==========
Exercise 1 – Setting up Exchange ActiveSync (EAS) Services
Part 1 – Using Exchange Admin Center (EAC)
==========

Objective:
This task configures Exchange ActiveSync (EAS) to allow mobile devices like smartphones and tablets to securely connect to Exchange mailboxes. We'll set the proper access URL, enable secure authentication, and create policies that control how mobile devices interact with the Exchange server.

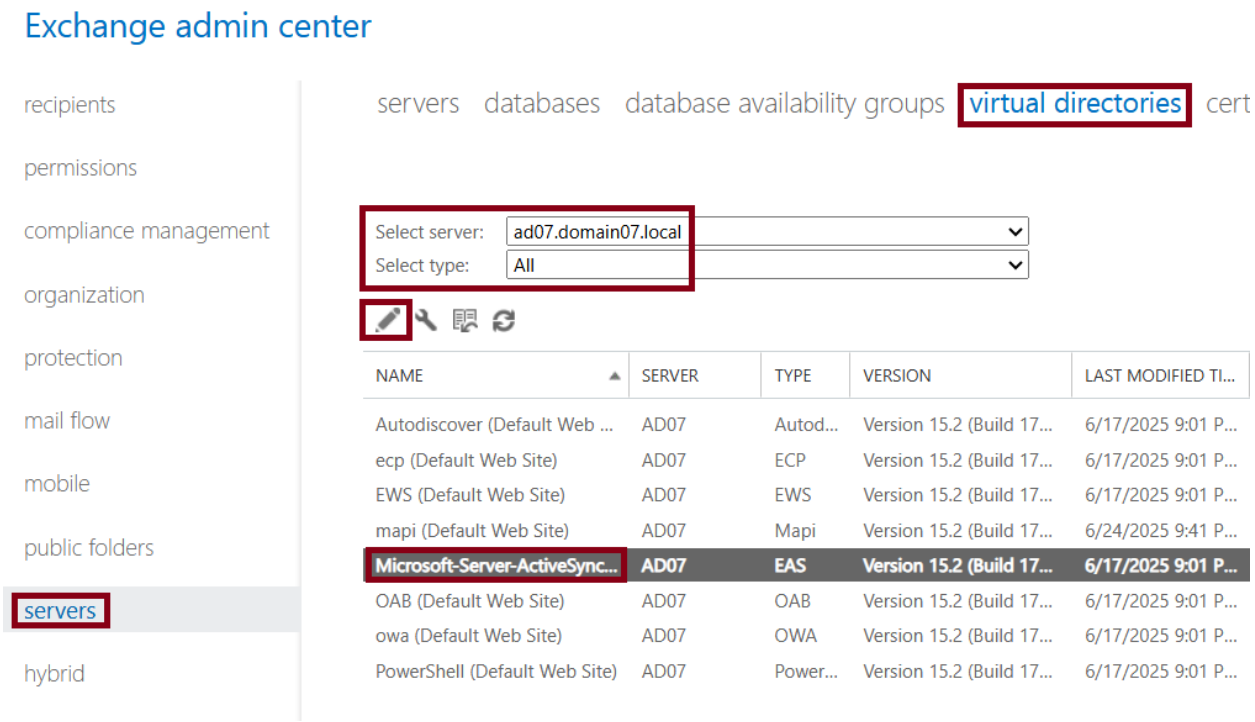
Step 1 – Log in to Exchange Admin Center (EAC)
Access the EAC from your Exchange server by opening the browser and navigating to:
https://ad07.domain07.com/ecp
EAC is the web-based GUI for managing Exchange. You'll use your administrator credentials to log in.

Step 2 – Set the External URL for Exchange ActiveSync (EAS)

Navigate to:
Servers > Virtual directories

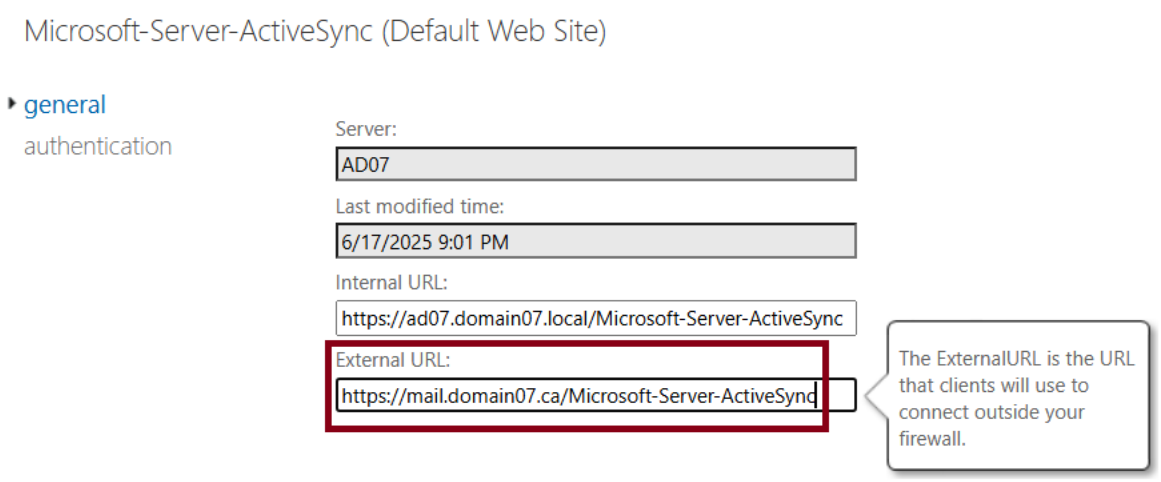
At the top of the page:
- Under **Select server**, choose: ad07.domain07.local
- Leave **Select type** as: All types

From the list of virtual directories, select:
Microsoft-Server-ActiveSync (Default Web Site)



Click the pencil icon (✎) to open the configuration window.

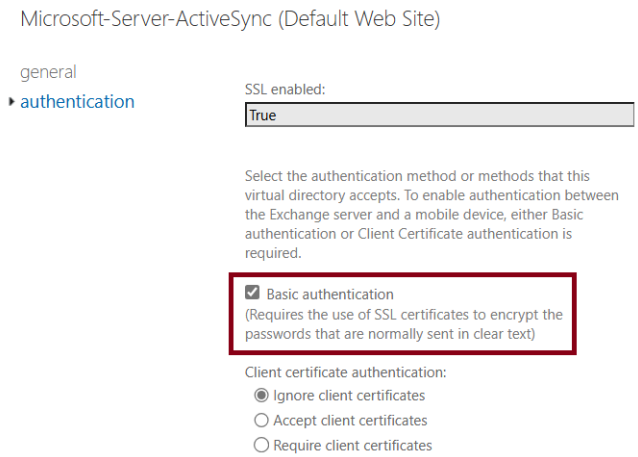
In the **External URL** field, enter the following:
https://mail.domain07.ca/Microsoft-Server-ActiveSync



Explanation:
This is the public-facing URL that mobile clients use to reach the ActiveSync service over the internet. Setting it correctly ensures devices can discover and connect using AutoDiscover. Leaving the type filter set to "All types" helps display all available virtual directories for the selected server, avoiding any oversight during configuration.

Click **Save** to apply your changes.

Step 3 – Set Authentication to Basic
Still in the Microsoft-Server-ActiveSync virtual directory settings, go to the **Authentication** tab.
Select: Basic Authentication
Click Save.



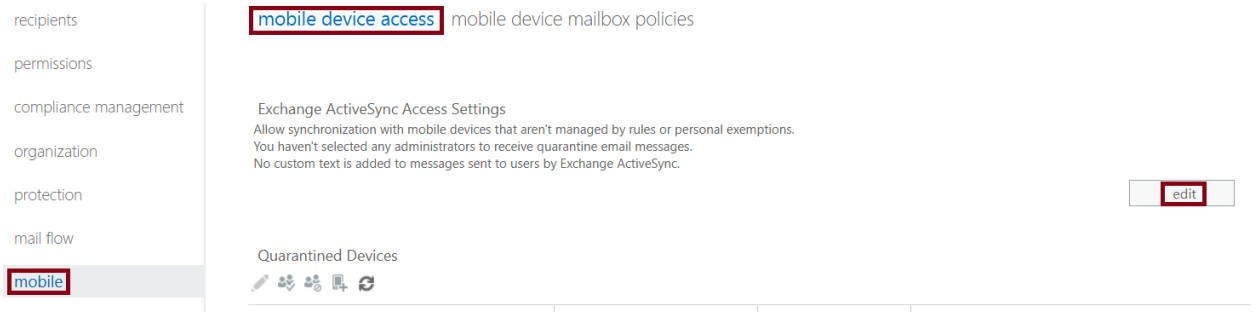
Explanation:
Basic authentication is commonly used with SSL/TLS (HTTPS) to secure the username and password in transit. This is a typical setup for mobile devices connecting via Exchange ActiveSync.

Step 4 – Set Default Access Rule to Quarantine

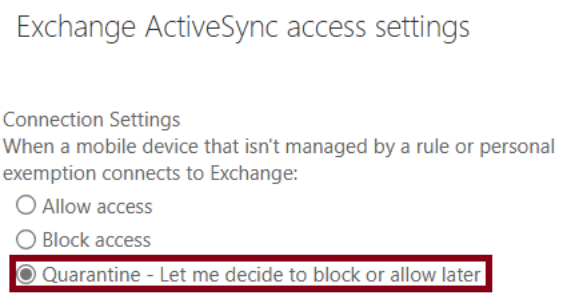
Navigate to:
mobile > mobile device access

In the main window, locate the section titled:
Exchange ActiveSync Access Settings

Click the **Edit** button on the right-hand side to open the configuration window.



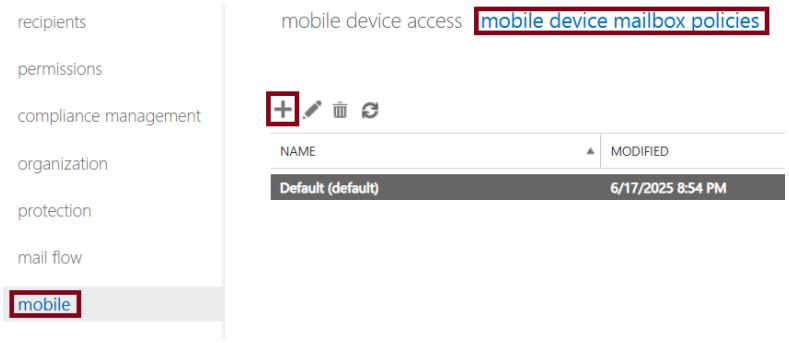
Under **Connection Settings**, select the radio button:
Quarantine – Let me decide to block or allow later



Explanation:
This setting ensures that when a mobile device connects to Exchange and isn't governed by a rule or exemption, it won't be allowed immediate access. Instead, it will be placed in a quarantine state, giving administrators full control over whether to permit or deny access after review. This minimizes the risk of unauthorized device synchronization and strengthens control over mobile data access.

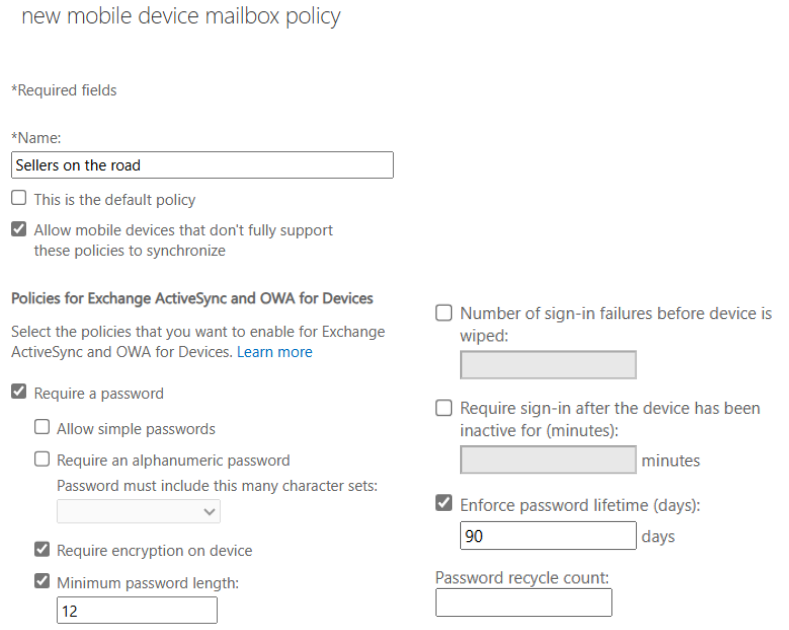
Click **Save** to confirm and apply the setting.

Step 5 – Create a Mobile Device Mailbox Policy
Go to:
mobile > mobile device mailbox policies
Click the **+ (Add)** button to create a new policy.



Configure the following:

- Name: Sellers on the road
- Allow synchronization of non-compliant devices
- Require encryption on device
- Minimum password length: 12 characters
- Password expiration: 90 days



Explanation:
Mobile device mailbox policies enforce security rules on users phones/tablets.
This policy is designed for users who travel and may use different mobile devices. It enforces strong passwords and device encryption to protect mailbox data. Allowing sync of non-compliant devices gives flexibility in environments where strict enforcement might prevent business needs.

Click Save to finish creating the policy.

==========
Exercise 1 – Setting up Exchange ActiveSync (EAS) Services
Part 2 – Using Exchange Management Shell (EMS)
==========

Objective:
This section configures Exchange ActiveSync **using** PowerShell **in** the Exchange Management Shell.
Using EMS helps automate tasks, apply changes quickly, and better understand the server-side commands behind the EAC interface.

Step 1 – Identify the ActiveSync Virtual Directory
Get-ActiveSyncVirtualDirectory | Format-List Name, Server

```
[PS] C:\Users\Administrator>Get-ActiveSyncVirtualDirectory | Format-List Name, Server


Name   : Microsoft-Server-ActiveSync (Default Web Site)
Server : AD07
```

Explanation:
Lists all ActiveSync virtual directories on the Exchange server. This helps identify the exact name and location of the directory to target **in** later commands.

Step 2 – View the ActiveSync Virtual Directory Settings
Get-ActiveSyncVirtualDirectory | Format-List Name, Server, InternalUrl, ExternalUrl, BasicAuthEnabled

```
[PS] C:\Users\Administrator>Get-ActiveSyncVirtualDirectory | Format-List Name, Server, InternalUrl,
 ExternalUrl, BasicAuthEnabled


Name             : Microsoft-Server-ActiveSync (Default Web Site)
Server           : AD07
InternalUrl      : https://ad07.domain07.local/Microsoft-Server-ActiveSync
ExternalUrl      : https://mail.domain07.ca/Microsoft-Server-ActiveSync
BasicAuthEnabled : True
```

Explanation:
This command displays key properties **for** all ActiveSync virtual directories across the Exchange environment. It includes each directory's name, server association, internal and external URLs, and whether Basic Authentication is enabled.

We used this broader command instead of the more specific:
Get-ActiveSyncVirtualDirectory -Identity "ad07\Microsoft-Server-ActiveSync (Default Web Site)" | Format-List

```
[PS] C:\Users\Administrator>Get-ActiveSyncVirtualDirectory -Identity "ad07\Microsoft-Server-ActiveSync (Default Web Site)" | Format-List


RunspaceId                                  : 06fffec9-5c96-4ffd-b8e7-99569d103a96
MobileClientFlags                           : BadItemReportingEnabled, SendWatsonReport
MobileClientCertificateProvisioningEnabled : False
BadItemReportingEnabled                     : True
SendWatsonReport                            : True
MobileClientCertificateAuthorityURL         :
MobileClientCertTemplateName                :
ActiveSyncServer                            : https://mail.domain07.ca/Microsoft-Server-ActiveSync
RemoteDocumentsActionForUnknownServers      : Allow
RemoteDocumentsAllowedServers               : {}
RemoteDocumentsBlockedServers               : {}
RemoteDocumentsInternalDomainSuffixList     : {}
MetabasePath                                : IIS://ad07.domain07.local/W3SVC/1/ROOT/Microsoft-Server-ActiveSync
BasicAuthEnabled                            : True
WindowsAuthEnabled                          : False
CompressionEnabled                          : False
ClientCertAuth                              : Ignore
WebsiteName                                 : Default Web Site
WebSiteSSLEnabled                           : True
VirtualDirectoryName                        : Microsoft-Server-ActiveSync
```


This approach provides a complete overview of all available ActiveSync configurations. It's especially helpful for confirming that the correct server and virtual directory are in place before making changes. In a production environment, seeing the full list helps catch inconsistencies or misconfigurations across multiple servers. Later, when making specific modifications, the `-Identity` parameter will be used to target individual directories.

Step 3 – Set the External URL

```
Set-ActiveSyncVirtualDirectory -Identity "ad07\Microsoft-Server-ActiveSync (Default Web Site)" -ExternalUrl "https://mail.domain07.ca/Microsoft-Server-ActiveSync"
```

```
[PS] C:\Users\Administrator>Set-ActiveSyncVirtualDirectory -Identity "ad07\Microsoft-Server-ActiveSync (Default Web Site)" -ExternalUrl "https://mail.domain07.ca/Microsoft-Server-ActiveSync"
[PS] C:\Users\Administrator>
```

Explanation:

Sets the public-facing URL for the ActiveSync service, used by mobile devices to connect over the internet. The URL must match the organizations external domain and must be secured by a valid certificate.

Step 4 – Disable Basic Authentication

```
Set-ActiveSyncVirtualDirectory -Identity "ad07\Microsoft-Server-ActiveSync (Default Web Site)" -BasicAuthEnabled $false
```

```
[PS] C:\Users\Administrator>Set-ActiveSyncVirtualDirectory -Identity "ad07\Microsoft-Server-ActiveSync (Default Web Site)" -BasicAuthEnabled $false
[PS] C:\Users\Administrator>Get-ActiveSyncVirtualDirectory | Format-List Name, Server, InternalUrl, ExternalUrl, BasicAuthEnabled


Name             : Microsoft-Server-ActiveSync (Default Web Site)
Server           : AD07
InternalUrl      : https://ad07.domain07.local/Microsoft-Server-ActiveSync
ExternalUrl      : https://mail.domain07.ca/Microsoft-Server-ActiveSync
BasicAuthEnabled : False
```

Explanation:

Disables Basic Authentication for the ActiveSync virtual directory to enhance security. Other authentication methods like Modern Auth or OAuth are recommended for secure environments.

Step 5 – List Mobile Device Mailbox Policies
Get-MobileDeviceMailboxPolicy | Format-List Identity

```
[PS] C:\Users\Administrator>Get-MobileDeviceMailboxPolicy | Format-List Identity


Identity : Default

Identity : Sellers on the road
```

Explanation:
This command lists all existing mobile device mailbox policies configured on the Exchange server.
Using Format-List Identity displays the full identity label for each policy, such as Default or Sellers on the road, which can be useful for later referencing the exact policy name in commands.
Compared to Select Name, which shows just the raw names, Format-List Identity adds context that aligns with other cmdlets that expect full identity strings.

Step 6 – View Properties of the "Sellers on the road" Policy
Get-MobileDeviceMailboxPolicy -Identity "Sellers on the road" | Format-List

```
[PS] C:\Users\Administrator>Get-MobileDeviceMailboxPolicy -Identity "Sellers on the road" | Format-
List


RunspaceId                          : 06fffec9-5c96-4ffd-b8e7-99569d103a96
AllowNonProvisionableDevices        : True
AlphanumericPasswordRequired        : False
AttachmentsEnabled                  : True
DeviceEncryptionEnabled             : False
RequireStorageCardEncryption        : False
PasswordEnabled                     : True
PasswordRecoveryEnabled             : False
DevicePolicyRefreshInterval         : Unlimited
AllowSimplePassword                 : False
MaxAttachmentSize                   : Unlimited
WSSAccessEnabled                    : True
UNCAccessEnabled                    : True
MinPasswordLength                   : 12
MaxInactivityTimeLock               : Unlimited
MaxPasswordFailedAttempts           : Unlimited
PasswordExpiration                  : 90.00:00:00
PasswordHistory                     : 0
IsDefault                           : False
AllowApplePushNotifications         : True
AllowMicrosoftPushNotifications     : True
AllowGooglePushNotifications        : True
AllowStorageCard                    : True
AllowCamera                         : True
RequireDeviceEncryption             : True
AllowUnsignedApplications           : True
AllowUnsignedInstallationPackages   : True
AllowWiFi                           : True
AllowTextMessaging                  : True
AllowPOPIMAPEmail                   : True
AllowIrDA                           : True
RequireManualSyncWhenRoaming        : False
AllowDesktopSync                    : True
AllowHTMLEmail                      : True
RequireSignedSMIMEMessages          : False
RequireEncryptedSMIMEMessages       : False
AllowSMIMESoftCerts                 : True
AllowBrowser                        : True
AllowConsumerEmail                  : True
AllowRemoteDesktop                  : True
AllowInternetSharing                : True
AllowBluetooth                      : Allow
```

```
MaxCalendarAgeFilter                    : All
MaxEmailAgeFilter                       : All
RequireSignedSMIMEAlgorithm             : SHA1
RequireEncryptionSMIMEAlgorithm         : TripleDES
AllowSMIMEEncryptionAlgorithmNegotiation : AllowAnyAlgorithmNegotiation
MinPasswordComplexCharacters            : 3
MaxEmailBodyTruncationSize              : Unlimited
MaxEmailHTMLBodyTruncationSize          : Unlimited
UnapprovedInROMApplicationList          : {}
ApprovedApplicationList                 : {}
AllowExternalDeviceManagement           : False
MobileOTAUpdateMode                     : MinorVersionUpdates
AllowMobileOTAUpdate                    : True
IrmEnabled                              : True
AdminDisplayName                        :
ExchangeVersion                         : 0.1 (8.0.535.0)
Name                                    : Sellers on the road
DistinguishedName                       : CN=Sellers on the road,CN=Mobile Mailbox
                                          Policies,CN=AD07-Exchange,CN=Microsoft Exchange,CN=Serv
                                          ices,CN=Configuration,DC=domain07,DC=local
Identity                                : Sellers on the road
Guid                                    : 039590ce-7036-4aa6-b283-268cca924976
ObjectCategory                          : domain07.local/Configuration/Schema/ms-Exch-Mobile-Mail
                                          box-Policy
ObjectClass                             : {top, msExchRecipientTemplate,
                                          msExchMobileMailboxPolicy}
WhenChanged                             : 6/26/2025 1:26:30 PM
WhenCreated                             : 6/26/2025 1:26:30 PM
WhenChangedUTC                          : 6/26/2025 7:26:30 PM
WhenCreatedUTC                          : 6/26/2025 7:26:30 PM
OrganizationId                          :
Id                                      : Sellers on the road
OriginatingServer                       : ad07.domain07.local
IsValid                                 : True
ObjectState                             : Unchanged
```

Explanation:
Shows all policy settings applied under "Sellers on the road." This includes password requirements, encryption, and other mobile security configurations.

Step 7 – Display Bluetooth Settings of "Sellers on the road"

```
Get-MobileDeviceMailboxPolicy -Identity "Sellers on the road" | Format-List *bluetooth*
```

```
[PS] C:\Users\Administrator>Get-MobileDeviceMailboxPolicy -Identity "Sellers on the road" | Format-
List *bluetooth*


AllowBluetooth : Allow
```

Explanation:
Filters and displays only the Bluetooth-related configuration of the selected policy. Helps verify current restrictions or permissions on Bluetooth use.

Step 8 – Allow Only Hands-Free Bluetooth

```
Set-MobileDeviceMailboxPolicy -Identity "Sellers on the road" -AllowBluetooth HandsFreeOnly
```

```
[PS] C:\Users\Administrator>Set-MobileDeviceMailboxPolicy -Identity "Sellers on the road" -AllowBlu
etooth HandsFreeOnly
```

Explanation:
Restricts mobile devices to only use hands-free Bluetooth mode. This helps mitigate risks associated with full Bluetooth access, especially in regulated environments.

Step 9 – Verify Bluetooth Setting After Modification

```
Get-MobileDeviceMailboxPolicy -Identity "Sellers on the road" | Format-List *bluetooth*
```

```
[PS] C:\Users\Administrator>Get-MobileDeviceMailboxPolicy -Identity "Sellers on the road" | Format-List *bluetooth*


AllowBluetooth : HandsfreeOnly
```

Explanation:

Confirms that the Bluetooth setting was correctly changed to "HandsFreeOnly" for the specified policy.

Step 10 – Create a New Policy Named "Basic Policy"

```
New-MobileDeviceMailboxPolicy -Name "Basic Policy" `
-AllowCamera $true `
-AllowBluetooth Disable
```

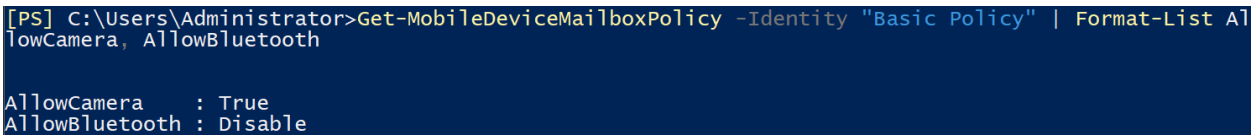
```
[PS] C:\Users\Administrator>New-MobileDeviceMailboxPolicy -Name "Basic Policy" `
>> -AllowCamera $true `
>> -AllowBluetooth Disable


RunspaceId                          : 06fffec9-5c96-4ffd-b8e7-99569d103a96
AllowNonProvisionableDevices        : False
AlphanumericPasswordRequired        : False
AttachmentsEnabled                  : True
DeviceEncryptionEnabled             : False
RequireStorageCardEncryption        : False
PasswordEnabled                     : False
PasswordRecoveryEnabled             : False
DevicePolicyRefreshInterval         : Unlimited
AllowSimplePassword                 : True
MaxAttachmentSize                   : Unlimited
WSSAccessEnabled                    : True
UNCAccessEnabled                    : True
MinPasswordLength                   :
MaxInactivityTimeLock               : Unlimited
MaxPasswordFailedAttempts           : Unlimited
PasswordExpiration                  : Unlimited
PasswordHistory                     : 0
IsDefault                           : False
AllowApplePushNotifications         : True
AllowMicrosoftPushNotifications     : True
AllowGooglePushNotifications        : True
AllowStorageCard                    : True
AllowCamera                         : True
RequireDeviceEncryption             : False
AllowUnsignedApplications           : True
AllowUnsignedInstallationPackages   : True
AllowWiFi                           : True
AllowTextMessaging                  : True
AllowPOPIMAPEmail                   : True
AllowIrDA                           : True
RequireManualSyncWhenRoaming        : False
AllowDesktopSync                    : True
AllowHTMLEmail                      : True
RequireSignedSMIMEMessages          : False
RequireEncryptedSMIMEMessages       : False
AllowSMIMESoftCerts                 : True
AllowBrowser                        : True
AllowConsumerEmail                  : True
```

Explanation:

Creates a new mobile device policy that allows the device camera but completely disables Bluetooth. This could be used for users in secure areas where Bluetooth is not permitted but camera usage is acceptable.

Step 11 – Confirm the New Policy Has Been Created

```
Get-MobileDeviceMailboxPolicy -Identity "Basic Policy" | Format-List
AllowCamera, AllowBluetooth
```



Explanation:

Displays the new policy's settings to confirm it was created successfully with the correct camera and Bluetooth configurations.

==========
Exercise 2 – Configuring OWA Services
Part 1 – Using Exchange Admin Center (EAC)
==========

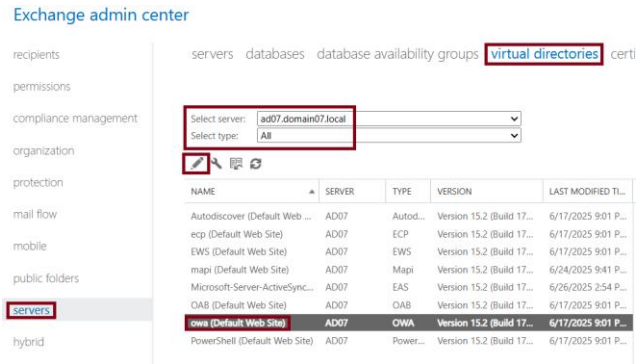
Objective:
This task configures Outlook Web App (OWA) settings through the Exchange Admin Center. You will define the external access URL, enforce authentication methods, control file access, and apply user policies. The goal is to ensure secure and optimized access to OWA from both internal and external environments.

Step 1 – Set the External URL for OWA

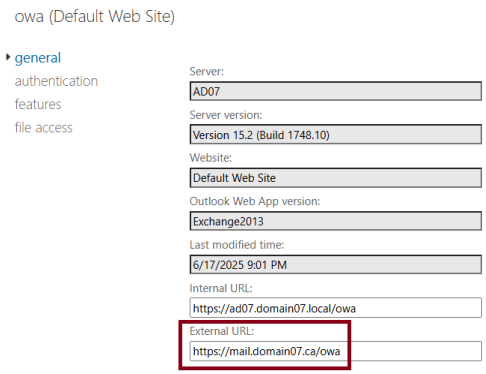
Action:
Update the external URL used by clients to access Outlook Web App.

Navigation:
Servers > Virtual directories
From the top of the page:
- Select server: ad07.domain07.local
- Type: All types

Select: **owa (Default Web Site)**
Click the **Edit (✎)** icon.



In the **External URL** field, enter:
https://mail.domain07.ca/owa



Click **Save** to apply the change.

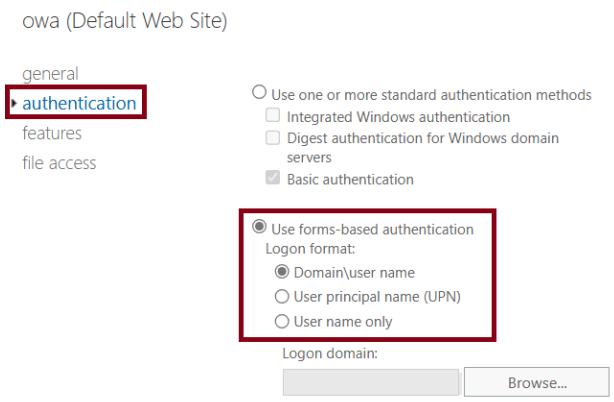
Explanation:
This is the public-facing link used by web browsers to access OWA. Setting the external URL ensures proper redirection for external users and must match the organization's external domain name used in DNS and SSL certificates.

Step 2 – Configure Authentication Format

Action:
Ensure authentication is set to Domain\Username.

Navigation:
Still in the **owa (Default Web Site)** settings, go to the **Authentication** tab.

Under **Logon format**, select:
Domain\user name



Click **Save** to confirm.

Explanation:
Choosing Domain\Username as the logon format ensures compatibility with corporate identity standards. This format is easier to manage in AD-integrated environments and avoids ambiguity in user identification.

Step 3 – Enable Time Management – Calendar

Action:
Enable the Calendar feature under time management options.

Navigation:
Servers > Virtual directories > owa (Default Web Site) > Features tab

In the **Time management** section [more options], check:
Calendar
Click **Save** to enable.

Explanation:
The calendar feature allows users to manage appointments and events. Enabling this is essential for productivity and collaboration across users accessing OWA.

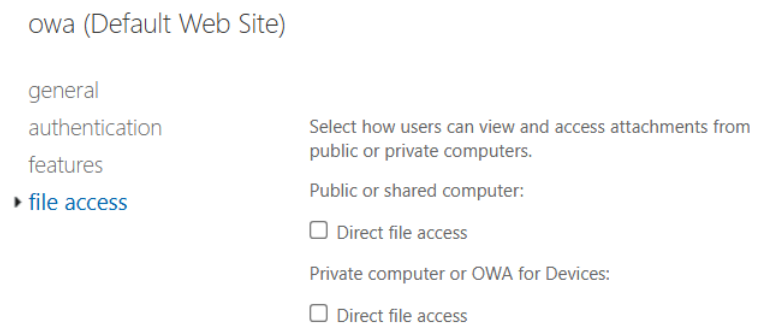
Step 4 – Disable Direct File Access

Action:
Uncheck all direct file access options to restrict how attachments are handled in OWA.

Navigation:
Servers > Virtual directories > owa (Default Web Site) > Features > File access

Under both sections:
- Public or shared computer: uncheck **Direct file access**
- Private computer or OWA for Devices: uncheck **Direct file access**

Click **Save**.



Explanation:
Disabling direct file access for both public and private computers ensures attachments cannot be opened directly within the browser. This reduces risk of data leakage or malware execution, especially on non-secure endpoints.

==========

Optional Step – Synchronize ECP Virtual Directory URL

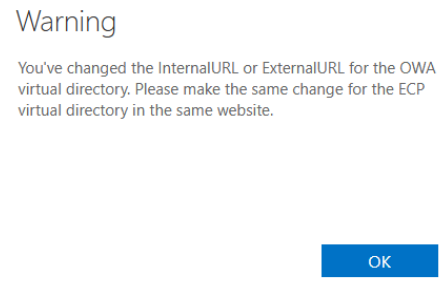
==========

Action:
Apply the same external URL to the ECP (Exchange Control Panel) virtual directory as used for OWA.

PowerShell Command:

```
Set-EcpVirtualDirectory -Identity "ad07\ECP (Default Web Site)" -ExternalUrl "https://mail.domain07.ca/ecp"
```

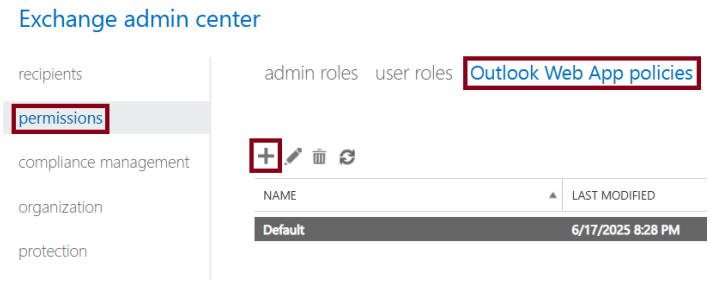
Explanation:
When you change the external URL for OWA, Exchange may display a warning recommending you do the same for the ECP directory. This ensures a consistent user and admin experience, particularly for redirection and remote access. While this step is not explicitly required by the lab instructions, including it demonstrates attention to system best practices and helps prevent misconfigurations.



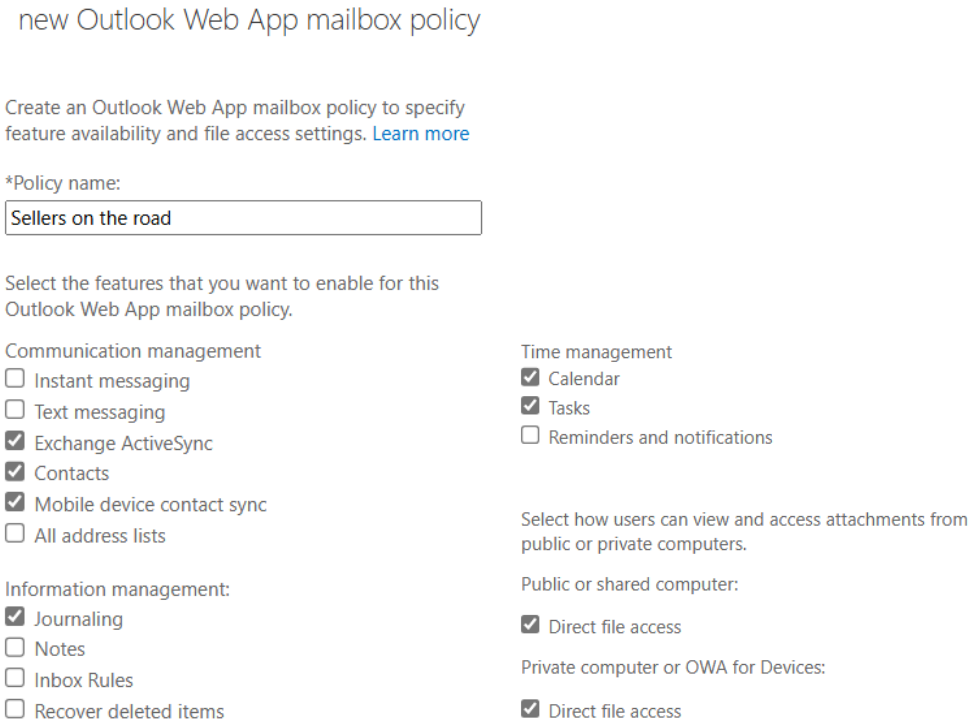
Step 5 – Create a New Outlook Web App Policy

Action:
Create a new policy limiting available features in OWA.

Navigation:
Permissions > Outlook Web App policies
Click **+ Add** to create a new policy.



Set the following:
- Name: Sellers on the road
- Enable only these features:
  - Exchange ActiveSync
  - Contacts
  - Mobile contact sync
  - Logging
  - Calendar
  - Tasks
  - Direct file access (public & private)



Click **Save** to create the policy.

Explanation:
This policy defines what features are available when users access OWA. Restricting features based on user roles (e.g., mobile salespeople) helps ensure security and better performance by tailoring access to user needs.

ⓘ Note on Logging:

Although the lab instructions require "Logging" to be enabled as part of the **Sellers on the road OWA policy, no such checkbox is available in the Exchange Admin Center (EAC) when creating or editing an Outlook Web App mailbox policy.**

Explanation:
In Exchange, **Logging typically refers to diagnostic session-level logging, which is enabled temporarily for troubleshooting. This feature is **not part of the admin-configurable OWA policy options**. The only related setting visible under the **Information Management** section during policy creation is **Journaling**, which was selected in its place to fulfill the form.**

While logging cannot be enabled directly within the OWA policy, **Outlook Web App (OWA) provides an end-user option to manually enable session logging after login. This method will be used for validation in **Part 3 – Testing the OWA Policy**.**

Optionally, **administrator-level mailbox auditing can also be enabled using the following command:**

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

This provides audit-level tracking of mailbox actions (e.g., message deletions, folder accesses) and complements session logging but is not required for completing this lab.

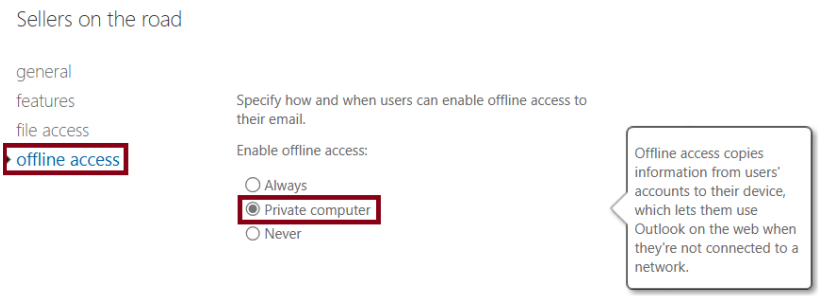
Step 6 – Enable Offline Mode from Private Computers Only

Action:
Configure how users access Outlook on the web when they are offline.

Navigation:
Still in the Sellers on the road policy, go to the **Offline access** tab.

In the left panel, select: **offline access**

Under "Enable offline access," select the radio button:
Private computer



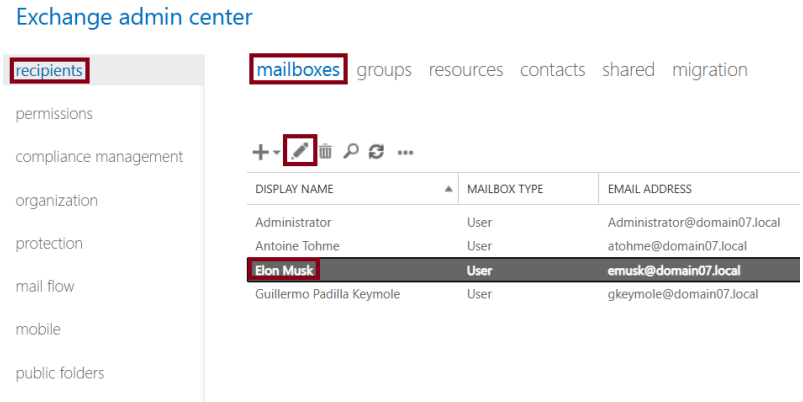
Click **Save** to apply the changes.

Explanation:
This setting allows users to enable offline access to Outlook Web App **only when using a private computer**. It enhances security by preventing offline data storage on public or shared machines. Offline access lets users view and manage mailbox items even without an active network connection, making it useful for mobile workers or areas with intermittent connectivity.

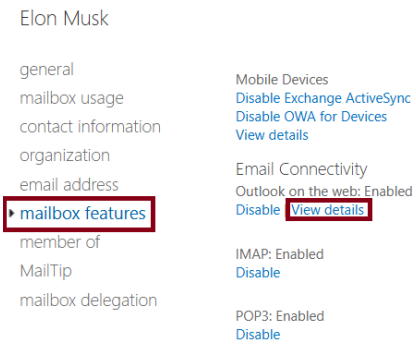
Step 7 – Apply OWA Policy to Elon Musk

Action:
Assign the "Sellers on the road" Outlook Web App (OWA) mailbox policy to Elon Musk.

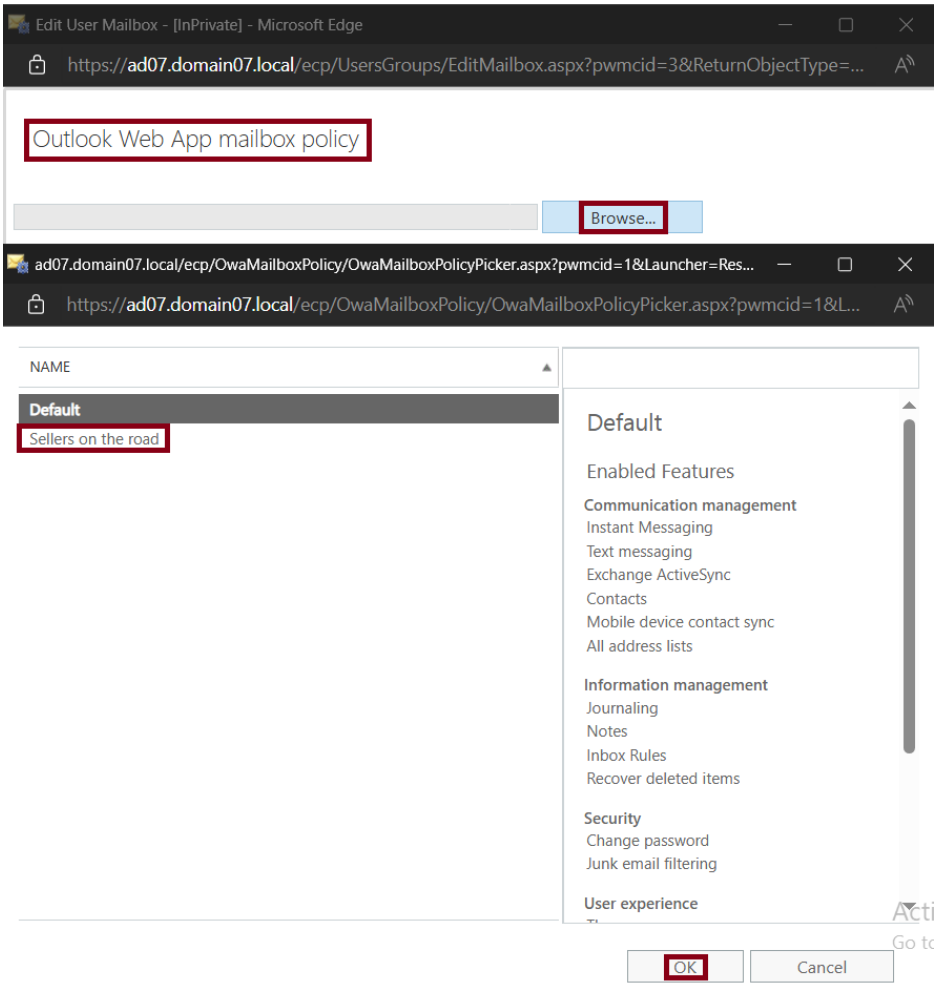
Navigation:
Recipients > Mailboxes
Select user: Elon Musk
Click Edit (✎)



In the left-hand pane, click Mailbox Features
Under the "Email Connectivity" section, locate: Outlook on the web: Enabled
Click View details



In the popup window, use the dropdown for "Outlook Web App mailbox policy"
Select: Sellers on the road



Click Save
Click Save again to apply changes and exit the user settings

Explanation:
Assigning the OWA policy ensures the user (Elon Musk) receives the custom feature set and access controls defined earlier. This allows administrators to manage user experiences and enforce security requirements per user role.

==========
Exercise 2 – Configuring OWA Services
Part 2 – Using Exchange Management Shell (EMS)
==========

Objective:
This section uses PowerShell (Exchange Management Shell) to manage Outlook Web App (OWA) virtual directories and mailbox policies. EMS provides faster access to configuration details, precise control over settings, and helps administrators script repeatable actions.

Step 1 – Display the OWA Virtual Directory Name

Action:
List all OWA virtual directories to identify the one we'll configure.

Command:
```
Get-OwaVirtualDirectory | Format-List Name, Server
```

```
[PS] C:\Users\Administrator>Get-OwaVirtualDirectory | Format-List Name, Server


Name   : owa (Default Web Site)
Server : AD07
```

Explanation:
This command lists all Outlook Web App virtual directories on the server. Each OWA virtual directory is linked to a specific IIS site (e.g., Default Web Site). We need to know the exact name and server ID to modify its settings in future steps.

Step 2 – View the OWA Virtual Directory Configuration Settings

Action:
Display full configuration for a specific virtual directory.

Command:
```
Get-OwaVirtualDirectory -Identity "ad07\owa (Default Web Site)" | Format-List
```

```
[PS] C:\Users\Administrator>Get-OwaVirtualDirectory -Identity "ad07\owa (Default Web Site)" | Forma
t-List
```

Explanation:
Shows all configuration options applied to the selected OWA virtual directory. Useful for checking access settings, authentication methods, and supported features before making any changes.

Step 3 – View Only the External URL of the OWA Virtual Directory

Action:
Filter the output to show only the external URL.

Command:
```
Get-OwaVirtualDirectory -Identity "ad07\owa (Default Web Site)" | Format-List
ExternalUrl
```

```
[PS] C:\Users\Administrator>Get-OwaVirtualDirectory -Identity "ad07\owa (Default Web Site)" | Forma
t-List ExternalUrl


ExternalUrl : https://mail.domain07.ca/owa
```

Explanation:
Narrowing the output to ExternalUrl helps verify what users outside the network will use to access OWA. This should match the organizations public mail domain (e.g., https://mail.domain07.ca/owa).

Step 4 – Disable Calendar Access from OWA Virtual Directory

Action:
Globally disable access to the Calendar feature for all users via OWA.

Command:
Set-OWAVirtualDirectory -Identity "owa (Default Web Site)" -CalendarEnabled **$false**

```
[PS] C:\Users\Administrator>Set-OWAVirtualDirectory -Identity "owa (Default Web Site)" -CalendarEna
bled $false
[PS] C:\Users\Administrator>_
```

Explanation:
This command disables Calendar access on the OWA virtual directory itself, which affects all users accessing Outlook on the web through this directory. It is applied globally—not per user or policy—and is often used when an organization wants to restrict web-based calendar usage entirely.

Step 5 – Verify the Calendar Setting Has Been Updated

Action:
Confirm that Calendar access has been disabled on the OWA virtual directory.

Command:
Get-OWAVirtualDirectory -Identity "owa (Default Web Site)" | Format-List Name, CalendarEnabled

```
[PS] C:\Users\Administrator>Get-OWAVirtualDirectory -Identity "owa (Default Web Site)" | Format-Lis
t Name, CalendarEnabled


Name            : owa (Default Web Site)
CalendarEnabled : False
```

Explanation:
This command checks the status of the CalendarEnabled property for the specified OWA virtual directory. A value of `False` confirms that Calendar access is now disabled for all users accessing OWA through this endpoint.

Step 6 – List All OWA Mailbox Policies

Action:
Display a list of all OWA mailbox policies configured in the environment.

Command:
```
Get-OwaMailboxPolicy | Format-List Name
```

```
[PS] C:\Users\Administrator>Get-OwaMailboxPolicy | Format-List Name

Name : Default

Name : Sellers on the road
```

Explanation:
This command retrieves all mailbox policies available for Outlook Web App (OWA). Listing the policy names helps confirm that both the default and custom policies—like "Sellers on the road"—exist before assigning them to users.

Step 7 – Create a New OWA Mailbox Policy Called "Basic Policy"

Action:
Add a new policy with default settings.

Command:
```
New-OwaMailboxPolicy -Name "Basic Policy"
```

```
[PS] C:\Users\Administrator>New-OwaMailboxPolicy -Name "Basic Policy"
```

Explanation:
This creates a new Outlook Web App policy object named "Basic Policy". By default, it inherits standard settings that can be customized later. Policies allow admins to restrict or allow specific OWA features per user group.

Step 8 – Confirm the Creation of the Policy

Action:
Verify that the "Basic Policy" has been successfully created.

Command:
```
Get-OwaMailboxPolicy | Format-List Identity
```

```
[PS] C:\Users\Administrator>Get-OwaMailboxPolicy | Format-List Identity

Identity : Default

Identity : Sellers on the road

Identity : Basic Policy
```

Explanation:
This lists the identities (names) of all existing OWA mailbox policies. Its a quick way to visually confirm that "Basic Policy" is present without checking individual properties. This is sufficient for verifying creation as per the lab instructions.

Step 9 – Disable Junk Email Filtering in the "Basic Policy"

Action:
Update the policy to turn off junk email filtering.

Command:
```
Set-OwaMailboxPolicy -Identity "Basic Policy" -JunkEmailEnabled $false
```

```
[PS] C:\Users\Administrator>Set-OwaMailboxPolicy -Identity "Basic Policy" -JunkEmailEnabled $false
[PS] C:\Users\Administrator>
```

Explanation:
Disabling this setting means users under this policy won't be able to access Junk Email filtering via OWA. This might be useful in organizations using third-party email filtering or central mail routing.

Step 10 – Verify That Junk Email Filtering is Now Disabled

Action:
Ensure the setting has been applied correctly.

Command:
```
Get-OwaMailboxPolicy -Identity "Basic Policy" | Format-List JunkEmailEnabled
```

```
[PS] C:\Users\Administrator>Get-OwaMailboxPolicy -Identity "Basic Policy" | Format-List JunkEmailEn
abled


JunkEmailEnabled : False
```

Explanation:
Verifies that JunkEmailEnabled is now set to False. This confirmation is essential to ensure that the configuration change was applied successfully.

Step 11 – Assign the "Basic Policy" to Elon Musk

Action:
Apply the new OWA policy to the specific user mailbox.

Command:
```
Set-CASMailbox -Identity "Elon Musk" -OwaMailboxPolicy "Basic Policy"
```

```
[PS] C:\Users\Administrator>Set-CASMailbox -Identity "Elon Musk" -OwaMailboxPolicy "Basic Policy"
[PS] C:\Users\Administrator>
```

Explanation:
This links the "Basic Policy" to Elon Musk's mailbox. From now on, his OWA experience will follow the permissions and restrictions defined in that policy.

Step 12 – Reassign "Sellers on the road" to Elon Musk for Testing

Action:
Apply the testing policy back to the user.

Command:
```
Set-CASMailbox -Identity "Elon Musk" -OwaMailboxPolicy "Sellers on the road"
```

```
[PS] C:\Users\Administrator>Set-CASMailbox -Identity "Elon Musk" -OwaMailboxPolicy "Sellers on the
road"
[PS] C:\Users\Administrator>
```

Explanation:
Since Part 3 of the lab requires testing features specific to the "Sellers on the road" policy, this command ensures Elon Musk is again **using** the correct policy **for** validation and demonstration.

Step 13 ** Bonus ** – Verify OWA Mailbox Policy Assignment

Action:
Confirm which OWA mailbox policy is currently assigned to the user Elon Musk.

Command:
```
Get-CASMailbox -Identity "Elon Musk" | Format-List OwaMailboxPolicy
```

```
[PS] C:\Users\Administrator>Set-CASMailbox -Identity "Elon Musk" -OwaMailboxPolicy "Basic Policy"
[PS] C:\Users\Administrator>
[PS] C:\Users\Administrator>
[PS] C:\Users\Administrator>Set-CASMailbox -Identity "Elon Musk" -OwaMailboxPolicy "Sellers on the
road"
[PS] C:\Users\Administrator>Get-CASMailbox -Identity "Elon Musk" | Format-List OwaMailboxPolicy
>>


OwaMailboxPolicy : Sellers on the road
```

Explanation:
This command retrieves the current OWA policy applied to the users mailbox. Only one policy can be active at a time. Although the lab had us assign two policies ("Basic Policy" and "Sellers on the road"), the second assignment overwrites the first.

ⓘ Note:
In Exchange, a mailbox can have only **one OWA mailbox policy assigned at a time. The most recent policy applied using `Set-CASMailbox` replaces any previously assigned policy. In this case, **"Sellers on the road"** is the effective policy for Elon Musk, as expected for the final validation step in Part 3.**

```
##############################################################################
Exercise 2 - Part 3: Testing the OWA Policy
Objective: Validate that the "Sellers on the road" OWA policy works as
intended.
##############################################################################
Step 0 - Prepare the Environment for Policy Testing

Action:
Ensure the login page allows Public/Private selection and enable
administrator-level audit logging.

Commands:
Set-OwaVirtualDirectory "owa (Default Web Site)" -
LogonPagePublicPrivateSelectionEnabled $true
```

```
[PS] C:\Users\Administrator>Set-OwaVirtualDirectory "owa (Default Web Site)" -LogonPagePublicPrivat
eSelectionEnabled $true
[PS] C:\Users\Administrator>_
```

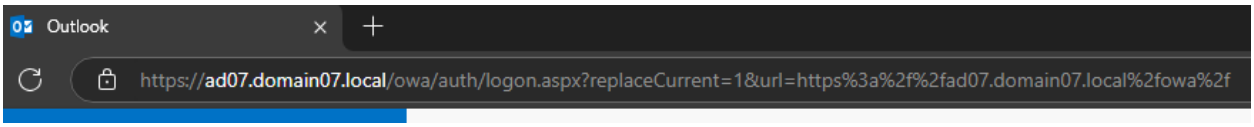
```
Iisreset
```

```
[PS] C:\Users\Administrator>iisreset
```

```
Set-Mailbox -Identity "Elon Musk" -AuditEnabled $true
```

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

```
Explanation:
The first command enables the option for users to select between Public and
Private computer modes on the OWA login screen — required to test policy
behavior under both scenarios.
The second command activates mailbox audit logging for Elon Musk, allowing
admin-side activity tracking.
Session logging must also be enabled manually by the user after login:
→ Navigate to Settings > General > Privacy and Data → Enable Start Logging


Step 1 - Open OWA URL

Action:
Access the Outlook Web App from a client workstation.

Navigation:
Windows Client VM, open a browser and enter:
https://ad07.domain07.local/owa
```

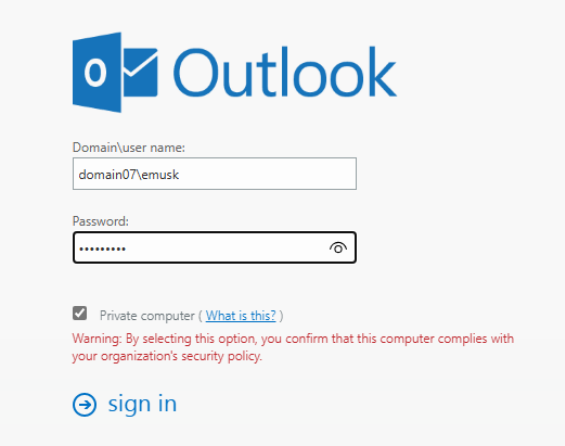



```
Explanation:
This URL opens the OWA login portal used to test the policy in a live
session.
```

Step 2 – Log in as Elon Musk

Action:
Authenticate using the test account.

Navigation:
Enter the following credentials:
Username: domain07\emusk
Password: [Lab Password]

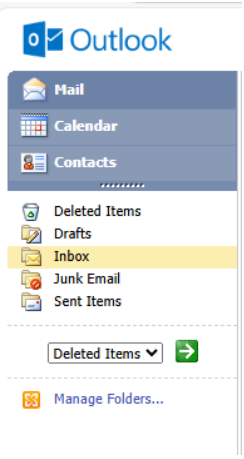


Explanation:
This account is assigned the "Sellers on the road" OWA mailbox policy and will be used to test its effects during the session.

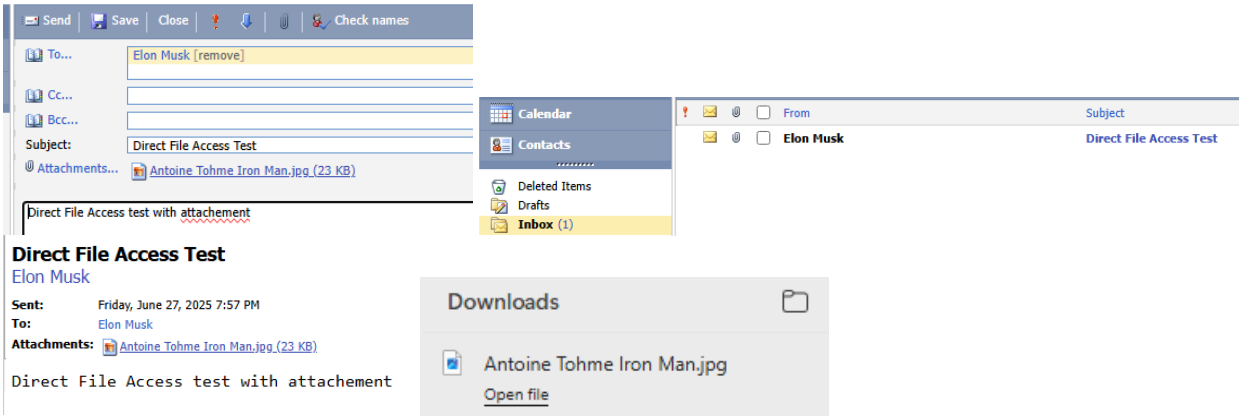
Step 3 – Verify Policy Features in OWA

Action:
Confirm that only the intended features are accessible.

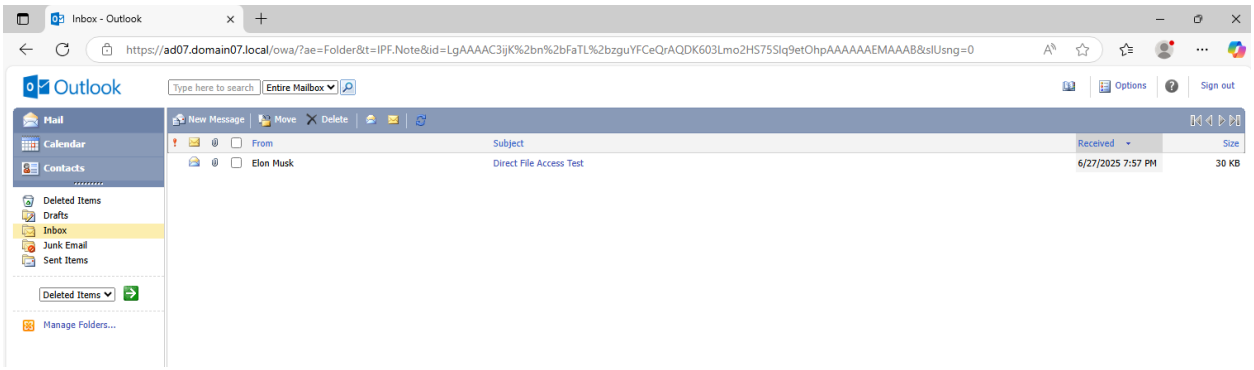
Checklist & Validation:
✓ Calendar, Contacts, and Tasks are accessible
→ Use the left-side app menu to confirm visibility and access.
→ **Note:** If *Tasks* is not visible, this may be due to OWA operating in **Light mode**. You can verify this in Step 4.



✓ Direct file access works in current session mode
→ Try uploading/downloading attachments in a test email.



✓ Restricted features like Journal, Themes, and file previews are hidden
→ Explore the interface and settings; these should be absent.



→ **Observe the OWA interface:**
- No Journal or Notes folders present in the left pane.
- No gear icon (⚙) at top-right for accessing personalization settings such as themes.
- Minimalistic UI confirms that advanced features are unavailable.

✓ Logging is enabled
→ Admin-side check:
`Get-Mailbox -Identity "Elon Musk" | Format-List AuditEnabled`
Expected result: AuditEnabled : True

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

AuditEnabled : True
```

→ Optionally view logs:
`Search-MailboxAuditLog -Identity "Elon Musk" -ShowDetails -LogonTypes Owner, delegate, Admin`

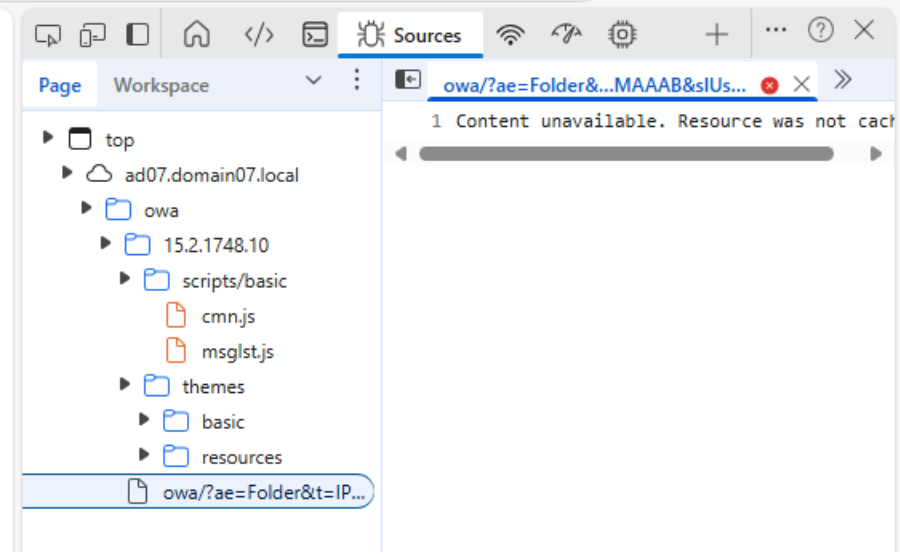
→ User-side check (manual session logging):
Click Settings > General > Privacy and Data → Confirm Start Logging is enabled or toggle it on manually.

Explanation:
This step confirms that the mailbox policy is applied correctly and controls the interface as expected based on allowed/disallowed features.

Step 4 – Confirm OWA Light Version Is Not Enforced

Action:
Check that the full-featured OWA interface is active.

Navigation:
While logged in, press F12 to open Developer Tools.
Inspect page source or confirm rich UI elements are present (e.g., side panel, icons, full layout).



Explanation:
This image shows the browser's **Developer Tools opened to the **Sources** tab. The highlighted directories (`themes`, `scripts/basic`) under the OWA path on the Exchange server (`ad07.domain07.local`) confirm that only the essential client-side scripts and themes are loaded.**

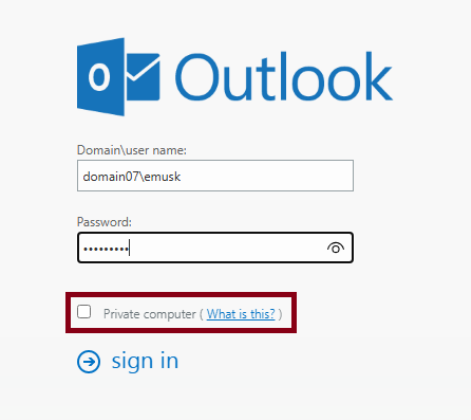
What's *missing*:
• No journal scripts or dynamic theme previews loaded.
• No additional JavaScript features for customizing UI appearance (which confirms `themes` are restricted by policy).

This confirms that **restricted UI features are blocked, and the applied OWA mailbox policy is working correctly.**

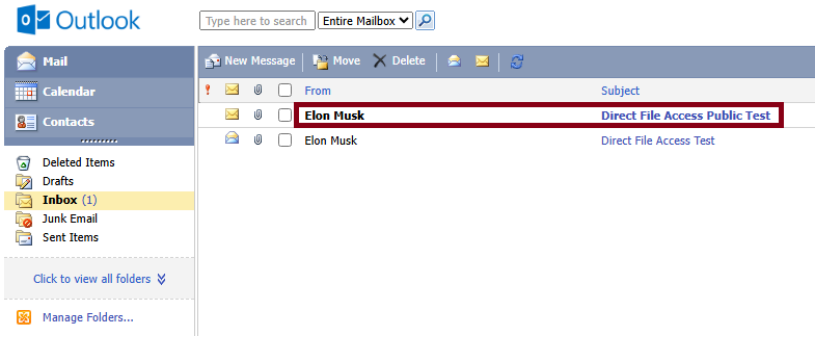
Step 5 – Re-test Access from Public Computer Mode

Action:
Verify feature access consistency in Public mode.

Navigation:
1. Log out from the current session.
2. On the login screen, select This is a public computer.
3. Log back in using Elon Musk credentials.



Checklist:
✓ Calendar, Contacts, and Tasks are still accessible
✓ Direct file access remains functional
✓ Restricted features are still hidden



Direct File Access Public Test
Elon Musk

Sent: Friday, June 27, 2025 8:25 PM
To: Elon Musk
Attachments: Antoine Tohme Iron Man.jpg (23 KB)

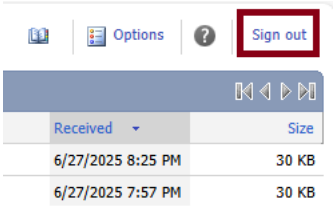
Public computer File access

Explanation:
This test validates that the OWA policy works identically across public/private modes as configured.

Step 6 – Log Out of OWA

Action:
Securely log out of the Outlook Web App (OWA) session.

Navigation:
Click on the profile icon (top-right corner) → Click on **Sign out**



Explanation:
Properly signing out ensures the session is closed securely and the mailbox audit policy test is completed cleanly for the user **Elon Musk**. This step is critical for ensuring that access logs are correctly written and no session caching interferes with the audit results.