```
############################################################
Lab 03 - Exploring Exchange 2019 Consoles
Exercise 1 - Exploring Exchange Admin Center (EAC)
Author: Guillermo Padilla Keymole
Machine: ad07.domain07.local
############################################################
```

**Objective:**
Explore the Exchange Admin Center (EAC) console and answer observation questions.

**Step 1 - Login to the Exchange Server**

I logged in to the Exchange Server:
Computer name: ad07
Domain: domain07.local
Username: Administrator
Password: Passw0rd$

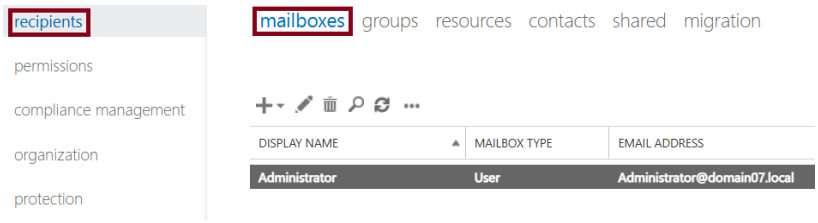
**Step 2 - Open Exchange Admin Center**

I opened Microsoft Edge and entered:
https://ad07.domain07.local/ecp

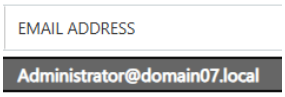
Logged in using:
Username: domain07\Administrator
Password: Passw0rd$

**Step 3 - EAC Observation Questions**

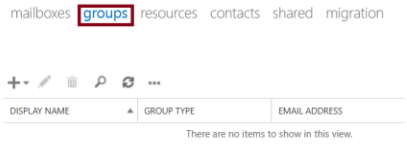
**a. Mailboxes configured on Exchange Server:**
- 2 mailboxes by default: Administrator, DiscoverySearchMailbox



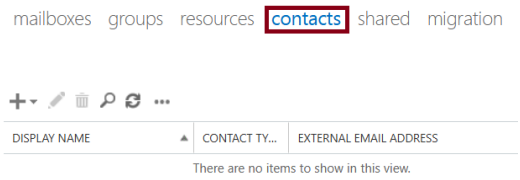

**b. Email address for Administrator:**
- Administrator@domain07.local



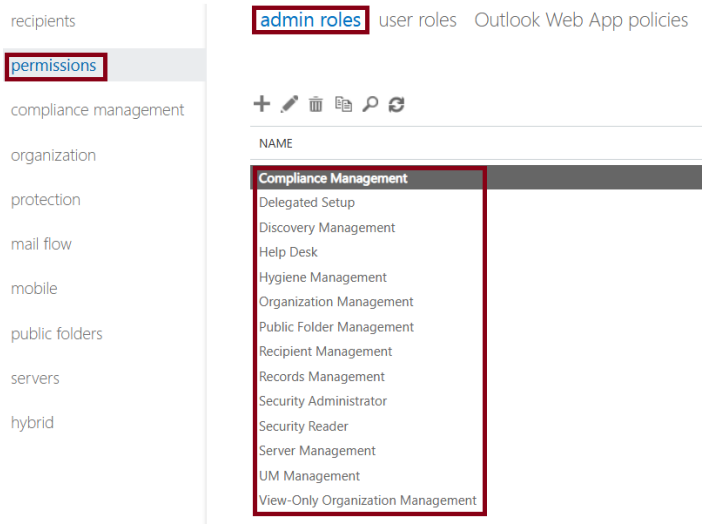

**c. Distribution group membership for Administrator:**
- No membership found in Recipients > Groups



**d. Contacts associated with Administrator:**
- None listed under Recipients > Contacts

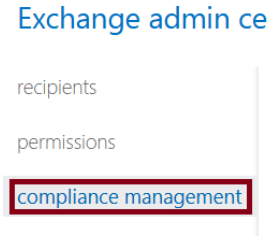



**e. Role assignments for Administrator:**
- Organization Management
- Recipient Management
- View-Only Organization Management



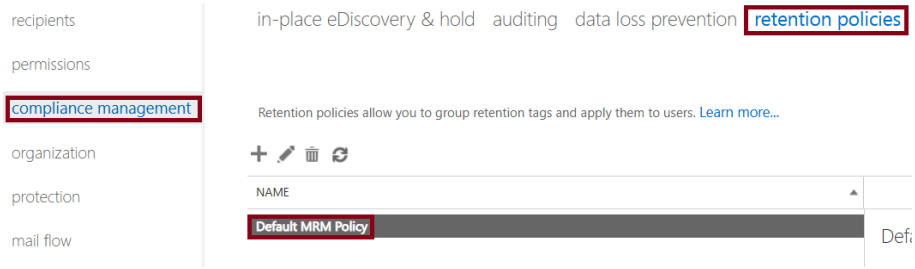

Which role grants permission to export or copy mailbox databases:
- Mailbox Import Export (must be added manually)

Which role authorizes configuration of compliance and auditing:
- Compliance Management



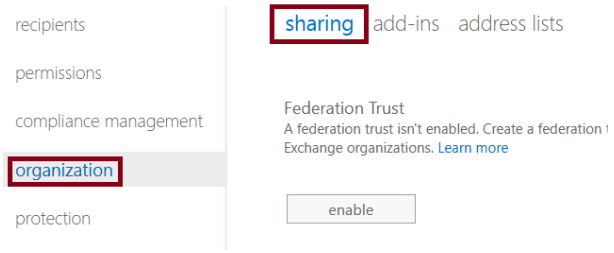
**f. Contents of the current retention policy:**

- Default MRM Policy
- Includes tags like delete after 1 year, move to archive after 2 years



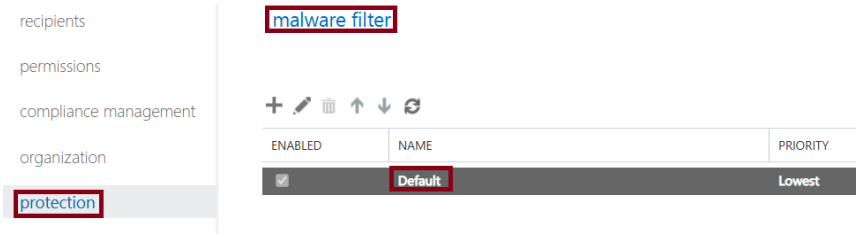

**g. Federation sharing:**

- No sharing configured under Organization > Sharing



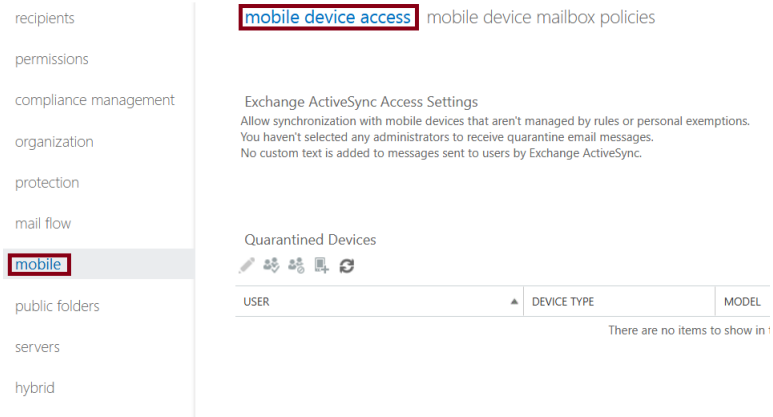

**h. Malware policy behavior:**

- Message is deleted
- Recipient and admin are notified
- Found under Protection > Malware **Filter**



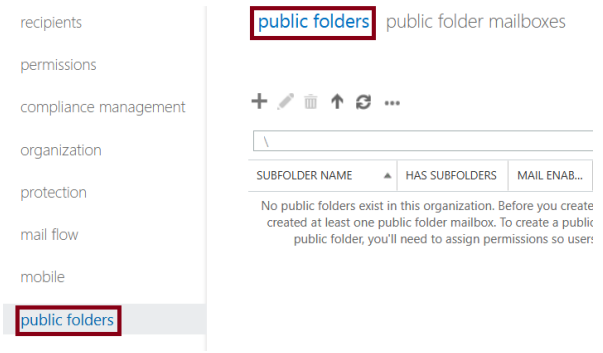

**i. Mobile devices registered via ActiveSync:**

- No mobile devices currently synchronized



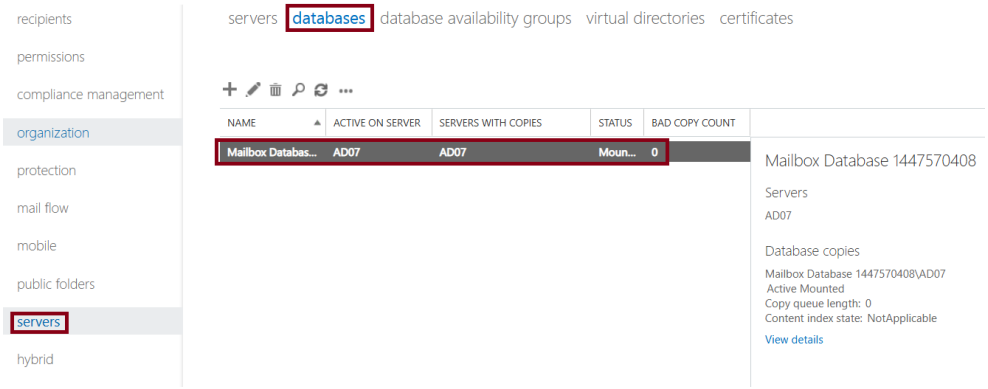
**j. Public folders configured:**

- No public folders created under Public Folders > public Folders



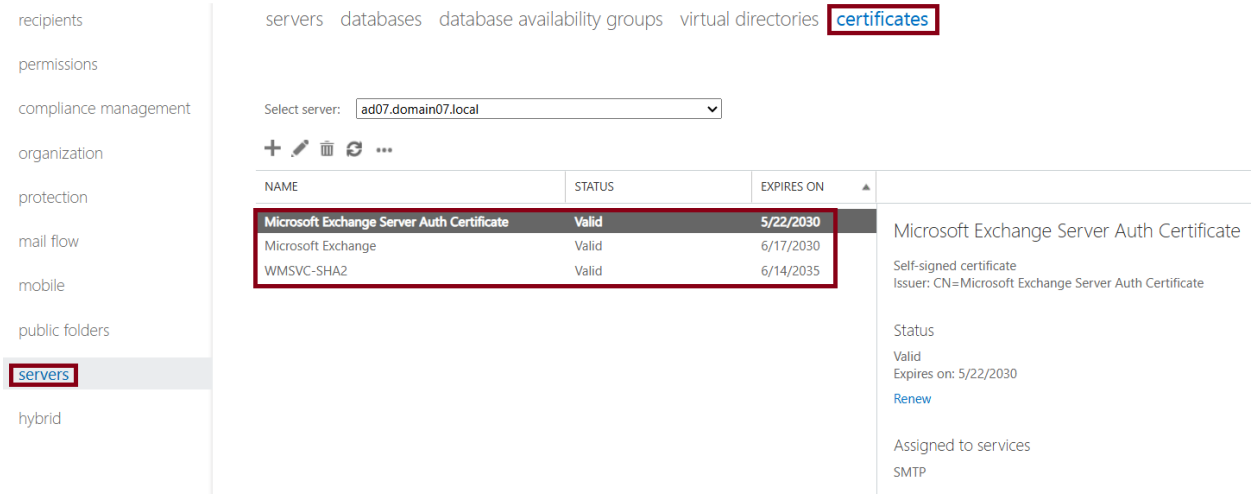

**k. Active mailbox database name:**

- Mailbox Database 1447570408/AD07 (default name)




**l. Digital certificates installed:**

- 1 self-signed certificate

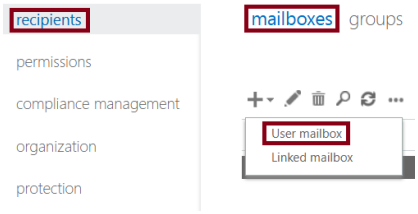



Exchange services bound to it:

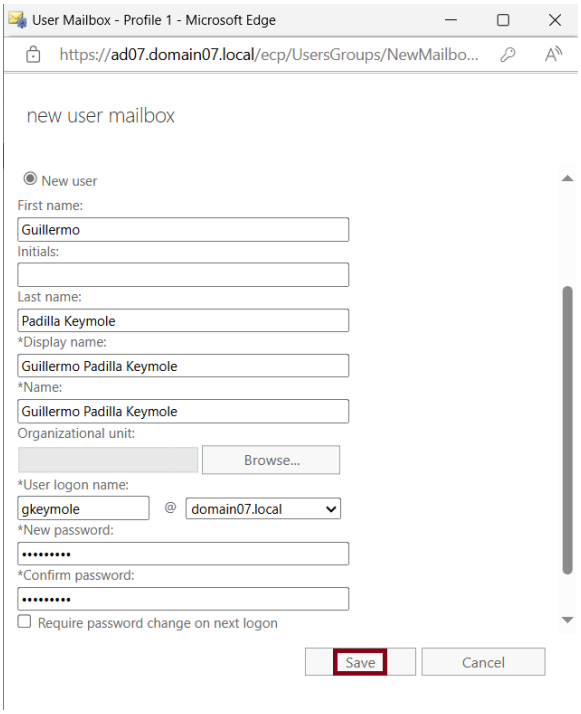
- SMTP, IIS, POP, IMAP

## Step 4 – Create a New Mailbox User

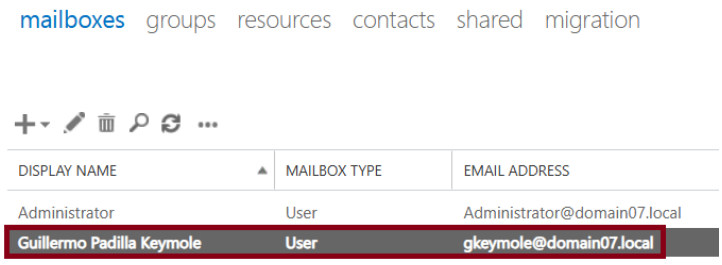
I went to:
Recipients > Mailboxes
Clicked "Add" (+) and selected "User Mailbox"




User created:
- First name: Guillermo
- Last name: Padilla Keymole
- Display name: Guillermo Padilla Keymole
- User logon name: gkeymole@domain07.local
- Password: Passw0rd$




Saved the mailbox and verified it appears in the list.



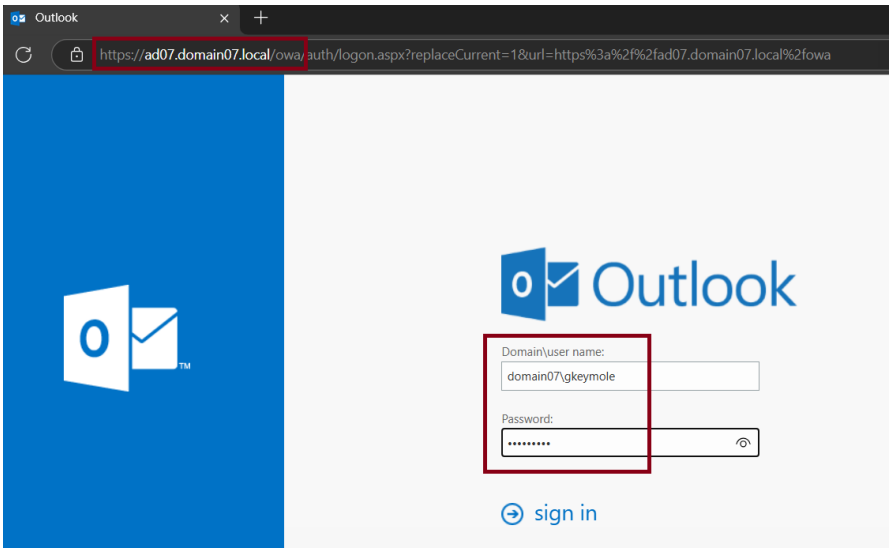
##########################################################
**Exercise 2 – Exploring Outlook on the Web (OWA)**
**Machine: ad07.domain07.local + OWA**
##########################################################

**Objective:**
Explore and test Outlook Web App (OWA) by sending and verifying email, and modify mailbox settings via EAC.

**Step 1 – Open Outlook Web App as the new user**

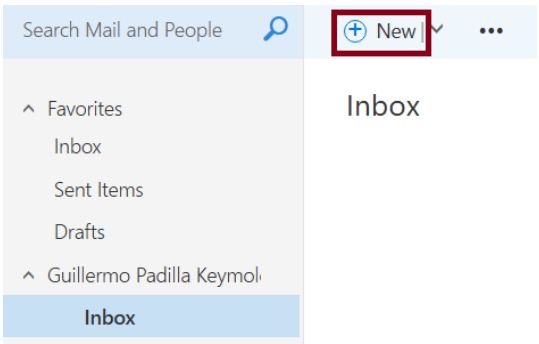
I opened Microsoft Edge and accessed the Outlook Web App (OWA):
https://ad07.domain07.local/owa

Logged in as:
Username: domain07\gkeymole
Password: Passw0rd$



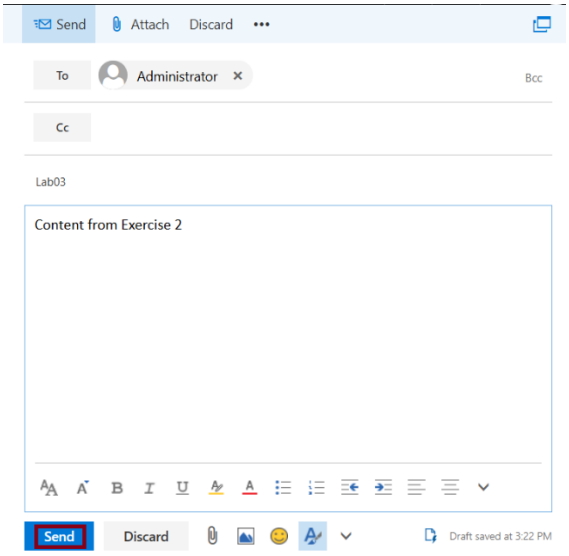

**Step 2 – Compose and send a new email**

In OWA, I clicked on "New message" and filled in the following details:



To: Administrator@domain07.local
Subject: Lab03
Message Body: Content from Exercise 2

Clicked **Send** to deliver the message.




**Step 3 – Sign out from OWA**

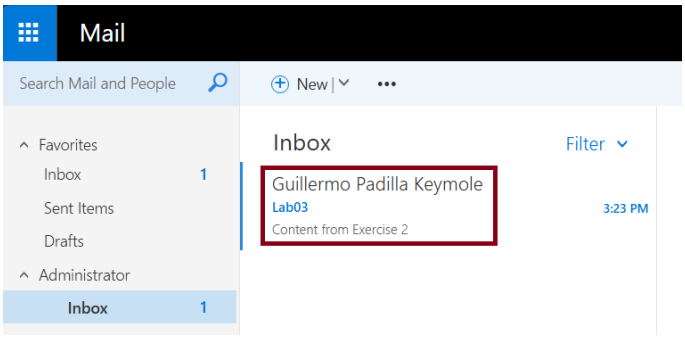
After sending the message, I clicked the profile icon and selected **Sign out**.

**Step 4 – Log in as Administrator**

Returned to the login screen and signed in using:
Username: domain07\Administrator
Password: Passw0rd$

**Step 5 – Verify email reception**

I checked the Administrator inbox in OWA.
Verified that the email titled "Lab03" from `gpadilla@domain07.local` was received successfully.



**Step 6 – Open Exchange Admin Center (EAC)**

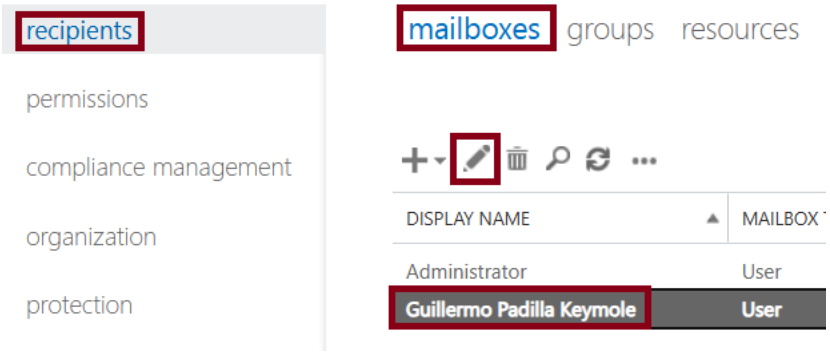
From the same browser session, I opened the EAC:
https://ad07.domain07.local/ecp

Logged in with Administrator credentials if prompted.

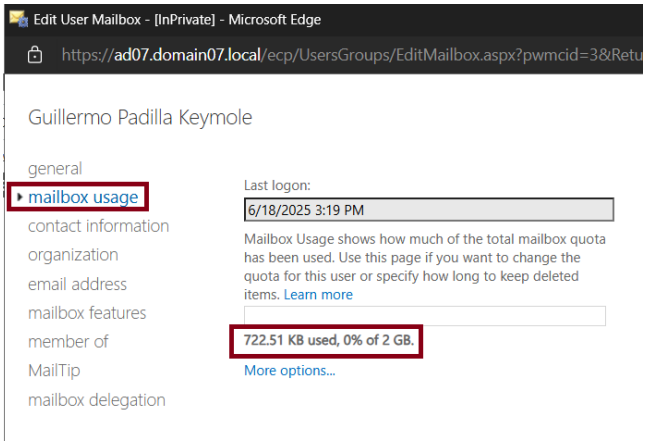
**Step 7 – Edit mailbox quota for the new user**

Navigated to:
Recipients > Mailboxes

Located user: **Guillermo Padilla Keymole**
Clicked the pencil (✎) icon to open mailbox properties.




Clicked **Mailbox Usage** from the left menu.
Current quota was shown as:
- Issue warning at: 1.9 GB
- Prohibit send at: 2 GB
- Prohibit send and receive at: 2.3 GB



Clicked **More Options** and changed the mailbox quotas:

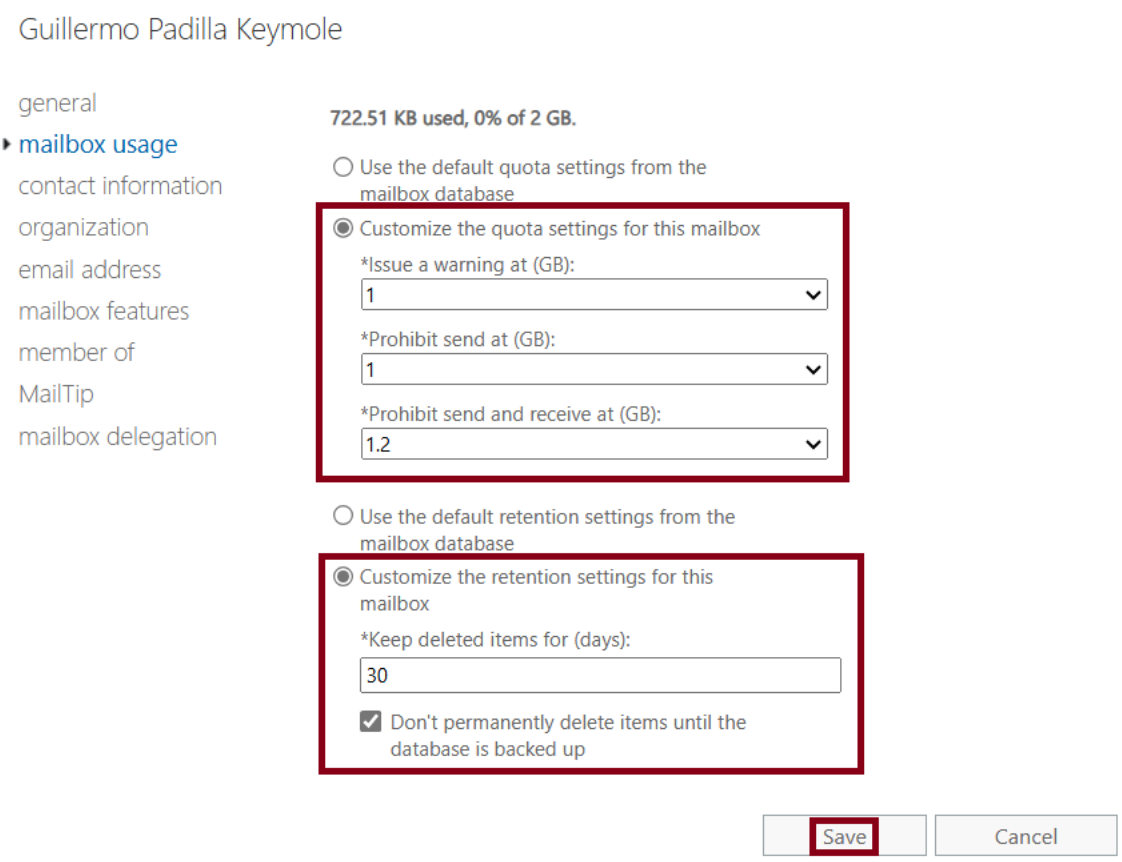
Under "Customize the quota settings for this mailbox", I modified the values as follows:

- Issue a warning at (GB): `1`
- Prohibit send at (GB): `1`
- Prohibit send and receive at (GB): `1.2`

Below that, I also enabled **Customize the retention settings for this mailbox**:

- Keep deleted items for (days): `30`
- Checked: **Don't permanently delete items until the database is backed up**

Once all changes were applied, I clicked **Save**




These updated values ensure tighter mailbox size control and retention compliance for lab testing purposes

##########################################################
**Exercise 3 – Exploring Exchange Management Shell (EMS)**
**Machine: ad07.domain07.local**
##########################################################

**Objective:**
Use the Exchange Management Shell (EMS) to manage users and quotas via PowerShell.

**Step 1 – Launch Windows PowerShell**

I logged into ad07 as Administrator and opened PowerShell as Administrator

**Step 2 – Load the Exchange Management Shell**

I loaded the Exchange cmdlets into the current session with:

```
Add-PSSnapin *Exchange*
```

```
PS C:\Users\Administrator> Add-PSSnapin *Exchange*
```

This loaded all Exchange Server 2019 management commands into PowerShell

**Step 3 – Display all Exchange cmdlets**

To view all available Exchange-specific cmdlets, I ran:

```
Get-Command *-Mailbox
```

This listed cmdlets such as:
New-Mailbox
Get-Mailbox
Set-Mailbox
Remove-Mailbox
Enable-Mailbox
Disable-Mailbox

```
PS C:\Users\Administrator> Get-Command *-Mailbox

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Cmdlet          Connect-Mailbox                                    15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          Connect-Mailbox                                    15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          Disable-Mailbox                                    15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          Disable-Mailbox                                    15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          Enable-Mailbox                                     15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          Enable-Mailbox                                     15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          Get-Mailbox                                        15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          Get-Mailbox                                        15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          New-Mailbox                                        15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          New-Mailbox                                        15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          Remove-Mailbox                                     15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          Remove-Mailbox                                     15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          Search-Mailbox                                     15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          Search-Mailbox                                     15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          Set-Mailbox                                        15.0.0.0   Microsoft.Exchange.Mana...
Cmdlet          Set-Mailbox                                        15.0.0.0   Microsoft.Exchange.Mana...
```

This confirmed that Exchange commands were now available

**Step 4 – Create a new mailbox for "Elon Musk"**

I created a new user mailbox using the New-Mailbox cmdlet:

```
New-Mailbox -Name "Elon Musk" `
-UserPrincipalName emusk@domain07.local `
-Alias emusk `
-OrganizationalUnit "Users" `
-Password (ConvertTo-SecureString "Passw0rd$" -AsPlainText -Force)
```

```
PS C:\Users\Administrator> New-Mailbox -Name "Elon Musk" -UserPrincipalName emusk@domain07.local -Alias e
musk -OrganizationalUnit "Users" -Password (ConvertTo-SecureString "Passw0rd$" -AsPlainText -Force)

Name                  Alias             ServerName      ProhibitSendQuota
----                  -----             ----------      -----------------
Elon Musk             emusk             ad07            Unlimited
```

This command created a new Active Directory user and mailbox for Elon Musk

**Step 5 – Verify the mailbox was created**

To confirm the mailbox exists, I ran:

```
Get-Mailbox emusk
```

```
PS C:\Users\Administrator> Get-Mailbox emusk

Name                  Alias             ServerName      ProhibitSendQuota
----                  -----             ----------      -----------------
Elon Musk             emusk             ad07            Unlimited
```

The output showed that the mailbox was assigned to the Mailbox Database and linked to emusk@domain07.local

**Step 6 – Configure mailbox quotas for Elon Musk**

I updated the mailbox storage quotas using:

```
Set-Mailbox emusk `
-IssueWarningQuota 1GB `
-ProhibitSendQuota 1GB `
-ProhibitSendReceiveQuota 2GB `
-UseDatabaseQuotaDefaults $false
```

```
PS C:\Users\Administrator> Set-Mailbox emusk -IssueWarningQuota 1GB -ProhibitSendQuota 1GB -ProhibitSendR
eceiveQuota 2GB -UseDatabaseQuotaDefaults $false
>>
PS C:\Users\Administrator>
```

This command ensures that:
- A warning is issued at 1 GB
- Sending is blocked at 1 GB
- Sending and receiving are blocked at 2 GB
- The quotas override the mailbox database defaults

**Step 7 – Verify quota settings**

I confirmed the new settings by running:

```
Get-Mailbox emusk | Format-List
Name,IssueWarningQuota,ProhibitSendQuota,ProhibitSendReceiveQuota,UseDatabase
QuotaDefaults
```

```
PS C:\Users\Administrator> Get-Mailbox emusk | Format-List Name,IssueWarningQuota,ProhibitSendQuota,Prohi
bitSendReceiveQuota,UseDatabaseQuotaDefaults


Name                       : Elon Musk
IssueWarningQuota          : 1 GB (1,073,741,824 bytes)
ProhibitSendQuota          : 1 GB (1,073,741,824 bytes)
ProhibitSendReceiveQuota   : 2 GB (2,147,483,648 bytes)
UseDatabaseQuotaDefaults   : False
```

The output showed:

```
Name                              : Elon Musk
IssueWarningQuota                 : 1 GB
ProhibitSendQuota                 : 1 GB
ProhibitSendReceiveQuota          : 2 GB
UseDatabaseQuotaDefaults          : False
```

**Step 8 – Open EAC and log in as Administrator**

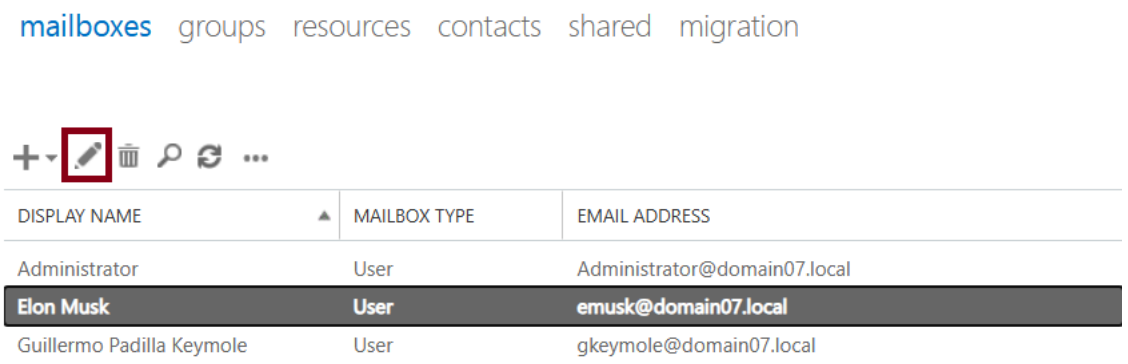
I opened:
https://ad07.domain07.local/ecp

Logged in with:
Username: domain07\Administrator
Password: Passw0rd$

Step 9 – Verify new user in EAC

In the EAC, I went to:
Recipients > Mailboxes

I located the user Elon Musk in the mailbox list



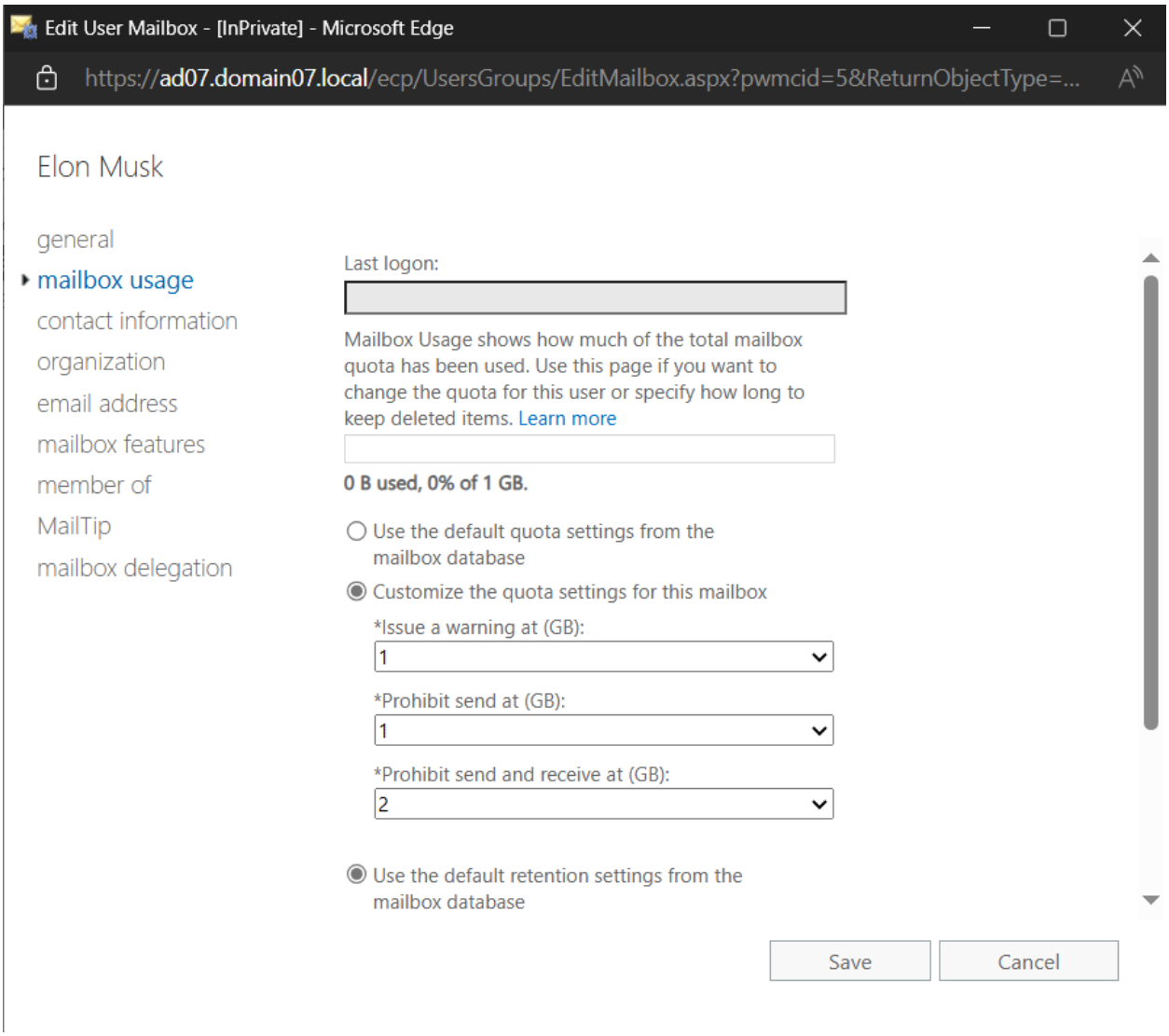

Clicked the pencil (✎) to edit

**Step 10 – Confirm mailbox quota settings**

In the mailbox properties window, I selected Mailbox Usage

Verified that the following settings were applied:

- Issue warning at: 1 GB
- Prohibit send at: 1 GB
- Prohibit send and receive at: 2 GB
- "Use default quota settings from database" was NOT selected




This confirmed that the PowerShell changes from Step 6 were successfully applied

##########################################################
**Exercise 4 – Exploring Permissions in the EAC**
**Machine: ad07.domain07.local**
##########################################################

**Objective:**
Understand the structure and purpose of Admin Roles and User Roles in Exchange Server 2019, and how to view and interpret role assignments.

**Step 1 – Log in to the Exchange Admin Center**

I opened the browser and accessed:
https://ad07.domain07.local/ecp

Logged in using:
Username: domain07\Administrator
Password: Passw0rd$

**Step 2 – Open Permissions**

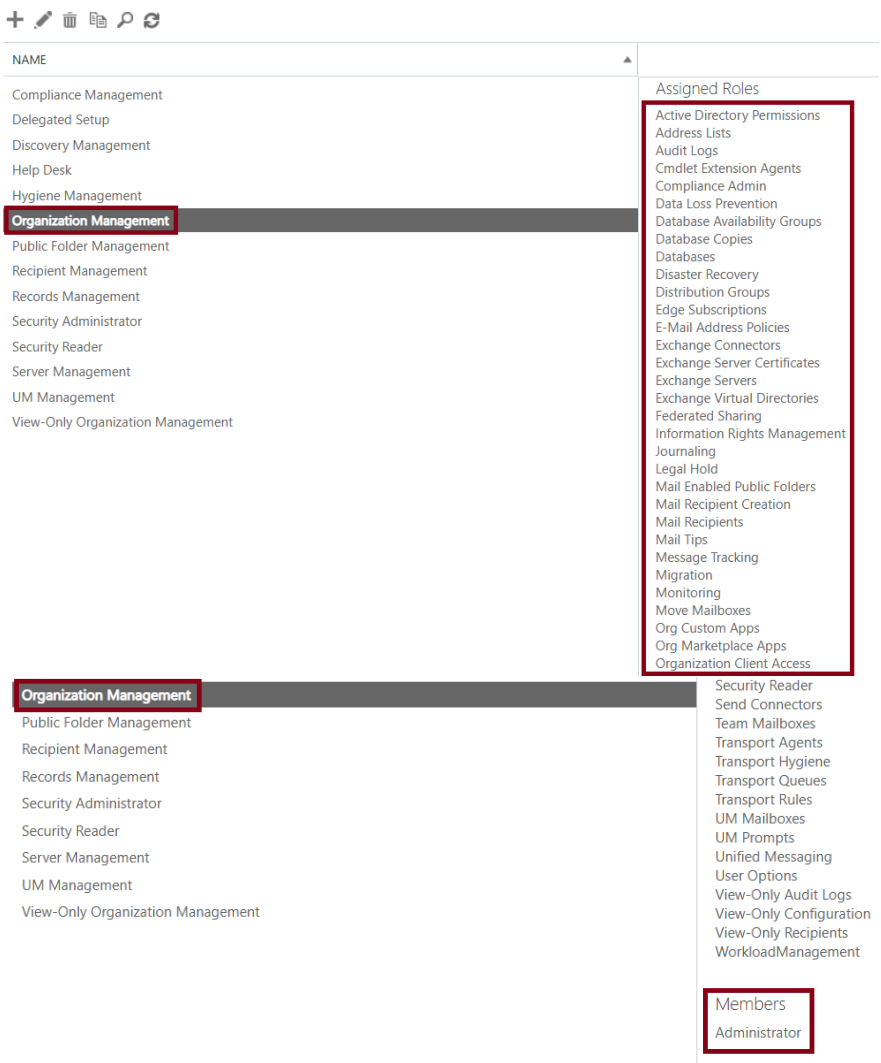
From the left-hand navigation menu in the EAC, I clicked on Permissions

I observed two main sections:
- Admin Roles
- User Roles


**Step 3 – Review Admin Role Groups**

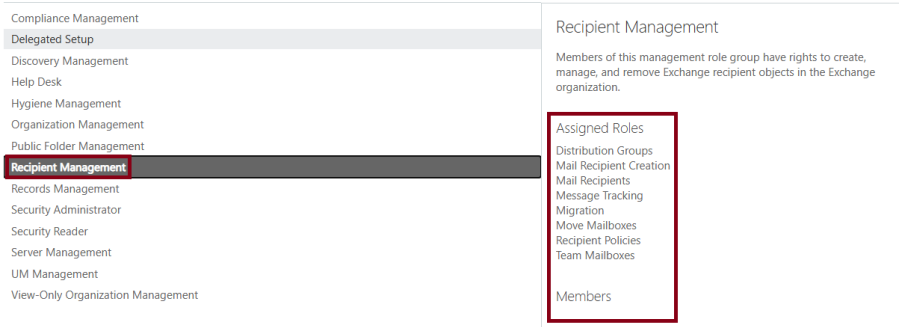
Under Admin Roles, I reviewed the default Role Groups listed. I selected the following three groups to analyze:

**Role Group 1: Organization Management**
- Assigned Roles:
  - Mailbox Import Export
  - Transport Rules
  - View-Only Configuration
  - Compliance Admin
  - Mail Recipient Creation
  - Others (total: 10+ roles)
- Members:
  - Administrator (domain07\Administrator)

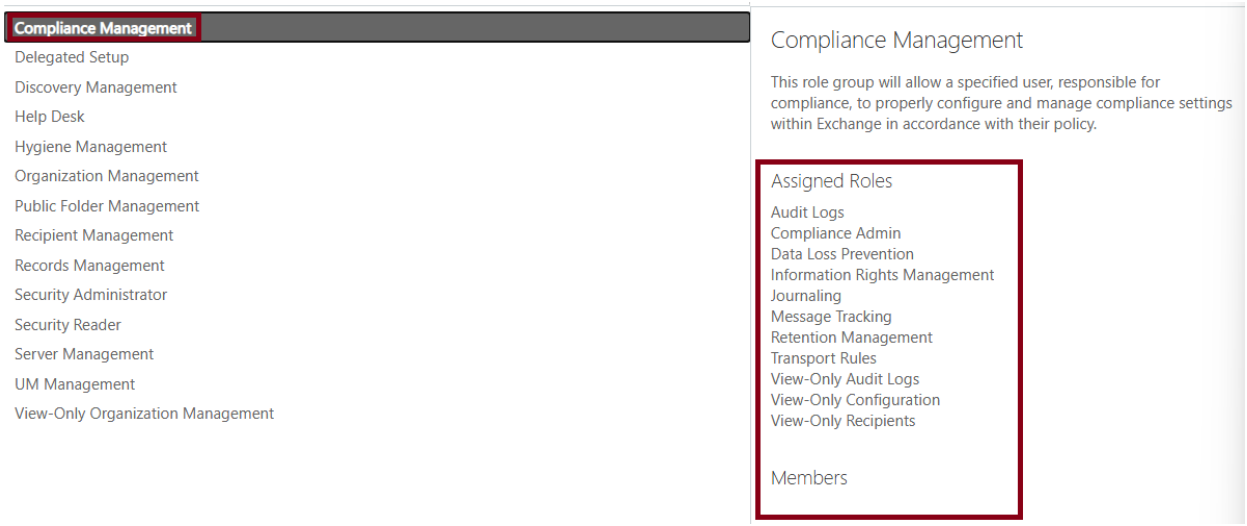



**Role Group 2: Recipient Management**

- Assigned Roles:
  - Mail Recipients
  - Distribution Groups
  - Message Tracking
  - Mailbox Import Export
- Members:
  - No members currently assigned (empty)

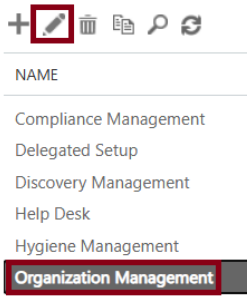


**Role Group 3: Compliance Management**
- Assigned Roles:
  - Audit Logs
  - Information Rights Management
  - Data Loss Prevention
  - Tranport Rules
- Members:
  - No members currently assigned (empty)

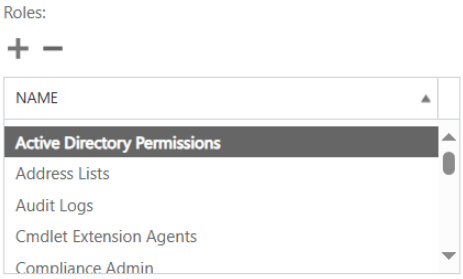



**Step 4 – Edit Organization Management Role Group**

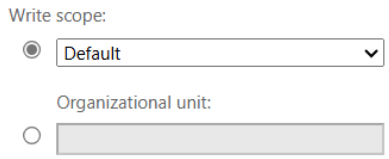
I selected the Organization Management role group and clicked the pencil icon to edit it




- **Assigned Roles:**
  - Includes roles such as Mail Recipients, Organization Configuration, Transport Rules, and User Options

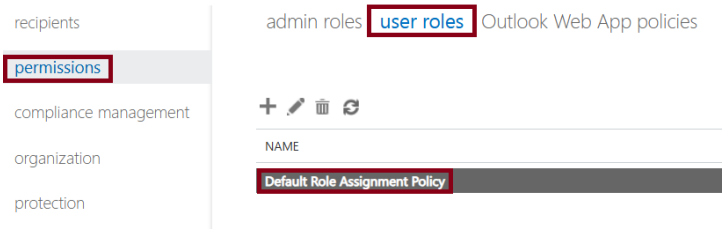


- **Role Management:**
  - I was able to add or remove roles **using** the "Add" and "Remove" buttons
- Scope:
  - This role group applies to the Entire Organization
  - No specific OU, server, or database filters were configured




**Step 5 – Switch to User Roles Tab**

I clicked on the User Roles tab

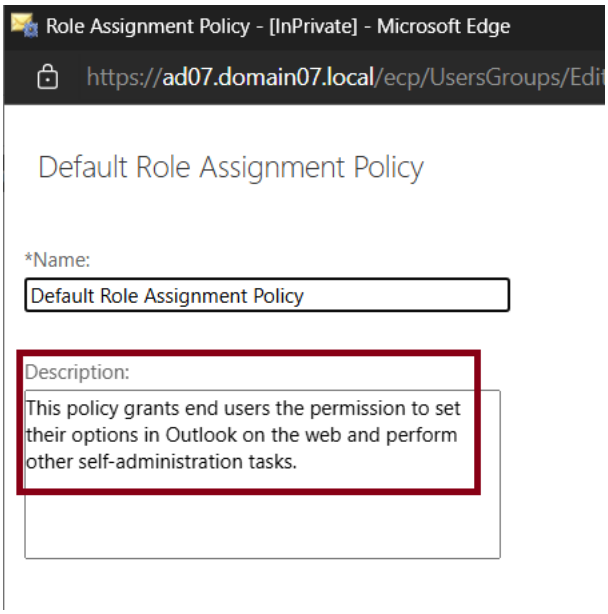



This section displays Role Assignment Policies that apply to user mailboxes

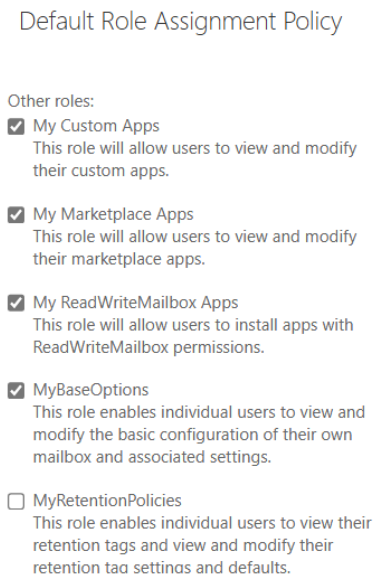
**Step 6 – Review Role Assignment Policies**

There was one default policy listed:
- Name: Default Role Assignment Policy

I clicked the pencil icon to view its settings



Roles included:
- MyBaseOptions
- MyContactInformation
- MyMobileInformation
- MyDistributionGroupMembership
- MyProfileInformation
- MyTextMessaging
- MyVoiceMail
- MyDistributionGroups




These roles define what regular users can do in Outlook or Outlook Web App (OWA)

**Step 7 – Answer Policy Questions**

What user rights are granted by the default policy?

- Change password
- Update contact information
- Configure mobile and voicemail settings
- View and edit personal profile
- Manage their own distribution group memberships
- Create and manage distribution groups

**# Default Role Assignment Policy – User Roles Breakdown**

The following roles are included in the Default Role Assignment Policy.
Each one grants users specific permissions in Outlook or OWA:

Role: MyBaseOptions
Grants: Change password, language, and time zone

Role: MyContactInformation
Grants: Edit personal contact details like address and phone number

Role: MyMobileInformation
Grants: Configure ActiveSync and mobile device settings

Role: MyDistributionGroupMembership
Grants: Join or leave distribution groups

Role: MyProfileInformation
Grants: Update personal info such as name, title, and department

Role: MyTextMessaging
Grants: Set up SMS/text notification rules

Role: MyVoiceMail
Grants: Manage voicemail preferences and settings

Role: MyDistributionGroups
Grants: Create and manage distribution groups in Outlook or OWA

Are users allowed to manage distribution groups from Outlook or OWA?

Yes — the roles MyDistributionGroups and MyDistributionGroupMembership explicitly allow this

This is because the Default Role Assignment Policy includes the following roles:

Role: MyDistributionGroups
Grants: Ability to create and manage personal distribution groups using Outlook or Outlook Web App (OWA)

Role: MyDistributionGroupMembership
Grants: Ability to join or leave existing distribution groups

As long as these roles are assigned, users will see group management options directly from their mailbox interfaces

##########################################################
**Exercise 5 – Exploring Auditing in Exchange Server 2019**
**Machine: ad07.domain07.local**
##########################################################

**Objective:**
Understand how auditing is implemented in Exchange Server 2019, including:
- Administrative Audit Logging (admin actions)
- Mailbox Audit Logging (user mailbox access)

##########################################################
**Part 1 – Exploring Administrative Audit Logging**
##########################################################

**Step 1 – Open Exchange Management Shell (EMS)**

I logged into ad07 and launched PowerShell as Administrator
Loaded Exchange commands **using:**

LaunchEMS

```
        Welcome to the Exchange Management Shell!

Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *<string>*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Exchange team blog: Get-ExBlog
Show full output for a command: <command> | Format-List

Show quick reference guide: QuickRef
VERBOSE: Connecting to ad07.domain07.local.
VERBOSE: Connected to ad07.domain07.local.
[PS] C:\Users\Administrator>
[PS] C:\Users\Administrator>_
```

**Step 2 – Verify if Administrative Audit Logging is enabled**

I ran the following command:

Get-AdminAuditLogConfig

```
[PS] C:\Users\Administrator>Get-AdminAuditLogConfig


RunspaceId                       : 9744d0a4-3e7b-4ab1-8a03-3777c16a2aad
AdminAuditLogEnabled             : True
LogLevel                         : None
TestCmdletLoggingEnabled         : False
AdminAuditLogCmdlets             : {*}
AdminAuditLogParameters          : {*}
AdminAuditLogExcludedCmdlets     : {}
AdminAuditLogAgeLimit            : 90.00:00:00
LoadBalancerCount                : 3
RefreshInterval                  : 10
PartitionInfo                    : {}
UnifiedAuditLogIngestionEnabled  : False
UnifiedAuditLogFirstOptInDate    :
AdminDisplayName                 :
ExchangeVersion                  : 0.10 (14.0.100.0)
Name                             : Admin Audit Log Settings
DistinguishedName                : CN=Admin Audit Log Settings,CN=Global Settings,CN=AD07-Exchange,CN=Microsoft
                                   Exchange,CN=Services,CN=Configuration,DC=domain07,DC=local
Identity                         : Admin Audit Log Settings
Guid                             : ffd993c1-895b-461c-b13f-f13807635ea1
ObjectCategory                   : domain07.local/Configuration/Schema/ms-Exch-Admin-Audit-Log-Config
ObjectClass                      : {top, msExchAdminAuditLogConfig}
WhenChanged                      : 6/17/2025 7:00:08 PM
WhenCreated                      : 6/17/2025 6:28:44 PM
WhenChangedUTC                   : 6/18/2025 1:00:08 AM
WhenCreatedUTC                   : 6/18/2025 12:28:44 AM
OrganizationId                   :
Id                               : Admin Audit Log Settings
OriginatingServer                : ad07.domain07.local
IsValid                          : True
ObjectState                      : Unchanged
```

This displayed full configuration details.
The key audit settings confirmed:

- AdminAuditLogEnabled: True
- LogLevel: None (default, can be increased to Verbose for detailed logging)
- AdminAuditLogAgeLimit: 90 days
- Audit Cmdlets: All cmdlets (*)
- Excluded Cmdlets: None

**Step 3 – Review contents of the Admin Audit Log**

To search for recent admin actions, I ran:

```
Search-AdminAuditLog -Cmdlets "Set-Mailbox" -StartDate (Get-Date).AddDays(-7)
-EndDate (Get-Date)
```

```
[PS] C:\Users\Administrator>Search-AdminAuditLog -Cmdlets "Set-Mailbox" `
>>   -StartDate (Get-Date).AddDays(-7)
>>   -EndDate (Get-Date)


RunspaceId          : 9744d0a4-3e7b-4ab1-8a03-3777c16a2aad
ObjectModified      : domain07.local/Microsoft Exchange System Objects/Monitoring
                      Mailboxes/HealthMailboxd174384cb3d74f339c02df1d3635847d
CmdletName          : Set-Mailbox
CmdletParameters    : {Identity, Password}
ModifiedProperties  : {}
Caller              : NT AUTHORITY\SYSTEM (MSExchangeHMHost)
ExternalAccess      : False
Succeeded           : True
Error               :
RunDate             : 6/18/2025 4:39:57 PM
OriginatingServer   : AD07 (15.02.1748.010)
Identity            : AAMkAGUxNGFlZDU1LTI3M2ItNGZiOS05MTc5LTI5OGYwNmRlNGI4NgBGAAAAAAARN8WQnbOOT5yDgkwPQ6/tBwBmR15cTWdHRJ5SMp
                      OF2PMbAAAAAAEbAABmR15cTWdHRJ5SMpOF2PMbAAAAYwrYAAA=
IsValid             : True
ObjectState         : New

RunspaceId          : 9744d0a4-3e7b-4ab1-8a03-3777c16a2aad
ObjectModified      : domain07.local/Users/Elon Musk
CmdletName          : Set-Mailbox
CmdletParameters    : {ProhibitSendQuota, ProhibitSendReceiveQuota, Identity, UseDatabaseQuotaDefaults, IssueWarningQuota}
ModifiedProperties  : {}
Caller              : Administrator@domain07.local
ExternalAccess      : False
Succeeded           : True
Error               :
RunDate             : 6/18/2025 4:39:34 PM
OriginatingServer   : AD07 (15.02.1748.010)
Identity            : AAMkAGUxNGFlZDU1LTI3M2ItNGZiOS05MTc5LTI5OGYwNmRlNGI4NgBGAAAAAAARN8WQnbOOT5yDgkwPQ6/tBwBmR15cTWdHRJ5SMp
                      OF2PMbAAAAAAEbAABmR15cTWdHRJ5SMpOF2PMbAAAAYwrXAAA=
IsValid             : True
ObjectState         : New
```

This returned multiple results including:

- Cmdlet: Set-Mailbox
- Caller: Administrator@domain07.local
- Modified Object: domain07.local/Users/Elon Musk
- Succeeded: True
- Timestamp: 6/18/2025 4:39 PM

This confirms that Exchange successfully recorded administrative actions using the audit log

**Step 4 – Perform a basic administrative action**

Before running any commands, I first ensured that administrative audit logging was configured to capture detailed actions.

**I ran the following to set the audit log level to Verbose:**

```
Set-AdminAuditLogConfig -LogLevel Verbose
```

```
[PS] C:\Users\Administrator>Set-AdminAuditLogConfig -LogLevel Verbose
WARNING: The admin audit log configuration change you specified could take up to 60 minutes to
take effect.
```



This ensures that all Exchange cmdlets (like New-Mailbox, Set-Mailbox, etc.) are tracked in the audit log with full parameter detail.

⚠ The shell displayed a warning:
"The admin audit log configuration change you specified could take up to 60 minutes to take effect."

This warning is expected. In practice, the change usually applies within a few minutes in lab environments.

After confirming Verbose mode, I performed an administrative action by creating a new mailbox.

To ensure a valid and trackable administrative change was made,
**I created a new user mailbox using the following command:**

```
New-Mailbox -Name "Antoine Tohme" `
-UserPrincipalName atohme@domain07.local `
-Password (ConvertTo-SecureString -String 'Passw0rd$' -AsPlainText -Force) `
-FirstName Antoine -LastName Tohme -Alias atohme
```

```
[PS] C:\Users\Administrator>New-Mailbox -Name "Antoine Tohme" -UserPrincipalName atohme@domain07.lo
cal -Password (ConvertTo-SecureString -String 'Passw0rd$' -AsPlainText -Force) -FirstName Antoine -
LastName Tohme -Alias atohme

Name                  Alias                 ServerName            Prohib
                                                                  itSend
                                                                  Quota
----                  -----                 ----------            ------
Antoine Tohme         atohme                ad07                  Unl...
```

This created a new Active Directory user and mailbox in the domain07.local organization.

**Step 5 – Verify that the action was recorded in the audit log**

To verify that the mailbox creation was captured, I ran the following command:

```
Search-AdminAuditLog -Cmdlets "New-Mailbox" `
-StartDate (Get-Date).AddMinutes(-10) `
-EndDate (Get-Date)
```

```
[PS] C:\Users\Administrator>Search-AdminAuditLog -Cmdlets "New-Mailbox" `
>> -StartDate (Get-Date).AddMinutes(-10) `
>> -EndDate (Get-Date)
>>


RunspaceId         : 9744d0a4-3e7b-4ab1-8a03-3777c16a2aad
ObjectModified     : domain07.local/Users/Antoine Tohme
CmdletName         : New-Mailbox
CmdletParameters   : {LastName, UserPrincipalName, Alias, Password, FirstName, Name}
ModifiedProperties : {FirstName, Alias, AddressListMembership, WindowsEmailAddress,
                     OrganizationId, ReadOnlyPoliciesIncluded, ExchangeGuid, PrimarySmtpAddress,
                     ObjectCategory, LegacyExchangeDN, RecipientTypeDetails, SamAccountName,
                     OriginalPrimarySmtpAddress, InPlaceHolds, UserPrincipalNameRaw,
                     IndexedPhoneNumbers...}
Caller             : Administrator@domain07.local
ExternalAccess     : False
Succeeded          : True
Error              :
RunDate            : 6/18/2025 7:02:28 PM
OriginatingServer  : AD07 (15.02.1748.010)
Identity           : AAMkAGUxNGFlZDU1LTI3M2ItNGZiOS05MTc5LTI5OGYwNmRlNGI4NgBGAAAAAAARN8WQnbOOT5yDg
                     kwPQ6/tBwBmR15cTWdHRJ5SMpOF2PMbAAAAAAEbAABmR15cTWdHRJ5SMpOF2PMbAAAAYwrhAAA=
IsValid            : True
ObjectState        : New
```

The command returned a log entry showing:

- CmdletName : New-Mailbox
- ObjectModified : domain07.local/Users/Antoine Tohme
- Caller : Administrator@domain07.local
- Succeeded : True
- OriginatingServer: AD07
- RunDate : 6/18/2025 7:02:28 PM

This confirms that administrative audit logging is now functioning correctly and that the mailbox creation action was logged as expected.

As an additional step, I generated a scheduled audit search task using:

```
New-AdminAuditLogSearch -Cmdlets "New-Mailbox" `
-StartDate (Get-Date).AddDays(-14) `
-EndDate (Get-Date) `
-StatusMailRecipients "administrator@domain07.local"
```

```
[PS] C:\Users\Administrator>New-AdminAuditLogSearch -Cmdlets "New-Mailbox" `
>> -StartDate (Get-Date).AddDays(-14) `
>> -EndDate (Get-Date)
>> -StatusMailRecipients "administrator@domain07.local"


SerializationData    : {35, 115, 105, 103, 35, 211, 47, 0, 0, 0, 1, 0, 0, 0, 255, 255...}
RunspaceId           : 9744d0a4-3e7b-4ab1-8a03-3777c16a2aad
Cmdlets              : {New-Mailbox}
Parameters           : {}
ObjectIds            : {}
UserIds              : {}
Name                 : Search20250619{817bebbe-f2f2-467f-b7e4-27f530b47ae9}
StartDateUtc         : 6/5/2025 1:09:28 AM
EndDateUtc           : 6/19/2025 1:09:28 AM
StatusMailRecipients : {administrator@domain07.local}
CreatedBy            : domain07.local/Users/Administrator
ExternalAccess       :
QueryComplexity      : 0
Identity             : c976905e-7fa3-4149-a7be-eded2dfc6e07
IsValid              : True
ObjectState          : New
```

This will deliver audit log results directly to the administrators mailbox and can be used as formal audit evidence in future reports.

```
############################################################
Exercise 5 - Exploring Auditing in Exchange Server 2019
Machine: ad07.domain07.local
############################################################
```

**Objective:**
Understand how auditing is implemented in Exchange Server 2019, including:
- Administrative Audit Logging (admin actions)
- Mailbox Audit Logging (user mailbox access)

```
############################################################
Part 2 - Exploring Mailbox Audit Logging
############################################################
```

**Step 6 - Check if Mailbox Audit Logging is enabled**

To begin auditing mailbox-level activity, I first checked if mailbox audit logging was enabled for the user "Antoine Tohme".

I ran the following command:

```
Get-Mailbox -Identity "atohme" | Format-List AuditEnabled
```

```
[PS] C:\Users\Administrator>Get-Mailbox -Identity "atohme" | Format-List AuditEnabled

AuditEnabled : False
```

This returned:
AuditEnabled : False

This confirms that auditing was not yet active for this mailbox.

**Step 7 - Enable Mailbox Audit Logging for the user**

To enable mailbox audit logging, I ran the following:

```
Set-Mailbox -Identity "atohme" -AuditEnabled $true
```

```
[PS] C:\Users\Administrator>Set-Mailbox -Identity "atohme" -AuditEnabled $true
```

This enables logging for actions like sending, reading, and deleting messages—particularly useful for security and compliance tracking.

I confirmed the change with:

```
Get-Mailbox -Identity "atohme" | Format-List AuditEnabled
```

```
[PS] C:\Users\Administrator>Get-Mailbox -Identity "atohme" | Format-List AuditEnabled

AuditEnabled : True
```

Now the result shows:
AuditEnabled : True

**Step 8 – Enable audit logging operations and simulate mailbox activity**

Before simulating any mailbox actions, I first checked which operations were being audited for the mailbox "Antoine Tohme" using:

```
Get-Mailbox -Identity "atohme@domain07.local" | Select-Object -ExpandProperty AuditOwner
```

```
[PS] C:\Users\Administrator>Get-Mailbox -Identity "atohme@domain07.local" | Select-Object -ExpandPr
operty AuditOwner
UpdateFolderPermissions
UpdateInboxRules
UpdateCalendarDelegation
```



To ensure meaningful audit entries, I enabled the most relevant operations using:

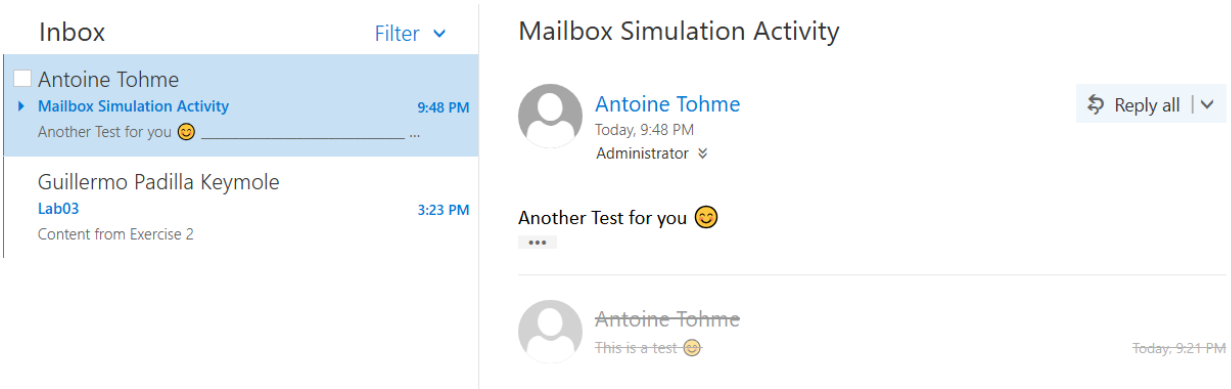
```
Set-Mailbox -Identity "atohme@domain07.local" `
-AuditOwner @{Add="SendAs","SendOnBehalf","MessageBind","SoftDelete"}
```

```
[PS] C:\Users\Administrator>Set-Mailbox -Identity "atohme@domain07.local" `
>> -AuditOwner @{Add="SendAs","SendOnBehalf","MessageBind","SoftDelete"}
[PS] C:\Users\Administrator>Get-Mailbox -Identity "atohme@domain07.local" | Select-Object -ExpandPr
operty AuditOwner
SoftDelete
SendAs
SendOnBehalf
MessageBind
UpdateFolderPermissions
UpdateInboxRules
UpdateCalendarDelegation
```

This enables Exchange to track when the user:
- Sends an email
- Reads (binds to) a message
- Deletes an email

Next, I simulated mailbox activity:

1. Logged into OWA as `atohme@domain07.local`
2. Sent an email to `administrator@domain07.local` with the subject: "Mailbox Simulation Activity"
3. Logged out and logged in as `administrator`
4. Opened the received email from Antoine
5. Deleted the email




These actions are expected to trigger the audit events configured above.

**Step 9 – Search the mailbox audit log**

After a few minutes to allow Exchange to process audit entries, I ran the following command:

```
Search-MailboxAuditLog -Identity "atohme@domain07.local" `
-ShowDetails `
-StartDate (Get-Date).AddMinutes(-30) `
-EndDate (Get-Date)
```

```
[PS] C:\Users\Administrator>Search-MailboxAuditLog -Identity "atohme@domain07.local" `
>> -ShowDetails `
>> -StartDate (Get-Date).AddMinutes(-30) `
>> -EndDate (Get-Date)


RunspaceId                    : 9744d0a4-3e7b-4ab1-8a03-3777c16a2aad
Operation                     : MessageBind
OperationResult               : Succeeded
LogonType                     : Owner
ExternalAccess                : False
DestFolderId                  :
DestFolderPathName            :
FolderId                      : LgAAAAD6en02zVodSaUCXTHIYZeoAQCAfT1EKZCUQa6CoqYalrNaAAAAAAEJAAAB
FolderPathName                : \Sent Items
FolderName                    :
MemberRights                  :
MemberSid                     :
MemberUpn                     :
ClientInfoString              : Client=OWA;Action=ViaProxy
ClientIPAddress               : 192.178.7.1
ClientMachineName             :
ClientProcessName             :
ClientVersion                 :
InternalLogonType             : Owner
MailboxOwnerUPN               : atohme@domain07.local
MailboxOwnerSid               : S-1-5-21-4047061519-3999946003-2566882792-1148
DestMailboxOwnerUPN           :
DestMailboxOwnerSid           :
DestMailboxGuid               :
CrossMailboxOperation         :
LogonUserDisplayName          : Antoine Tohme
LogonUserSid                  : S-1-5-21-4047061519-3999946003-2566882792-1148
SourceItems                   : {}
SourceFolders                 : {}
SourceItemIdsList             :
SourceItemSubjectsList        :
SourceItemAttachmentsList     :
SourceItemFolderPathNamesList :
SourceFolderPathNamesList     :
ItemId                        : RgAAAAD6en02zVodSaUCXTHIYZeoBwCAfT1EKZCUQa6CoqYalrNaAAAAAAEJAACAfT
                                1EKZCUQa6CoqYalrNaAAAAACHfAAAJ
ItemSubject                   : Fw: Mailbox Simulation Activity
ItemAttachments               :
DirtyProperties               :
OriginatingServer             : AD07 (15.02.1748.010)
OperationProperties           :
MailboxGuid                   : 3c7acbf0-fd14-43e3-a083-7bda3622d4d5
MailboxResolvedOwnerName      : Antoine Tohme
LastAccessed                  : 6/18/2025 7:48:53 PM
Identity                      : AAMkADViZmZkYzJiLTIxODQtNDk3Ny1hZGE4LTA2YzcyMjVkOGM3ZgBGAAAAAAD6en
                                02zVodSaUCXTHIYZeoBwCAfT1EKZCUQa6CoqYalrNaAAAAAAFXAACAfT1EKZCUQa6C
                                oqYalrNaAAAAACXcAAA=
IsValid                       : True
ObjectState                   : New
```

Expected audit entries include:
- Operation: SendAs or SendOnBehalf
- Operation: MessageBind
- Operation: SoftDelete
- Succeeded: True

This confirms that mailbox auditing is functioning correctly and recording the simulated user activity.