

```
#####
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

The screenshot shows the Exchange Admin Center interface. On the left, there's a navigation bar with links like 'recipients' (highlighted in red), 'mailboxes' (highlighted in red), 'groups', 'resources', 'contacts', 'shared', and 'migration'. Under 'mailboxes', there are sub-links for 'permissions', 'compliance management', 'organization', and 'protection'. The main area has a toolbar with icons for '+', edit, delete, search, and more. Below the toolbar is a table with columns: DISPLAY NAME, MAILBOX TYPE, and EMAIL ADDRESS. A single row is visible for the 'Administrator' mailbox, which is highlighted in red. The table header includes 'DISPLAY NAME', 'MAILBOX TYPE', and 'EMAIL ADDRESS'.

DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS
Administrator	User	Administrator@domain07.local

b. Email address for Administrator:

- Administrator@domain07.local

The screenshot shows the 'Groups' section of the Exchange Admin Center. At the top, there's a toolbar with icons for '+', edit, delete, search, and more. Below the toolbar is a table with columns: DISPLAY NAME, GROUP TYPE, and EMAIL ADDRESS. A single row is visible for the 'Administrator' group, which is highlighted in red. The table header includes 'DISPLAY NAME', 'GROUP TYPE', and 'EMAIL ADDRESS'. A message at the bottom of the table says 'There are no items to show in this view.'

DISPLAY NAME	GROUP TYPE	EMAIL ADDRESS
Administrator	Group	Administrator@domain07.local

c. Distribution group membership for Administrator:

- No membership found **in** Recipients > Groups

The screenshot shows the 'Groups' section under 'Recipients' in the Exchange Admin Center. At the top, there's a toolbar with icons for '+', edit, delete, search, and more. Below the toolbar is a table with columns: DISPLAY NAME, GROUP TYPE, and EMAIL ADDRESS. A single row is visible for the 'Administrator' group, which is highlighted in red. The table header includes 'DISPLAY NAME', 'GROUP TYPE', and 'EMAIL ADDRESS'. A message at the bottom of the table says 'There are no items to show in this view.'

DISPLAY NAME	GROUP TYPE	EMAIL ADDRESS
Administrator	Group	Administrator@domain07.local

d. Contacts associated with Administrator:

- None listed under Recipients > Contacts

mailboxes groups resources **contacts** shared migration

DISPLAY NAME	CONTACT TY...	EXTERNAL EMAIL ADDRESS
There are no items to show in this view.		

e. Role assignments for Administrator:

- Organization Management
- Recipient Management
- View-Only Organization Management

NAME
Compliance Management
Delegated Setup
Discovery Management
Help Desk
Hygiene Management
Organization Management
Public Folder Management
Recipient Management
Records Management
Security Administrator
Security Reader
Server Management
UM 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

Exchange admin center

recipients

permissions

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

The screenshot shows the 'Retention policies' section in the Microsoft 365 admin center. On the left, there's a sidebar with links: recipients, permissions, compliance management (which is highlighted with a red box), organization, protection, and mail flow. The main area has a heading 'in-place eDiscovery & hold auditing data loss prevention' followed by a 'retention policies' button. Below this, it says 'Retention policies allow you to group retention tags and apply them to users.' with a 'Learn more...' link. There's a table with columns 'NAME' and 'DEFINITION'. A single row is visible: 'Default MRM Policy'. At the bottom right of the table, it says 'Defining retention tags'.

g. Federation sharing:

- No sharing configured under Organization > Sharing

The screenshot shows the 'Sharing' section in the Microsoft 365 admin center. The sidebar on the left has links: recipients, permissions, compliance management, organization (which is highlighted with a red box), protection, and mail flow. The main area has a heading 'sharing' followed by 'add-ins address lists'. Below this, it says 'Federation Trust' with a note: 'A federation trust isn't enabled. Create a federation' and a 'Learn more' link. There's a large 'enable' button at the bottom.

h. Malware policy behavior:

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

The screenshot shows the 'malware filter' section in the Microsoft 365 admin center. The sidebar on the left has links: recipients, permissions, compliance management, organization, protection (which is highlighted with a red box), and mail flow. The main area has a heading 'malware filter' followed by a table with columns 'ENABLED', 'NAME', and 'PRIORITY'. One row is visible: 'Enabled' (checkbox checked), 'Default' (highlighted with a red box), and 'Lowest'.

i. Mobile devices registered via ActiveSync:

- No mobile devices currently synchronized

The screenshot shows the 'mobile device access' section in the Microsoft 365 admin center. The sidebar on the left has links: recipients, permissions, compliance management, organization, protection, mail flow, mobile (which is highlighted with a red box), public folders, servers, and hybrid. The main area has a heading 'mobile device access' followed by 'mobile device mailbox policies'. Below this, it says 'Exchange ActiveSync Access Settings' with notes about synchronization rules and exemptions. It also shows a table for 'Quarantined Devices' with columns 'USER', 'DEVICE TYPE', and 'MODEL'. The note at the bottom says 'There are no items to show in !'.

j. Public folders configured:

- No public folders created under Public Folders > public Folders

recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders

public folders public folder mailboxes

+ ⚪ 🗑️ 🔍 ⏮ ⏹ ⏷ ...

\

SUBFOLDER NAME	HAS SUBFOLDERS	MAIL ENAB...
No public folders exist in this organization. Before you create at least one public folder mailbox. To create a public folder, you'll need to assign permissions so user:		

k. Active mailbox database name:

- Mailbox Database **1447570408/AD07** (default name)

recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
servers

databases database availability groups virtual directories certificates

+ ⚪ 🗑️ 🔍 ⏹ ⏷ ...

NAME	ACTIVE ON SERVER	SERVERS WITH COPIES	STATUS	BAD COPY COUNT
Mailbox Databas...	AD07	AD07	Moun...	0

Mailbox Database 1447570408

Servers
AD07

Database copies
Mailbox Database 1447570408/AD07
Active Mounted
Copy queue length: 0
Content index state: NotApplicable
[View details](#)

l. Digital certificates installed:

- 1 self-signed certificate

recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
servers

servers databases database availability groups virtual directories **certificates**

Select server: ad07.domain07.local

+ ⚪ 🗑️ 🔍 ⏹ ⏷ ...

NAME	STATUS	EXPIRES ON
Microsoft Exchange Server Auth Certificate	Valid	5/22/2030
Microsoft Exchange	Valid	6/17/2030
WMSVC-SHA2	Valid	6/14/2035

Microsoft Exchange Server Auth Certificate

Self-signed certificate
Issuer: CN=Microsoft Exchange Server Auth Certificate

Status
Valid
Expires on: 5/22/2030
[Renew](#)

Assigned to services
SMTP

Exchange services bound to it:

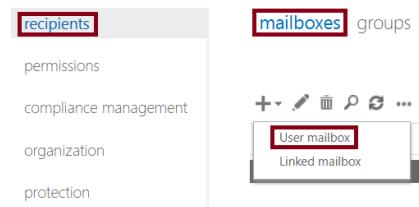
- SMTP, IIS, POP, IMAP

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\$

User Mailbox - Profile 1 - Microsoft Edge
https://ad07.domain07.local/ecp/UsersGroups/NewMailbox...
new user mailbox

First name: Guillermo
Initials:
Last name: Padilla Keymole
Display name: Guillermo Padilla Keymole
Name: Guillermo Padilla Keymole
Organizational unit:
User logon name: gkeymole @ domain07.local
New password:
Confirm password:
Require password change on next logon
Save Cancel

Saved the mailbox and verified it appears in the list.

mailboxes groups resources contacts shared migration

DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS
Administrator	User	Administrator@domain07.local
Guillermo Padilla Keymole	User	gkeymole@domain07.local

```
#####
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.

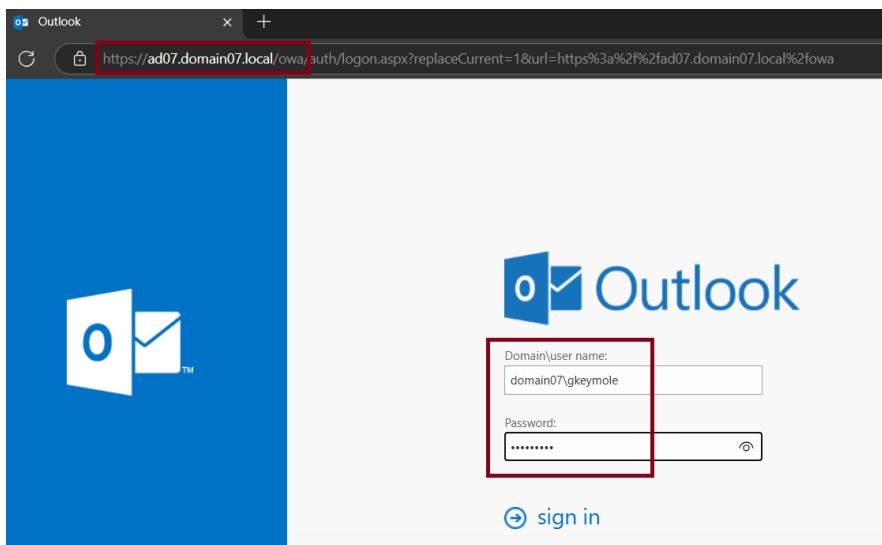
Step 1 - Open Outlook Web App as the new user

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

Logged **in** as:

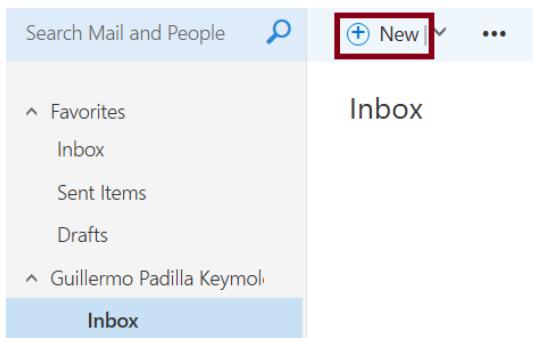
Username: domain07\gkeymole

Password: Passw0rd\$



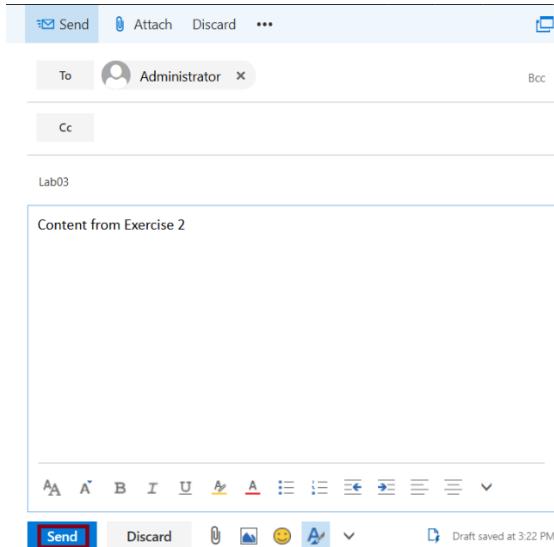
Step 2 - Compose and send a new email

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:

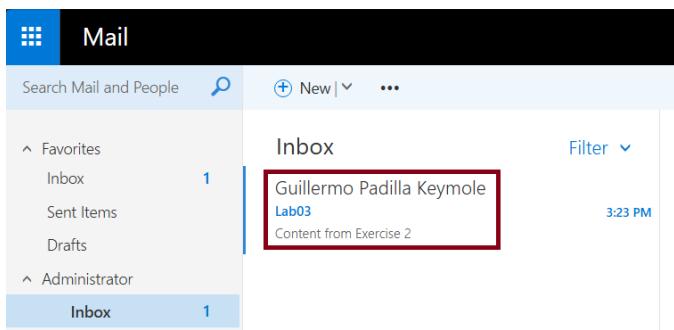
Username: domain07\Administrator

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.

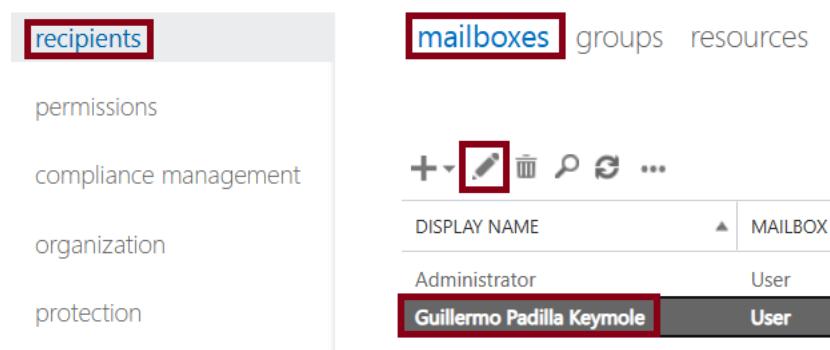
Step 7 – Edit mailbox quota for the new user

Navigated to:

Recipients > Mailboxes

Located user: **Guillermo Padilla Keymole**

Clicked the pencil (edit) icon to open mailbox properties.

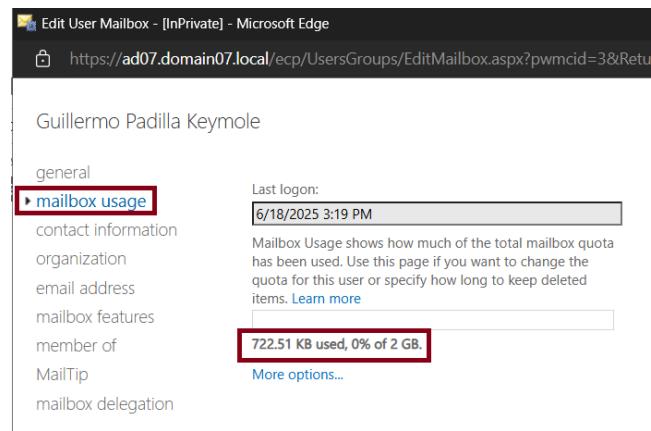


The screenshot shows the Exchange Admin Center (EAC) interface. The top navigation bar has tabs for 'recipients', 'mailboxes' (which is highlighted in blue), 'groups', and 'resources'. On the left, there's a sidebar with links for 'permissions', 'compliance management', 'organization', and 'protection'. The main area shows a list of mailboxes with columns for 'DISPLAY NAME' and 'MAILBOX'. An entry for 'Guillermo Padilla Keymole' is selected, and the 'User' role is highlighted. Above the list are icons for adding (+), editing (pencil), deleting (trash), searching (magnifying glass), and more (ellipsis).

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



The screenshot shows the 'Edit User Mailbox' page for Guillermo Padilla Keymole. The URL is https://ad07.domain07.local/ecp/UsersGroups/EditMailbox.aspx?pwmcid=3&Retu... The left sidebar has links for general, mailbox usage (which is selected and highlighted in red), contact information, organization, email address, mailbox features, member of, MailTip, and mailbox delegation. The main content area shows 'Last logon' as 6/18/2025 3:19 PM. Below it, a section titled 'Mailbox Usage' states: 'Mailbox Usage shows how much of the total mailbox quota has been used. Use this page if you want to change the quota for this user or specify how long to keep deleted items.' It also says '722.51 KB used, 0% of 2 GB.' and has a 'More options...' link.

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****

Guillermo Padilla Keymole

general 722.51 KB used, 0% of 2 GB.

▶ **mailbox usage**

contact information
organization
email address
mailbox features
member of
MailTip
mailbox delegation

Use the default quota settings from the mailbox database
 Customize the quota settings for this mailbox

*Issue a warning at (GB):
1

*Prohibit send at (GB):
1

*Prohibit send and receive at (GB):
1.2

Use the default retention settings from the mailbox database
 Customize the retention settings for this mailbox

*Keep deleted items for (days):
30

Don't permanently delete items until the database is backed up

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$
```

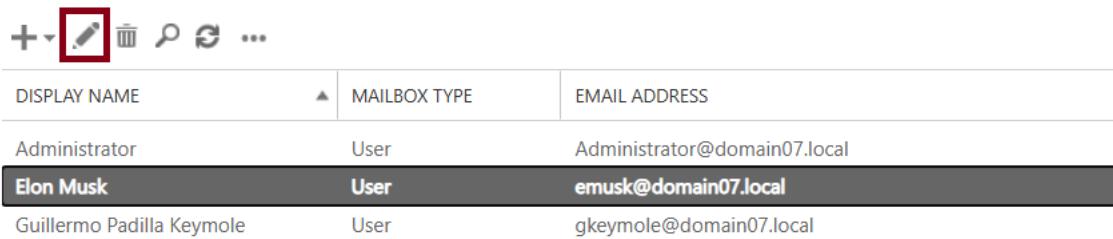
Step 9 – Verify new user in EAC

In the EAC, I went to:

```
Recipients > Mailboxes
```

I located the user Elon Musk in the mailbox list

mailboxes groups resources contacts shared migration



DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS
Administrator	User	Administrator@domain07.local
Elon Musk	User	emusk@domain07.local
Guillermo Padilla Keymole	User	gkeymole@domain07.local

Clicked the pencil (edit icon) 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

The screenshot shows the 'Edit User Mailbox' page in Microsoft Edge. The URL is https://ad07.domain07.local/ecp/UsersGroups/EditMailbox.aspx?pwmcid=5&ReturnObjectType=... The user selected is 'Elon Musk'. The left sidebar has links for general, contact information, organization, email address, mailbox features, member of, MailTip, and mailbox delegation. The 'mailbox usage' link is selected. On the right, under 'Last logon:', there is a note: 'Mailbox Usage shows how much of the total mailbox quota has been used. Use this page if you want to change the quota for this user or specify how long to keep deleted items.' Below it, it says '0 B used, 0% of 1 GB.' There are two radio button options: 'Use the default quota settings from the mailbox database' (unchecked) and 'Customize the quota settings for this mailbox' (checked). Under 'Customize', there are three dropdown menus:

- *Issue a warning at (GB): 1
- *Prohibit send at (GB): 1
- *Prohibit send and receive at (GB): 2

At the bottom, a note says '(C) Use the default retention settings from the mailbox database' (radio button checked). At the very bottom are 'Save' and 'Cancel' buttons.

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)

NAME	
Compliance Management	
Delegated Setup	
Discovery Management	
Help Desk	
Hygiene Management	
Organization Management	
Public Folder Management	
Recipient Management	
Records Management	
Security Administrator	
Security Reader	
Server Management	
UM Management	
View-Only Organization Management	

Assigned Roles
Active Directory Permissions
Address Lists
Audit Logs
Cmdlet Extension Agents
Compliance Admin
Data Loss Prevention
Database Availability Groups
Database Copies
Databases
Disaster Recovery
Distribution Groups
Edge Subscriptions
E-Mail Address Policies
Exchange Connectors
Exchange Server Certificates
Exchange Servers
Exchange Virtual Directories
Federated Sharing
Information Rights Management
Journaling
Legal Hold
Mail Enabled Public Folders
Mail Recipient Creation
Mail Recipients
Mail Tips
Message Tracking
Migration
Monitoring
Move Mailboxes
Org Custom Apps
Org Marketplace Apps
Organization Client Access

Members
Administrator

Role Group 2: Recipient Management

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

Compliance Management	Recipient Management
Delegated Setup	
Discovery Management	
Help Desk	
Hygiene Management	
Organization Management	
Public Folder Management	
Recipient Management	
Records Management	
Security Administrator	
Security Reader	
Server Management	
UM Management	
View-Only Organization Management	

Assigned Roles
Distribution Groups
Mail Recipient Creation
Mail Recipients
Message Tracking
Migration
Move Mailboxes
Recipient Policies
Team Mailboxes

Members

Role Group 3: Compliance Management

- Assigned Roles:
 - Audit Logs
 - Information Rights Management
 - Data Loss Prevention
 - Transport Rules
- Members:
 - No members currently assigned (empty)

The screenshot shows the 'Compliance Management' role group details. On the left, a sidebar lists various management categories. On the right, the main pane displays the role group's purpose, assigned roles, and member status.

Compliance Management

Delegated Setup
Discovery Management
Help Desk
Hygiene Management
Organization Management
Public Folder Management
Recipient Management
Records Management
Security Administrator
Security Reader
Server Management
UM Management
View-Only Organization Management

Compliance Management

This role group will allow a specified user, responsible for compliance, to properly configure and manage compliance settings within Exchange in accordance with their policy.

Assigned Roles

Audit Logs
Compliance Admin
Data Loss Prevention
Information Rights Management
Journaling
Message Tracking
Retention Management
Transport Rules
View-Only Audit Logs
View-Only Configuration
View-Only Recipients

Members

Step 4 - Edit Organization Management Role Group

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

The screenshot shows the 'Edit Role Group' interface for the 'Organization Management' group. It includes fields for name, a list of assigned roles, and a list of available roles.

NAME

Compliance Management
Delegated Setup
Discovery Management
Help Desk
Hygiene Management
Organization Management

Roles:

+ -

NAME
Active Directory Permissions
Address Lists
Audit Logs
Cmdlet Extension Agents
Compliance Admin

- 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

Write scope:

Default

Organizational unit:

[redacted]

Step 5 - Switch to User Roles Tab

I clicked on the User Roles tab

The screenshot shows the 'User Roles' tab selected in the ECP interface. On the left, there's a sidebar with categories: recipients, permissions (which is selected), compliance management, organization, and protection. The main area shows a list of role assignment policies. One policy, 'Default Role Assignment Policy', is highlighted with a red box.

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

The screenshot shows the 'Edit Role Assignment Policy' page for the 'Default Role Assignment Policy'. The 'Name' field is filled with 'Default Role Assignment Policy'. The 'Description' field contains the text: 'This policy grants end users the permission to set their options in Outlook on the web and perform other self-administration tasks.'

Roles included:

- MyBaseOptions
- MyContactInformation
- MyMobileInformation
- MyDistributionGroupMembership
- MyProfileInformation
- MyTextMessaging
- MyVoiceMail
- MyDistributionGroups

Default Role Assignment Policy

Other roles:

- My Custom Apps
This role will allow users to view and modify their custom apps.
- My Marketplace Apps
This role will allow users to view and modify their marketplace apps.
- My ReadWriteMailbox Apps
This role will allow users to install apps with ReadWriteMailbox permissions.
- MyBaseOptions
This role enables individual users to view and modify the basic configuration of their own mailbox and associated settings.
- MyRetentionPolicies
This role enables individual users to view their retention tags and view and modify their retention tag settings and defaults.

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        : 
Name                  : 
DistinguishedName      : 
Identity               : 
Guid                  : ffd993c1-895b-461c-b13f-f13807635ea1
ObjectCategory         : 
ObjectClass            : 
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           : AAMkAGUXNGF1ZDUlLTi3M2ItNGZios05MTc5LTI5OGYwNmR1NGI4NgBGAAAAAAARN8WQnbOOT5yDgkwPQ6/tBwBmR15cTwDRJ5Sm  
OF2PMbAAAAAAEbaABmR15cTwDRJ5SmP0F2PMbAAAAYwrYAAA=  
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           : AAMkAGUXNGF1ZDUlLTi3M2ItNGZios05MTc5LTI5OGYwNmR1NGI4NgBGAAAAAAARN8WQnbOOT5yDgkwPQ6/tBwBmR15cTwDRJ5Sm  
OF2PMbAAAAAAEbaABmR15cTwDRJ5SmP0F2PMbAAAAYwrXAAA=  
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          Activate Windows
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.local -Password (ConvertTo-SecureString -String 'Passw0rd$' -AsPlainText -Force) -FirstName Antoine -LastName Tohme -Alias atohme
```

Name	Alias	ServerName	ProhibitSendQuota
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          : AAMkAGUXNGF1ZDU1LTi3M2ItNGZios05MTc5LTi5OGYwNmRlNGI4NgBGAAAAAAARN8WQnb00T5yDg
kwPQ6/tBwBmR15cTwdHRj5SmP0F2PMbAAAAAEbAABmR15cTwdHRj5SmP0F2PMbAAAAAYwrhAAA=
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}
StartTimeUtc         : 6/5/2025 1:09:28 AM
EndTimeUtc          : 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 -ExpandProperty AuditOwner
UpdateFolderPermissions
UpdateInboxRules
UpdateCalendarDelegation
```

Activate Windows

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 -ExpandProperty 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

The screenshot shows the Microsoft Outlook inbox on the left and a detailed view of an email on the right. In the inbox, there is one unread email from "Antoine Tohme" with the subject "Mailbox Simulation Activity". The email body contains the text "Another Test for you 😊". On the right, a detailed view of the same email is shown under the heading "Mailbox Simulation Activity". The email is from "Antoine Tohme" at "Today, 9:48 PM" and is marked as an "Administrator". The body of the email is identical to the one in the inbox. Below the email, there is a small "..." button.

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 :
FolderPathName :
FolderName :
MemberRights :
MemberSid :
MemberUpn :
ClientInfoString : Client=OWA;Action=ViaProxy
ClientIPAddress : 192.178.7.1
ClientMachineName :
ClientProcessName :
ClientVersion :
InternalLogonType :
MailboxOwnerUPN :
MailboxOwnerId :
DestMailboxOwnerUPN :
DestMailboxOwnerId :
DestMailboxGuid :
CrossMailboxOperation :
LogonUserDisplayName :
LogonUserId :
SourceItems :
SourceFolders :
SourceItemIdsList :
SourceItemSubjectsList :
SourceItemAttachmentsList :
SourceItemFolderPathNamesList :
SourceFolderPathNamesList :
ItemId :
ItemSubject : Antoine Tohme
ItemAttachments :
DirtyProperties :
OriginatingServer :
OperationProperties :
MailboxGuid :
MailboxResolvedOwnerName :
LastAccessed :
Identity :
IsValid :
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.