.

✅ **Configuration Steps**

Security & Compliance Center

1. Configure **Anti-Malware Policies → Safe Attachments / Safe Links**.
2. Block file types: `.exe`, `.js`, `.scr`.
3. Set quarantine or delete actions.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline



# Block specific attachment types

Set-HostedContentFilterPolicy -Identity "Default"
-BlockedAttachmentFileTypes ".exe",".js",".scr"
```

✅ **Validation**

- Send test malicious attachments → ensure blocked/quarantined.

✅ **Best Practices**

- Regularly update blocked file types.
- Combine with user training and DLP.

✅ **Use Case**
Emails with ransomware attachments blocked → reduces security incidents.

---

78. Advanced Email Rules for Security Compliance

✅ **Purpose**
Create **custom email rules** to enforce security and compliance automatically.

✅ **Configuration Steps**

Exchange Admin Center / PowerShell

1. Navigate → **Mail flow** → **Rules** → **+ New Rule**.
2. Example actions:
    - Block emails with sensitive content externally.
    - Append disclaimers.
    - Notify compliance team on rule triggers.

PowerShell Example

```
# Block emails with credit card numbers to external recipients

New-TransportRule -Name "Block Credit Card Data" -
```

79. Configure Safe Links & Safe Attachments in Microsoft Defender for Office 365

✅ **Purpose**
Protects users from **malicious links and attachments** in emails.

✅ **Configuration Steps**

Security & Compliance Center

1. Navigate → **Threat management** → **Policy** → **Safe Links / Safe Attachments**.
2. Enable **real-time scanning** for URLs and attachments.

3. Configure policies per user/group:
    - Block malicious URLs.
    - Detonate attachments in a virtual environment.

PowerShell

```
# Connect to Security & Compliance Center

Connect-IPPSSession


# Create safe links policy

New-SafeLinksPolicy -Name "AllUsersPolicy" -EnableSafeLinks $true
-EnableForATPUsers $true
```

✅ **Validation**

- Test by sending simulated phishing links → should be blocked or rewritten.

✅ **Best Practices**

- Apply to all users for consistent protection.
- Monitor alerts and reports.

✅ **Use Case**
Finance team receives suspicious email → Safe Links rewrites URL and blocks access → prevents phishing.

---

80. Configure Office 365 Message Encryption (OME)

✅ **Purpose**
Encrypt emails for **secure communication with internal and external recipients**.

✅ **Configuration Steps**

EAC / Microsoft 365 Compliance Center

1. Navigate → **Mail flow** → **Rules** → **+ Create new rule** → **Apply Office 365 Message Encryption**.
2. Conditions: sensitive keywords, external recipients, or specific departments.
3. Action: encrypt email.

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline



# Create OME rule for external recipients

New-TransportRule -Name "Encrypt External Finance Emails" -SentToScope
NotInOrganization -SubjectContainsWords "Financial Report" -ApplyOME
$true
```

✅ **Validation**

- Send test email → external recipient receives encrypted email.
- Check email can only be opened after authentication.

✅ **Best Practices**

- Use OME for confidential and sensitive information.
- Educate recipients on decryption steps.

✅ **Use Case**
The company sends quarterly financial statements → automatically encrypted for external partners.

---

81. Configure Microsoft 365 Sensitivity Labels & Policies

✅ **Purpose**
Sensitivity labels classify and protect **emails, documents, and sites**.

✅ **Configuration Steps**

Microsoft 365 Compliance Center

1. Navigate → **Information protection** → **Labels** → **+ Create label**.
2. Configure protection settings: encryption, content marking, visual markings.
3. Publish label via **Label Policy** to users/groups.

PowerShell

```
# Connect to Security & Compliance Center

Connect-IPPSSession


# Create sensitivity label example

New-Label -Name "Confidential" -Type Sensitivity -EncryptionEnabled $true
```

✅ **Validation**

- Apply label to email → ensure encryption and markings applied.
- Check label enforcement in Outlook, OWA, and Office apps.

✅ **Best Practices**

- Align labels with organizational classification policies.
- Educate users on proper label usage.

✅ **Use Case**
Legal documents automatically tagged as “Confidential” → protected with encryption and access restrictions.

---

82. Configure Advanced Threat Protection (ATP) Policies

✅ **Purpose**
Protects against **phishing, malware, and zero-day attacks** in Microsoft 365.

✅ **Configuration Steps**

Security & Compliance Center

1. Navigate → **Threat management** → **Policy** → **ATP Safe Links / Safe Attachments**.
2. Configure policies for **users, groups, or the entire organization**.
3. Enable **real-time scanning and detonation**.
4. Monitor reports for **blocked emails and links**.

✅ **Validation**

- Send test malicious email → ATP blocks or quarantines the message.

✅ **Best Practices**

- Combine with **DLP and sensitivity labels**.
- Review ATP reports regularly for threat trends.

✅ **Use Case**
ATP blocks phishing email containing malicious attachment → prevents ransomware infection.

---

83. Configure DLP (Data Loss Prevention) Policies

✅ **Purpose**
Prevents **sensitive data from leaving the organization** via email or documents.

✅ **Configuration Steps**

Microsoft 365 Compliance Center

1. Navigate → **Data loss prevention** → **+ Create policy**.
2. Select template (PCI, GDPR, HIPAA) → configure locations: Exchange, OneDrive, SharePoint.
3. Define rules: block, notify, encrypt.
4. Test policy → enforce.

✅ **Validation**

- Send email with sensitive content → verify policy action (block, encrypt, notify).

✅ **Best Practices**

- Start in **test mode** → review before enforcement.
- Use clear notification messages to users.

✅ **Use Case**
Emails containing credit card numbers are automatically blocked → reduces risk of data breaches.

---

84. Configure Insider Risk Management Policies

✅ **Purpose**
Detects and responds to **risky user activity** within Microsoft 365.

✅ **Configuration Steps**

Microsoft 365 Compliance Center

1. Navigate → **Insider risk management** → **Policies** → **+ Create policy**.
2. Define scenarios: data theft, policy violations, risky sharing.

3. Assign users/groups → configure alerts and actions.

✅ **Validation**

- Monitor alerts for unusual file sharing or downloads.
- Test with simulated scenarios.

✅ **Best Practices**

- Combine with **audit logs and DLP**.
- Adjust risk indicators based on organizational behavior.

✅ **Use Case**
Employee attempts to download large amounts of sensitive files → alert triggers investigation → prevents data exfiltration.

---

85. Configure Microsoft 365 Security & Compliance Alerts

✅ **Purpose**
Alerts notify admins of **security or compliance events** across Microsoft 365.

✅ **Configuration Steps**

Microsoft 365 Compliance Center / Security Center

1. Navigate → **Alerts** → **+ New alert policy**.
2. Define activity: mailbox access, admin changes, malware detection.
3. Set recipients → severity → alert actions.

✅ **Validation**

- Trigger test alert → verify notification received by admins.
- Confirm alert details are actionable.

✅ **Best Practices**

- Prioritize critical alerts → avoid alert fatigue.
- Regularly review alert policies → update with new threats.

✅ **Use Case**
Admin receives alert for unusual mailbox forwarding → investigation prevents potential data breach.

---

86. Configure Microsoft 365 Conditional Access Policies

✅ **Purpose**
Conditional Access policies **control access to Microsoft 365 resources** based on conditions like user, device, location, and risk.

✅ **Configuration Steps**

Azure AD / Microsoft 365 Admin Center

1. Navigate → **Azure Active Directory → Security → Conditional Access → + New Policy**.
2. Assign users/groups.
3. Select cloud apps (Exchange Online, SharePoint, Teams).
4. Define conditions: location, device state, client apps, risk level.
5. Set access controls:
    - Require MFA
    - Require compliant device
    - Block access
6. Enable policy → save.

✅ **Validation**

- Test sign-in with compliant and non-compliant devices.
- Confirm access granted/blocked as per policy.

✅ **Best Practices**

- Start in **report-only mode** → monitor impact.
- Apply policies incrementally → avoid locking out users.
- Review and update policies regularly.

✅ **Use Case**
The finance team can only access Exchange Online from corporate devices → MFA enforced → reduces risk of unauthorized access.

---

87. Configure Microsoft 365 Secure Score & Recommendations

✅ **Purpose**
Secure Score provides a **security assessment of Microsoft 365 environment** and actionable recommendations.

✅ **Configuration Steps**

1. Navigate → **Microsoft 365 Security Center** → **Secure Score**.
2. Review current score → identify improvement actions.
3. Implement recommended actions:
    - Enable MFA
    - Disable legacy protocols
    - Configure DLP policies
    - Apply Conditional Access
4. Track score improvements over time.

✅ **Validation**

- Monitor Secure Score dashboard → ensure recommended actions are implemented.

✅ **Best Practices**

- Prioritize high-impact recommendations.
- Assign owners for remediation tasks.
- Regularly reassess → maintain strong security posture.

✅ **Use Case**
Secure Score identifies unprotected legacy protocols → admin disables POP/IMAP → reduces risk exposure.

---

88. Configure Microsoft 365 Privileged Access Management (PAM)

✅ **Purpose**
Privileged Access Management **controls and monitors high-privilege accounts** (Global Admin, Exchange Admin) to reduce security risks.

✅ **Configuration Steps**

Microsoft 365 Compliance / Security Center

1. Navigate → **Azure AD** → **Privileged Identity Management (PIM)**.
2. Assign eligible roles → define activation requirements.
3. Configure MFA, approval workflow, and time-limited access.
4. Enable auditing and alerts for privileged role activation.

✅ **Validation**

- Activate role as eligible user → ensure MFA and approval prompts appear.

- Review activity logs for privileged account usage.

✅ **Best Practices**

- Use **just-in-time access** → avoid standing admin privileges.
- Monitor all privileged account activity.
- Require **MFA and approval workflows**.

✅ **Use Case**
Exchange Admin role assigned via PIM → only activated when needed → access automatically removed after a set period.

---

89. Configure Microsoft 365 Insider Risk Management Alerts

✅ **Purpose**
Detect and respond to **insider threats** or risky behavior in the organization.

✅ **Configuration Steps**

1. Navigate → **Compliance Center → Insider Risk Management → Policies → + Create policy**.
2. Define risk indicators:
    - Data exfiltration
    - Policy violations
    - Unusual file downloads
3. Assign users/groups → configure alert severity and recipients.
4. Enable policy → monitor alerts.

✅ **Validation**

- Trigger test scenarios → ensure alert notifications are received.

- Confirm alerts include actionable details.

✅ **Best Practices**

- Review and tune risk indicators periodically.
- Combine with audit logs, DLP, and conditional access.
- Limit access to insider risk investigations → maintain privacy compliance.

✅ **Use Case**
An employee attempts mass download of sensitive documents → alert triggers compliance review → prevents data exfiltration.

---

90. Configure Microsoft 365 eDiscovery & Legal Hold Advanced Settings

✅ **Purpose**
Advanced eDiscovery and Legal Hold help **retain, search, and export content** for legal, regulatory, and compliance investigations.

✅ **Configuration Steps**

Compliance Center

1. Navigate → **eDiscovery** → **Advanced eDiscovery** → **+ New Case**.
2. Add custodians → assign mailboxes, SharePoint sites, Teams.
3. Configure **holds**: preserve emails and documents, even if deleted.
4. Create **searches and exports**: define keywords, date ranges, and content locations.
5. Export results → PST or review in eDiscovery tool.

PowerShell Example

```
# Connect to Security & Compliance Center

Connect-IPPSSession
```

```
# Place mailbox on litigation hold

Set-Mailbox -Identity "user1@contoso.com" -LitigationHoldEnabled $true
-LitigationHoldDuration 365
```

✅ **Validation**

- Verify content remains accessible → even after deletion.
- Run test search → confirm results include all relevant items.

✅ **Best Practices**

- Document all holds and search activities.
- Retain content per **legal and regulatory requirements**.
- Review eDiscovery cases periodically → close or archive completed cases.

✅ **Use Case**
The legal department places key employee mailboxes on litigation hold → preserves data for ongoing investigation → ensures regulatory compliance.

---

91. Configure Hybrid Exchange Environment

✅ **Purpose**
Hybrid Exchange allows **coexistence between on-premises Exchange and Exchange Online** for seamless mail flow, calendar sharing, and unified management.

✅ **Configuration Steps**

1. Prepare **on-premises Exchange environment** → ensure supported version.
2. Run **Hybrid Configuration Wizard (HCW)** from Exchange Admin Center.
3. Configure:

    - Mail flow (Centralized or Direct)
    - Free/busy calendar sharing
    - Mailbox move options
4. Verify **mail routing and directory synchronization** with Azure AD Connect.

✅ **Validation**

- Test mail flow between on-premises and cloud mailboxes.
- Verify calendar sharing and free/busy lookups.

✅ **Best Practices**

- Backup on-premises Exchange environment before hybrid setup.
- Ensure **TLS certificates** are valid.
- Monitor hybrid mail flow logs.

✅ **Use Case**
Company migrates to Exchange Online gradually → hybrid setup allows coexistence → users can communicate seamlessly.

---

92. Migrate Mailboxes to Exchange Online (Cutover, Staged, Hybrid)

✅ **Purpose**
Mailbox migration moves users from on-premises Exchange to **Exchange Online** with minimal downtime.

✅ **Configuration Steps**

1. **Cutover migration**: Move all mailboxes at once → suitable for <150 users.
2. **Staged migration**: Move batches → for >150 users or gradual migration.

3. **Hybrid migration**: Use for coexistence → Exchange Online and on-premises mailboxes.

PowerShell Example (for batch migration)

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Start migration batch

New-MigrationBatch -Name "Batch1" -CSVData (Get-Content
"C:\Users.csv") -TargetDeliveryDomain "contoso.mail.onmicrosoft.com"
-AutoStart
```

✅ **Validation**

- Mailboxes appear in Exchange Online → send/receive test emails.
- Verify calendar and contacts migrated successfully.

✅ **Best Practices**

- Communicate migration schedule to users.
- Test pilot batch first.
- Monitor migration reports and troubleshoot errors promptly.

✅ **Use Case**
Company migrates 500 users → staged migration avoids disruption → Exchange Online fully deployed.

---

93. Configure Directory Synchronization (Azure AD Connect)

✅ **Purpose**
Sync on-premises AD users, groups, and attributes to **Azure AD / Microsoft 365**.

✅ **Configuration Steps**

1. Install **Azure AD Connect** on an on-premises server.
2. Choose synchronization options:
    - Password hash sync
    - Pass-through authentication
    - Federation (optional)
3. Select organizational units (OUs) to sync.
4. Verify initial sync → users/groups appear in Microsoft 365.

✅ **Validation**

- Check user accounts in Microsoft 365 Admin Center.
- Verify password sync works → test login.

✅ **Best Practices**

- Exclude unnecessary OUs → reduce sync load.
- Monitor sync logs regularly.
- Enable **staging server** for disaster recovery.

✅ **Use Case**
User accounts in on-premises AD automatically appear in Exchange Online → reduces manual account creation.

---

94. Configure Mail Flow Between On-Premises and Exchange Online

✅ **Purpose**
Ensures **reliable mail delivery and routing** in hybrid environments.

✅ **Configuration Steps**

1. Hybrid Configuration Wizard automatically configures:
    - Connectors for inbound/outbound mail flow
    - TLS encryption settings
2. Verify **MX records** → mail delivery to correct destination.
3. Test **mail flow** between on-premises and cloud users.

✅ **Validation**

- Send test emails → confirm delivery and message headers.
- Verify anti-spam policies applied as intended.

✅ **Best Practices**

- Enable logging for connectors → troubleshoot mail flow issues.
- Review SPF, DKIM, DMARC records.

✅ **Use Case**
Hybrid mail flow ensures employees on-premises and in the cloud can send/receive emails without delays.

---

95. Configure Coexistence Features (Free/Busy, GAL Sync)

✅ **Purpose**
Coexistence features maintain **consistent experience for users** during migration.

✅ **Configuration Steps**

1. Free/Busy Sharing:
    - Configured via **Hybrid Configuration Wizard** → enables calendar availability lookup.

2. Global Address List (GAL) Sync:
    - Sync on-premises GAL with Azure AD → users see all contacts.
3. Test cross-premises scheduling → verify visibility.

✅ **Validation**

- Schedule meetings → free/busy info visible.
- Verify GAL entries match on-premises AD.

✅ **Best Practices**

- Use **Address Book Policies** if required for segmented GALs.
- Periodically verify sync consistency.

✅ **Use Case**
Employees schedule meetings → see availability of both cloud and on-premises colleagues → seamless collaboration.

---

96. Configure Hybrid Public Folders

✅ **Purpose**
Allows **on-premises public folders** to coexist with **Exchange Online**.

✅ **Configuration Steps**

1. Run **Hybrid Configuration Wizard** → enable public folder coexistence.
2. Sync public folder hierarchy to Exchange Online.
3. Assign permissions → users can access folders from Outlook/OWA.

✅ **Validation**

- Test access to public folders → create, read, and post items.

- Verify cross-premises users can access folders.

✅ **Best Practices**

- Migrate only required public folders → reduce complexity.
- Monitor replication → ensure consistency.

✅ **Use Case**
Team uses shared public folder for project documents → available to all users during hybrid migration.

---

97. Configure Exchange Online Protection (EOP) Policies

✅ **Purpose**
Protects organizations from **spam, malware, and phishing attacks**.

✅ **Configuration Steps**

1. Navigate → **Security & Compliance** → **Threat Management** → **Policy** → **Anti-spam / Anti-malware**.
2. Configure policies:
    - Spam filtering
    - Connection filtering
    - Malware detection and quarantine
3. Assign policies to all users/groups → save.

✅ **Validation**

- Monitor quarantine → confirm malicious emails blocked.
- Send test spam → verify filtering.

✅ **Best Practices**

- Enable **zero-hour auto purge** → remove harmful emails quickly.
- Review filtering reports weekly.

✅ **Use Case**
Employees no longer receive phishing emails → reduces security incidents.

---

98. Configure Shared Mailbox Migration from On-Premises

✅ **Purpose**
Move shared mailboxes from on-premises to Exchange Online without disruption.

✅ **Configuration Steps**

1. Prepare shared mailbox → ensure no licensing conflicts.
2. Use **Hybrid Configuration Wizard / PowerShell** to migrate.
3. Assign **permissions post-migration** → Full Access, Send As, Send on Behalf.

✅ **Validation**

- Users can access migrated mailboxes → send/receive test emails.

✅ **Best Practices**

- Communicate mailbox migration schedule to users.
- Verify permissions after migration.

✅ **Use Case**
Support team shared mailbox migrated → uninterrupted email access.

---

99. Configure Teams & M365 Groups Coexistence

✅ **Purpose**
Ensure **Teams, Microsoft 365 Groups, and Exchange Online** integrate properly in hybrid environments.

✅ **Configuration Steps**

1. Enable **Teams upgrade coexistence mode** in Teams Admin Center.
2. Configure **M365 Group mailbox policies** for Teams.
3. Ensure **calendar and mailbox integration** works across platforms.

✅ **Validation**

- Create a Team → associated mailbox appears in Exchange Online.
- Users can schedule Team meetings via Outlook.

✅ **Best Practices**

- Standardize naming conventions for Teams and Groups.
- Educate users on mailbox and Team integration.

✅ **Use Case**
Project Phoenix Team → uses Teams for collaboration → mailbox accessible in Outlook → shared files, chat, and calendar unified.

---

100. Perform Tenant-to-Tenant Migration

✅ **Purpose**
Tenant-to-Tenant migration allows **mergers, acquisitions, or divestitures** to consolidate Microsoft 365 tenants.

✅ **Configuration Steps**

1. Plan migration → inventory users, mailboxes, Teams, SharePoint, OneDrive.
2. Use third-party migration tools (BitTitan, Quest, etc.) or Microsoft native tools.
3. Migrate users/mailboxes → update DNS and MX records.
4. Validate **mail flow, calendar, and Teams** after migration.

✅ **Validation**

- Test email delivery → cross-tenant communication works.
- Confirm Teams, SharePoint, and OneDrive data accessible.

✅ **Best Practices**

- Perform pilot migration → minimize downtime.
- Communicate to users → provide new credentials and access instructions.
- Document the entire migration process.

✅ **Use Case**
Company merges with another → tenant-to-tenant migration consolidates users and data → single Microsoft 365 environment.

101. Configure Shared Mailbox Permissions in Bulk

✅ **Purpose**
Efficiently assign **Full Access, Send As, or Send on Behalf permissions** to multiple users for shared mailboxes.

✅ **Configuration Steps**

PowerShell Example

```
# Connect to Exchange Online

Connect-ExchangeOnline



# Assign Full Access permissions in bulk

Import-Csv "C:\SharedMailboxUsers.csv" | ForEach-Object {

    Add-MailboxPermission -Identity $_.Mailbox -User $_.User
-AccessRights FullAccess -InheritanceType All

}
```

```
# Assign Send As permissions in bulk

Import-Csv "C:\SharedMailboxUsers.csv" | ForEach-Object {

    Add-RecipientPermission -Identity $_.Mailbox -Trustee $_.User
-AccessRights SendAs

}
```

✅ **Validation**

- Users can access a shared mailbox → send/receive emails.
- Test Send As and Send on Behalf functionality.

✅ **Best Practices**

- Keep CSV documentation of permission assignments.
- Periodically review permissions → remove unnecessary access.

✅ **Use Case**
The IT department sets Full Access for the support team → ensures all team members can respond from a shared mailbox.

---

102. Configure Office 365 Message Trace for Compliance

✅ **Purpose**
Track email delivery and troubleshoot **compliance, security, and delivery issues**.

✅ **Configuration Steps**

1. Navigate → **Exchange Admin Center** → **Mail flow** → **Message trace**.
2. Select date range, sender, recipient, and status.

3. Run trace → download results for compliance records.

PowerShell Example

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Trace email

Get-MessageTrace -StartDate "2025-08-01" -EndDate "2025-08-29"
-SenderAddress "user@contoso.com"
```

✅ **Validation**

- Confirm emails delivered, delayed, or blocked.
- Export and retain for compliance audits.

✅ **Best Practices**

- Schedule periodic message trace audits.
- Use trace data to identify phishing or data loss events.

✅ **Use Case**
Compliance team reviews email traces → ensures sensitive information was not sent externally by mistake.

---

103. Configure Microsoft 365 Data Classification

✅ **Purpose**
Classify emails and documents for **regulatory compliance and security enforcement**.

✅ **Configuration Steps**

1. Navigate → **Microsoft 365 Compliance** → **Information Protection** → **Labels**.
2. Create labels: Confidential, Internal, Public.
3. Apply encryption, access restrictions, or visual markings.
4. Publish labels via **Label Policy** → assign to users/groups.

✅ **Validation**

- Test by applying labels → confirm encryption and markings appear.

✅ **Best Practices**

- Align with corporate data classification policies.
- Train users on proper label usage.

✅ **Use Case**
Financial documents automatically tagged as “Confidential” → encrypted → restricted access to authorized users only.

---

104. Configure Exchange Online Mailbox Auto-Forwarding Restrictions

✅ **Purpose**
Prevent unauthorized **automatic email forwarding** to external recipients → reduces data leaks.

✅ **Configuration Steps**

Exchange Admin Center / PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline


# Disable auto-forwarding for all users
```

```
Set-RemoteDomain Default -AutoForwardEnabled $false
```

✅ **Validation**

- Test sending auto-forward rule to external address → confirm blocked.
- Monitor alerts for attempted forwarding.

✅ **Best Practices**

- Combine with DLP and sensitivity labels.
- Communicate policy changes to users.

✅ **Use Case**
User attempts to forward company emails to personal account → blocked → prevents data breach.

---

105. Configure Exchange Online Quarantine Policies

✅ **Purpose**
Manage **spam, phishing, and malware emails** before they reach user mailboxes.

✅ **Configuration Steps**

1. Navigate → **Security & Compliance** → **Threat Management** → **Review** → **Quarantine Policies**.
2. Configure policies:
    - Who can release messages
    - Retention period
    - Notifications to users
3. Assign policies to users/groups.

✅ **Validation**

- Confirm phishing/spam emails quarantined.
- Test user access to release legitimate messages.

✅ **Best Practices**

- Educate users on quarantined email review.
- Regularly monitor quarantine reports.

✅ **Use Case**
Users no longer receive phishing emails directly → admin reviews and releases safe messages.

---

106. Configure Mailbox Auto-Reply / Out-of-Office Policies

✅ **Purpose**
Set up **automatic replies for vacation, leave, or shared mailboxes**.

✅ **Configuration Steps**

EAC / PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline



# Enable automatic replies

Set-MailboxAutoReplyConfiguration -Identity "user@contoso.com"
-AutoReplyState Enabled -InternalMessage "I am out of office"
-ExternalMessage "I am out of office"
```

✅ **Validation**

- Send test email → verify automatic reply received internally and externally.

✅ **Best Practices**

- Include alternate contact information in the message.
- Disable after the leave period ends.

✅ **Use Case**
Employee on vacation → automatic replies inform clients → ensures communication continuity.

---

107. Configure Mailbox Delegation Policies

✅ **Purpose**
Allow **Full Access, Send As, or Send on Behalf permissions** on user or shared mailboxes.

✅ **Configuration Steps**

EAC / PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline



# Assign Send on Behalf

Set-Mailbox -Identity "Manager@contoso.com" -GrantSendOnBehalfTo
"Assistant@contoso.com"
```

✅ **Validation**

- Test delegated access → verify actions performed successfully.

✅ **Best Practices**

- Document delegated permissions.
- Review delegation periodically.

✅ **Use Case**
The assistant can send emails on behalf of the manager → maintain workflow efficiency.

---

108. Configure Shared Mailbox Auto-Mapping

✅ **Purpose**
Automatically maps shared mailboxes to users' Outlook → no manual setup required.

✅ **Configuration Steps**

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline



# Grant Full Access without auto-mapping

Add-MailboxPermission -Identity "SharedMailbox@contoso.com" -User
"User1@contoso.com" -AccessRights FullAccess -AutoMapping $false
```

✅ **Validation**

- Confirm mailbox appears in Outlook → auto-mapped.
- Test send/receive emails.

✅ **Best Practices**

- Use auto-mapping only for frequent access.
- Review mailbox access periodically.

✅ **Use Case**
The support team automatically sees a shared mailbox in Outlook → efficient handling of support emails.

---

109. Configure Microsoft 365 Retention Policies

✅ **Purpose**
Retain or delete emails and documents **automatically for compliance or data governance**.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **Information Governance** → **Retention Policies**.
2. Create policy: select locations (Exchange, SharePoint, OneDrive).
3. Define retention duration and actions (retain, delete, trigger event-based retention).
4. Assign policy to users/groups.

✅ **Validation**

- Test retention → emails older than retention period deleted/retained.

✅ **Best Practices**

- Align policies with legal/regulatory requirements.
- Monitor policy application and effectiveness.

✅ **Use Case**
Company retains financial emails for 7 years → ensures compliance → automates deletion after retention period.

---

110. Configure Microsoft 365 Mailbox Audit Logging

✅ **Purpose**
Track mailbox actions (send, delete, access) for **security, compliance, and investigations**.

✅ **Configuration Steps**

PowerShell

```
# Connect to Exchange Online

Connect-ExchangeOnline
```

```
# Enable mailbox audit logging

Set-Mailbox -Identity "user@contoso.com" -AuditEnabled $true
-AuditLogAgeLimit 90



# Specify actions to audit

Set-Mailbox -Identity "user@contoso.com" -AuditAdmin SendOnBehalf,
SendAs, Update
```

✅ **Validation**

- Search audit log → confirm actions logged.
- Test by performing audited actions → verify entry recorded.

✅ **Best Practices**

- Enable auditing for high-risk users by default.
- Retain audit logs per compliance requirements.
- Review logs regularly.

✅ **Use Case**
Admin investigates suspicious email deletion → mailbox audit log provides timestamps and responsible user → resolves issue.

111. Configure Microsoft 365 Message Encryption for External Recipients

✅ **Purpose**
Encrypt emails sent to **external recipients** to protect sensitive data.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **Mail flow** → **Rules** → **+ Create new rule**.
2. Condition: Sent to external recipients.
3. Action: Apply **Office 365 Message Encryption (OME)**.
4. Save and enforce rules.

PowerShell Example

```
Connect-ExchangeOnline

New-TransportRule -Name "Encrypt External Emails" -SentToScope
NotInOrganization -ApplyOME $true
```

✅ **Validation**

- Send test email to external address → recipient receives encrypted email.

✅ **Best Practices**

- Use templates for recurring encryption scenarios.
- Train recipients to open encrypted messages.

✅ **Use Case**
The legal team sends sensitive contracts externally → automatically encrypted → secure communication.

---

112. Configure Shared Mailbox Auto-Reply for Multiple Users

✅ **Purpose**
Provide **automatic replies** from shared mailboxes for out-of-office or notifications.

✅ **Configuration Steps**

PowerShell Example

```
Connect-ExchangeOnline

Set-MailboxAutoReplyConfiguration -Identity "Support@contoso.com"
-AutoReplyState Enabled -InternalMessage "We received your request"
-ExternalMessage "We received your request"
```

✅ **Validation**

- Send test email → auto-reply received by internal and external users.

✅ **Best Practices**

- Update message regularly for accurate information.
- Include alternative contact if needed.

✅ **Use Case**
Support shared mailbox → auto-reply confirms receipt of requests → improves customer experience.

---

113. Configure Exchange Online Mailbox Delegation via Groups

✅ **Purpose**
Assign **Full Access, Send As, or Send on Behalf** permissions to multiple users via **security or distribution groups**.

✅ **Configuration Steps**

PowerShell Example

```
Connect-ExchangeOnline

Add-MailboxPermission -Identity "Manager@contoso.com" -User
"FinanceGroup" -AccessRights FullAccess

Add-RecipientPermission -Identity "Manager@contoso.com" -Trustee
"FinanceGroup" -AccessRights SendAs
```

✅ **Validation**

- Group members can access mailboxes → send/receive as intended.

✅ **Best Practices**

- Maintain group membership accurately → ensures correct access.
- Review delegated permissions regularly.

✅ **Use Case**
The finance department group granted Send As permissions → multiple team members can respond on behalf of the manager.

---

114. Configure Office 365 ATP Anti-Phishing Policies

✅ **Purpose**
Protect users from **phishing attacks** in emails.

✅ **Configuration Steps**

1. Navigate → **Security & Compliance** → **Threat Management** → **Policy** → **Anti-Phishing**.
2. Create custom policy → assign to users/groups.
3. Configure:
    - Impersonation protection
    - Domain spoofing protection
    - User notifications
4. Enable policy → save.

✅ **Validation**

- Send a test phishing email → verify it's blocked or quarantined.

✅ **Best Practices**

- Combine with **Safe Links** and **Safe Attachments**.
- Regularly review reports and tweak policies.

✅ **Use Case**
CEO impersonation attempt → ATP detects → email quarantined → prevents phishing attack.

---

115. Configure Office 365 ATP Safe Links for SharePoint & OneDrive

✅ **Purpose**
Protect users from **malicious links in documents stored in SharePoint or OneDrive**.

✅ **Configuration Steps**

1. Navigate → **Security & Compliance** → **Safe Links**.
2. Enable **real-time scanning** for SharePoint, OneDrive, and Teams.
3. Apply policies to users/groups.

✅ **Validation**

- Click test malicious URL in SharePoint/OneDrive → blocked.

✅ **Best Practices**

- Combine with **Safe Attachments** policies.
- Educate users about safe document sharing practices.

✅ **Use Case**
Finance folder in SharePoint → Safe Links blocks malicious URLs → prevents malware spread.

---

116. Configure Exchange Online Spam Filter Policies

✅ **Purpose**
Prevent **spam emails from reaching user inboxes**.

✅ **Configuration Steps**

1. Navigate → **Security & Compliance** → **Threat Management** → **Anti-Spam**.
2. Create a custom spam filter policy → assign to users/groups.
3. Configure actions: move to Junk, quarantine, notify admin.

✅ **Validation**

- Send test spam email → verify action applied.
- Check quarantine for blocked messages.

✅ **Best Practices**

- Regularly monitor spam reports.
- Combine with **Safe Sender / Blocked Sender Lists**.

✅ **Use Case**
Spam emails filtered before reaching employees → reduces inbox clutter → protects from phishing.

---

117. Configure Exchange Online Quarantine Notification Policies

✅ **Purpose**
Notify users when **emails are quarantined** for spam, malware, or phishing.

✅ **Configuration Steps**

1. Navigate → **Security & Compliance** → **Threat Management** → **Review** → **Quarantine Policies**.

2. Enable **user notification** → frequency: daily/weekly.
3. Customize notification email content.

✅ **Validation**

- Test by sending spam email → notification received by users.

✅ **Best Practices**

- Educate users on reviewing quarantined messages.
- Avoid excessive notifications → reduce alert fatigue.

✅ **Use Case**
Employees receive daily quarantine notifications → can release legitimate emails → improves workflow.

---

118. Configure Microsoft 365 Sensitivity Labels for Teams & Groups

✅ **Purpose**
Apply **data protection policies** to Teams, SharePoint, and Groups based on sensitivity labels.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **Information Protection** → **Labels**.
2. Create sensitivity label → configure encryption, access, and external sharing.
3. Publish label → assign to Teams/Groups.

✅ **Validation**

- Label applied to Team → access restricted → external sharing blocked.

✅ **Best Practices**

- Align labels with organizational classification policies.
- Review label usage periodically.

✅ **Use Case**
HR Team labeled “Confidential” → only HR users access files → external sharing restricted.

---

119. Configure Microsoft 365 Data Loss Prevention (DLP) Policies for Teams

✅ **Purpose**
Prevent **sensitive data leaks via Teams chat and channels**.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **Data Loss Prevention** → **+ Create Policy**.
2. Select location: Teams chat, Teams channel messages.
3. Define rules → block, notify, encrypt.
4. Assign to users/groups → enforce policy.

✅ **Validation**

- Send a test message with sensitive content → action triggered.
- Verify notifications and block actions.

✅ **Best Practices**

- Start in **test mode** → monitor before enforcement.
- Communicate DLP rules to users.

✅ **Use Case**
Employee attempts to share Social Security numbers in Teams → DLP blocks → prevents sensitive data leak.

---

120. Configure Microsoft 365 Retention Labels for Teams, SharePoint, & OneDrive

✅ **Purpose**
Retain or delete **Teams messages and documents** automatically for compliance.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **Information Governance** → **Labels**.
2. Create retention label → specify retention period and actions.
3. Publish label via **Label Policy** → assign to Teams, SharePoint, OneDrive.

✅ **Validation**

- Apply label to Team or document → retention enforced.
- Test deletion/retention according to policy.

✅ **Best Practices**

- Align retention with regulatory requirements.
- Monitor label application and adjust policies as needed.

✅ **Use Case**
Project Team messages retained for 7 years → legal compliance → automatic deletion after retention period.

---

121. Configure Microsoft 365 Retention Policies for Exchange Online Mailboxes

✅ **Purpose**
Automatically retain or delete emails in user mailboxes for **compliance and regulatory requirements**.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **Information Governance** → **Retention Policies** → **+ Create Policy**.
2. Select locations: Exchange Online mailboxes.
3. Define retention actions: retain, delete, or trigger event-based retention.
4. Assign policy to users or groups → publish.

✅ **Validation**

- Verify older emails are retained/deleted according to policy.
- Test by sending emails and monitoring application of policy.

✅ **Best Practices**

- Align with corporate and regulatory requirements.
- Monitor and adjust policies periodically.

✅ **Use Case**
Financial emails retained for 7 years automatically → ensures compliance.

---

122. Configure Microsoft 365 Retention Policies for SharePoint and OneDrive

✅ **Purpose**
Retain or delete documents in **SharePoint and OneDrive** for compliance.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **Information Governance** → **Retention Policies**.
2. Select locations: SharePoint sites and OneDrive accounts.
3. Define retention period and actions → publish.

✅ **Validation**

- Confirm files are retained or deleted according to retention rules.
- Test on sample document libraries.

✅ **Best Practices**

- Start with non-critical data → validate before organization-wide deployment.
- Review reports to confirm policy enforcement.

✅ **Use Case**
Project documents in SharePoint retained for 10 years → ensures regulatory compliance.

---

123. Configure Microsoft 365 eDiscovery & Legal Hold for Teams

✅ **Purpose**
Preserve Teams messages and channel content for **legal and compliance investigations**.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **eDiscovery** → **Advanced eDiscovery** → **+ New Case**.
2. Add custodians → select Teams messages and channels.
3. Apply legal hold → preserve content.
4. Create searches → export results as needed.

✅ **Validation**

- Verify messages are preserved → test deletion attempt.
- Run search → confirm expected content returned.

✅ **Best Practices**

- Limit custodians to necessary users.
- Document holds and searches for audits.

✅ **Use Case**
HR places legal hold on employee Teams chat → preserves evidence during investigation.

---

124. Configure Microsoft 365 eDiscovery & Legal Hold for SharePoint & OneDrive

✅ **Purpose**
Preserve **documents and files** stored in SharePoint or OneDrive for compliance.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **eDiscovery** → **+ New Case**.
2. Add custodians → select SharePoint sites or OneDrive accounts.
3. Enable litigation hold → preserve content.
4. Create searches → export for review.

✅ **Validation**

- Verify files remain accessible → even if deleted by the user.

✅ **Best Practices**

- Document preserved locations and custodians.
- Periodically review holds → remove when no longer needed.

✅ **Use Case**
Legal team preserves documents from departing employee's OneDrive → supports investigation.

---

125. Configure Microsoft 365 Audit Logging for Mailboxes and Teams

✅ **Purpose**
Track user and admin activities for **security, compliance, and investigations**.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **Audit** → **Start recording user and admin activities**.
2. Select activities: mailbox login, message deletion, Teams messages, file access.
3. Generate reports or export for review.

✅ **Validation**

- Perform test actions → verify audit logs capture activity.

✅ **Best Practices**

- Enable logging for high-risk users by default.
- Retain logs per compliance requirements.

✅ **Use Case**
Admin investigates suspicious email deletion → audit logs confirm responsible user → issue resolved.

---

126. Configure Microsoft 365 Message Trace for Security Investigations

✅ **Purpose**
Trace email delivery for **compliance, security investigations, or troubleshooting**.

✅ **Configuration Steps**

1. Navigate → **Exchange Admin Center** → **Mail flow** → **Message trace**.

2. Filter by sender, recipient, date, status.
3. Run trace → download results.

✅ **Validation**

- Confirm email path and delivery status.
- Use PowerShell for advanced trace queries.

✅ **Best Practices**

- Schedule periodic message trace audits.
- Retain traces for compliance review.

✅ **Use Case**
Investigating a phishing attempt → message trace confirms delivery path → mitigates risk.

---

127. Configure Microsoft 365 Anti-Malware & Safe Attachments Policies

✅ **Purpose**
Protect users from **malicious attachments** in emails.

✅ **Configuration Steps**

1. Navigate → **Security & Compliance** → **Threat Management** → **Policy** → **Safe Attachments**.
2. Enable policy → choose action: block, replace, or monitor.
3. Apply to all users or specific groups.

✅ **Validation**

- Send test attachment → confirm action applied (blocked/quarantined).

✅ **Best Practices**

- Combine with Anti-Phishing and Safe Links policies.
- Monitor weekly reports.

✅ **Use Case**
Malware attachment blocked from reaching employees → reduces infection risk.

---

128. Configure Microsoft 365 Anti-Spam & Phishing Policies

✅ **Purpose**
Prevent **spam and phishing emails** from reaching mailboxes.

✅ **Configuration Steps**

1. Navigate → **Security & Compliance** → **Threat Management** → **Policy** → **Anti-Spam**.
2. Create custom policy → assign to users/groups.
3. Enable features: connection filtering, spoof intelligence, quarantine actions.

✅ **Validation**

- Send test spam/phishing email → verify blocked or quarantined.

✅ **Best Practices**

- Regularly review spam reports → adjust policies.
- Train users to recognize phishing attempts.

✅ **Use Case**
Employees no longer receive CEO impersonation phishing emails → reduces security incidents.

---

129. Configure Exchange Online Mailbox Quotas & Alerts

✅ **Purpose**
Manage mailbox **storage limits and notifications** for users.

✅ **Configuration Steps**

1. Navigate → **Exchange Admin Center** → **Recipients** → **Mailboxes** → **Select User** → **Mailbox Usage**.
2. Set quotas:
    - Warning limit
    - Prohibit send limit
    - Prohibit send and receive limit
3. Enable email notifications for nearing quota.

✅ **Validation**

- Test mailbox → verify warnings and restrictions applied.

✅ **Best Practices**

- Monitor quota usage regularly.
- Adjust limits based on user role and storage requirements.

✅ **Use Case**
User reaches mailbox limit → receives warning → deletes unnecessary emails → prevents disruption.

---

130. Configure Exchange Online Mailbox Auto-Expanding Archive

✅ **Purpose**
Provide users with **unlimited archive storage** by enabling auto-expanding archives.

✅ **Configuration Steps**

1. Navigate → **Exchange Admin Center** → **Recipients** → **Mailboxes** → **Archive**.

2. Enable archive → set auto-expanding archive.

PowerShell Example

```
Connect-ExchangeOnline

Enable-Mailbox -Identity "user@contoso.com" -Archive
```

✅ **Validation**

- Archive mailbox visible in Outlook/OWA → stores emails beyond primary quota.
- Send test email → verify archive accessible.

✅ **Best Practices**

- Combine with retention policies → automatically move old emails to archive.
- Educate users about accessing archive mailboxes.

✅ **Use Case**
Employee mailbox exceeds 100 GB → auto-expanding archive ensures continued email storage without manual intervention.

---

131. Configure Microsoft 365 Shared Mailbox Auto-Expanding Archive

✅ **Purpose**
Provide **shared mailboxes** with unlimited archive storage by enabling auto-expanding archives.

✅ **Configuration Steps**

1. Navigate → **Exchange Admin Center** → **Recipients** → **Shared Mailboxes** → **Archive**.
2. Enable archive → set auto-expanding archive.

PowerShell Example

```
Connect-ExchangeOnline

Enable-Mailbox -Identity "Support@contoso.com" -Archive
```

✅ **Validation**

- Shared mailbox archive visible in Outlook/OWA → stores emails beyond primary quota.

✅ **Best Practices**

- Combine with retention policies → automatically move old emails to archive.
- Inform users of archive location and access.

✅ **Use Case**
Support shared mailbox exceeds primary quota → auto-expanding archive ensures continued email storage.

---

132. Configure Microsoft 365 Retention Policies for Groups and Teams

✅ **Purpose**
Apply retention rules to **Teams messages and Microsoft 365 Group emails** for compliance.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **Information Governance** → **Retention Policies**.
2. Select locations: Teams chats, Teams channels, Group mailboxes.
3. Define retention period and actions → publish policy.

✅ **Validation**

- Messages or emails retained/deleted according to policy.
- Test on sample Teams channels or Group mailbox.

✅ **Best Practices**

- Align policies with regulatory requirements.
- Periodically review applications and adjust.

✅ **Use Case**
Project Team messages retained for 7 years → ensures regulatory compliance.

---

133. Configure Exchange Online Mailbox Litigation Hold

✅ **Purpose**
Preserve **all mailbox content** for compliance or legal investigations.

✅ **Configuration Steps**

1. Navigate → **Exchange Admin Center** → **Recipients** → **Mailboxes** → **Select User** → **Litigation Hold**.
2. Enable hold → optionally set hold duration.

PowerShell Example

```
Connect-ExchangeOnline

Set-Mailbox -Identity "user@contoso.com" -LitigationHoldEnabled $true
-LitigationHoldDuration 365
```

✅ **Validation**

- Test deletion of emails → items preserved in Recoverable Items folder.

✅ **Best Practices**

- Apply only to required users → reduces storage overhead.
- Monitor mailbox size and adjust archive policies.

✅ **Use Case**
Employee mailbox under investigation → all emails preserved for 1 year automatically.

---

134. Configure Exchange Online Mailbox In-Place Hold

✅ **Purpose**
Preserve **specific mailbox items** based on query for compliance/legal reasons.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **eDiscovery** → **In-Place Hold**.
2. Create hold → define query (keywords, dates, senders).
3. Apply hold to selected mailboxes.

✅ **Validation**

- Test by deleting matching items → items retained according to query.

✅ **Best Practices**

- Document holds criteria.
- Periodically review and remove holds when no longer required.

✅ **Use Case**
HR places in-place hold on emails mentioning “termination” → preserves relevant messages for investigation.

---

135. Configure Office 365 Advanced Threat Protection (ATP) Safe Attachments

✅ **Purpose**
Protect users from **unknown malware in attachments**.

✅ **Configuration Steps**

1. Navigate → **Security & Compliance** → **Threat Management** → **Safe Attachments**.
2. Create policy → choose action: block, replace, monitor.
3. Apply to all mailboxes or specific groups.

✅ **Validation**

- Send test attachment → blocked/quarantined or monitored.

✅ **Best Practices**

- Combine with Safe Links → full protection against attachments and malicious URLs.
- Review policy reports regularly.

✅ **Use Case**
Finance receives suspicious Excel attachments → blocked by Safe Attachments → prevents infection.

---

136. Configure Office 365 Advanced Threat Protection (ATP) Safe Links

✅ **Purpose**
Protect users from **malicious URLs in emails, Teams, SharePoint, and OneDrive**.

✅ **Configuration Steps**

1. Navigate → **Security & Compliance** → **Threat Management** → **Safe Links**.
2. Enable real-time scanning → apply to emails, Teams, SharePoint, OneDrive.
3. Assign policy to users/groups.

✅ **Validation**

- Click test malicious URL → blocked or warned.

✅ **Best Practices**

- Combine with anti-phishing policies.
- Educate users to report unsafe links.

✅ **Use Case**
User clicks malicious link in Teams → Safe Links blocks access → prevents malware infection.

---

137. Configure Microsoft 365 DLP Policies for SharePoint and OneDrive

✅ **Purpose**
Prevent sensitive data leaks via **documents stored in SharePoint or OneDrive**.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **Data Loss Prevention** → **+ Create Policy**.
2. Select locations: SharePoint sites, OneDrive accounts.
3. Define rules → block, notify, or encrypt sensitive content.

✅ **Validation**

- Test by uploading a document with sensitive content → policy triggered.

✅ **Best Practices**

- Start in test mode → monitor before enforcement.
- Communicate rules to users.

✅ **Use Case**
Employee attempts to upload documents containing credit card numbers → DLP blocks → prevents data leak.

---

138. Configure Microsoft 365 DLP Policies for Teams

✅ **Purpose**
Prevent **sensitive data sharing in Teams messages and channels**.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **Data Loss Prevention** → **+ Create Policy**.
2. Select Teams chats and channel messages.
3. Define rules → notify, block, or encrypt messages.

✅ **Validation**

- Test sending sensitive content → policy triggered.

✅ **Best Practices**

- Educate users → explain why certain content is blocked.
- Monitor incidents → refine rules as needed.

✅ **Use Case**
Employee attempts to share SSN via Teams chat → DLP blocks message → ensures compliance.

---

139. Configure Microsoft 365 Insider Risk Management Policies

✅ **Purpose**
Detects and mitigate **internal security threats** in Exchange Online, Teams, SharePoint, and OneDrive.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **Insider Risk Management** → **+ Create Policy**.
2. Select scenarios: data exfiltration, policy violations.
3. Assign users/groups → set risk indicators and thresholds.

✅ **Validation**

- Review alerts and incidents → verify policy triggers appropriately.

✅ **Best Practices**

- Limit scope to high-risk users initially.
- Regularly refine risk indicators and thresholds.

✅ **Use Case**
Alerts triggered when an employee attempts mass download of sensitive files → prevent insider data leak.

---

140. Configure Microsoft 365 Communication Compliance Policies

✅ **Purpose**
Monitor and remediate **inappropriate or non-compliant communication** across Exchange, Teams, and Yammer.

✅ **Configuration Steps**

1. Navigate → **Compliance Center** → **Communication Compliance** → **+ Create Policy**.
2. Select locations: Exchange Online, Teams messages, Yammer posts.
3. Define rules: offensive language, harassment, or sensitive information sharing.

✅ **Validation**

- Test communication → policy flags inappropriate content.
- Review alerts and incidents.

✅ **Best Practices**

- Combine with user training → improve compliance culture.

- Adjust rules as organizational needs evolve.

✅ **Use Case**
HR monitors Team communication → flags harassment language → takes corrective action → ensures a safe workplace.

---

141. Configure Microsoft 365 Retention Policies for Hybrid Environments

✅ **Purpose**
Apply consistent retention rules across **on-premises Exchange and Exchange Online mailboxes** in hybrid setups.

✅ **Configuration Steps**

1. Ensure **Hybrid Configuration** is in place.
2. Navigate → **Compliance Center** → **Retention Policies** → **+ Create Policy**.
3. Select locations: Exchange Online and on-premises mailboxes (via hybrid configuration).
4. Define retention duration and actions → publish.

✅ **Validation**

- Verify retention rules apply to both on-prem and cloud mailboxes.

✅ **Best Practices**

- Align hybrid retention policies with corporate and legal requirements.
- Test on pilot mailboxes before organization-wide deployment.

✅ **Use Case**
Company retains emails for 7 years → ensures compliance across hybrid environments.

---

142. Configure Exchange Online Hybrid Mailbox Migration

✅ **Purpose**
Move **mailboxes from on-premises Exchange to Exchange Online** for cloud adoption.

✅ **Configuration Steps**

1. Set up **Hybrid Configuration Wizard**.
2. Prepare mailboxes → ensure Active Directory attributes synced.
3. Initiate migration batch → monitor progress.
4. Complete migration → decommission on-prem mailbox if needed.

✅ **Validation**

- Confirm mailbox content is intact in Exchange Online.
- Test sending/receiving emails.

✅ **Best Practices**

- Communicate migration schedules to users.
- Backup critical mailboxes before migration.

✅ **Use Case**
IT migrates 100 user mailboxes to Exchange Online → minimal downtime → improves cloud adoption.

---

143. Configure Exchange Online Public Folder Migration

✅ **Purpose**
Migrate **on-premises public folders** to Exchange Online while preserving access and permissions.

✅ **Configuration Steps**

1. Prepare public folders → clean up unused folders.
2. Create **public folder mailboxes** in Exchange Online.

3. Use **Exchange PowerShell** to migrate content and permissions.
4. Verify migration → decommission on-prem public folders.

✅ **Validation**

- Confirm folder hierarchy and content is intact.
- Test user access and permissions.

✅ **Best Practices**

- Migrate during low-usage hours.
- Document permissions and folder mapping.

✅ **Use Case**
Company moves legacy public folders to Exchange Online → improves cloud collaboration.

---

144. Configure Exchange Online Cross-Premises Mail Flow

✅ **Purpose**
Ensure **mail routing between on-premises Exchange and Exchange Online** in hybrid setups.

✅ **Configuration Steps**

1. Configure **send and receive connectors** in on-prem Exchange and Exchange Online.
2. Test mail flow between environments → internal and external.
3. Enable transport rules if needed for compliance.

✅ **Validation**

- Send test emails → verify delivery.
- Check message trace for correct routing.

✅ **Best Practices**

- Monitor hybrid mail flow logs regularly.
- Maintain connectors documentation.

✅ **Use Case**
User on-prem sends email to cloud user → seamless delivery → hybrid environment works correctly.

---

145. Configure Exchange Online Transport Rules for Hybrid Environment

✅ **Purpose**
Enforce **mail flow rules** across hybrid mailboxes for compliance or security.

✅ **Configuration Steps**

1. Navigate → **Exchange Admin Center** → **Mail flow** → **Rules** → **+ Create Rule**.
2. Define conditions and actions (e.g., block, redirect, apply disclaimer).
3. Apply to hybrid mailboxes → test.

✅ **Validation**

- Test rule by sending sample emails.
- Check logs → ensure proper rule enforcement.

✅ **Best Practices**

- Document all rules → avoid conflicts.
- Test rules before applying globally.

✅ **Use Case**
Automatically apply disclaimers to emails sent from hybrid users → ensures legal compliance.

---

146. Configure Exchange Online Mailbox Delegation Across Hybrid Environment

✅ **Purpose**
Allow **Full Access, Send As, or Send on Behalf permissions** for hybrid mailboxes.

✅ **Configuration Steps**

1. Assign permissions via **Exchange Admin Center or PowerShell**.
2. For hybrid mailboxes, ensure proper **Active Directory sync**.
3. Test delegated access for all hybrid users.

✅ **Validation**

- Confirm delegated users can access mailboxes → send emails on behalf.

✅ **Best Practices**

- Maintain proper documentation.
- Review delegation permissions periodically.

✅ **Use Case**
Executive assistant granted Send As permission for hybrid mailbox → seamless workflow.

---

147. Configure Exchange Online Hybrid Free/Busy and Calendar Sharing

✅ **Purpose**
Enable **cross-premises calendar visibility** for scheduling meetings.

✅ **Configuration Steps**

1. Ensure **Hybrid Configuration Wizard** completed.
2. Configure **Availability Service** → verify federation.

3. Test Free/Busy sharing between on-prem and cloud users.

✅ **Validation**

- Schedule test meetings → confirm visibility of availability.

✅ **Best Practices**

- Maintain proper calendar permissions.
- Communicate cross-premises scheduling capabilities to users.

✅ **Use Case**
Cloud and on-prem employees can view availability → schedules meetings efficiently.

---

148. Configure Exchange Online Hybrid Mailbox Auditing

✅ **Purpose**
Enable auditing for **hybrid mailboxes** for compliance.

✅ **Configuration Steps**

1. Navigate → **Exchange Admin Center** → **Recipients** → **Mailboxes** → **Enable Audit Logging**.
2. Apply auditing settings for send, receive, delete, and mailbox access.
3. Review logs regularly.

✅ **Validation**

- Perform test actions → verify audit logs capture activity.

✅ **Best Practices**

- Enable auditing by default for high-risk users.
- Retain audit logs per compliance requirements.

✅ **Use Case**
Monitor hybrid mailboxes for sensitive actions → ensures regulatory compliance.

---

149. Configure Exchange Online Hybrid Mailbox Auto-Mapping

✅ **Purpose**
Automatically map **shared or delegated mailboxes** for hybrid users in Outlook.

✅ **Configuration Steps**

1. Assign **Full Access permissions** via PowerShell → AutoMapping enabled.
2. Test in Outlook → mailbox automatically appears.

✅ **Validation**

- Confirm hybrid mailbox auto-mapped in Outlook.
- Test send/receive functionality.

✅ **Best Practices**

- Limit auto-mapping to frequently accessed mailboxes.
- Document mailbox assignments.

✅ **Use Case**
Hybrid support mailbox auto-mapped for team members → simplifies mailbox access.

---

150. Configure Microsoft 365 Hybrid Mailbox Migration Reporting

✅ **Purpose**
Track **status and progress** of mailbox migrations in a hybrid environment.

✅ **Configuration Steps**

1. Use **Exchange Admin Center → Recipients → Migration → Migration Batches**.
2. Monitor progress → check success, errors, and pending mailboxes.
3. Export reports for stakeholders.

PowerShell Example

```
Connect-ExchangeOnline

Get-MigrationBatch | Get-MigrationUserStatistics
```

✅ **Validation**

- Confirm all mailboxes migrated → errors addressed.

✅ **Best Practices**

- Schedule regular reports → keep IT and management informed.
- Document issues and resolutions.

✅ **Use Case**
IT team migrates 200 users → reports track batch completion → ensures smooth migration