

## 1. What is Microsoft 365?

- ✓ Microsoft 365 is an integrated experience of apps and services with the latest features and security updates.
- ✓ This is the web-based version of Microsoft office suite which provides a bundle of features and apps to make smooth daily office work.
- ✓ Products & Services available –
  - Office Pro Plus
  - Windows 10
  - Enterprise Mobility + Security

## 2. How to sign up for Microsoft 365 trial tenant?

Here I select Microsoft 365 Enterprise E3 trial tenant.

1. First, we need to go - <https://signup.microsoft.com/create-account/signup?OfferId=B07A1127-DE83-4a6d-9F85-2C104BDAE8B4&dl=ENTERPRISEPACK&ali=1&products=cfq7ttc0k59j:0009>
2. Then fill up all information, verify the phone number, choose suitable domain and username and login to admin panel.

## 3. Is there any other way to register a trial tenant?

- ✓ Please go to – [www.microsoft.365](http://www.microsoft.365)
- ✓ Choose any option –
  - For Home
  - For Business
  - For Enterprise
- ✓ Click **See Plan & Pricing**
- ✓ Choose your desired License according to your needs
- ✓ Click **Try for 1 month**

## 4. How many types of services are offered in Microsoft 365?

There are basically 3-types of products/services offered in Microsoft 365. These are –

- a. Windows 10
- b. Enterprise Mobility + Security (EMS)
- c. Office Pro Plus
  - I. Office (Word, Excel, PowerPoint, Access, OneNote)
  - II. Files & Content (**OneDrive**, Stream, Sway)
  - III. Task Management (Power Apps, Power Automate, Planner, To Do)
  - IV. Workflows (Forms, Flow. Powerapps)
  - V. Social (**SharePoint**, Yammer)

- VI. Email (**Exchange Online**, Outlook)
- VII. Advanced Analytics (MyAnalytics, Power BI Pro)
- VIII. Meeting & Voice (Teams, **Skype Business**)

**5. What is the difference between Microsoft 365 and Traditional Microsoft Office?**

Traditional Microsoft Office	Microsoft 365
Less Benefits	More Benefits
One-time purchase	Subscription Based (Monthly/Annually)
Costly	Cost-effective solution
Need to buy products/services individually	Huge range of products/services under a single subscription
Not cloud-based but possible to share	Fully cloud-based
Not to contact always	Call to support center directly
Can meet individual purpose/goal	Can meet organizational purpose/goal from a single tenant

**6. For how long account/data is kept after the license gets expired?**

Stages of Subscription	Description
1. Active	<ul style="list-style-type: none"> <li>✓ Data is safe and accessible (both admin &amp; user)</li> <li>✓ Have to pay regular subscription fee</li> </ul>
2. Expired	<ul style="list-style-type: none"> <li>✓ Have normal access for both admin &amp; user</li> <li>✓ Data is accessible</li> <li>✓ Maximum timeline 30 days</li> </ul>
3. Disabled	<ul style="list-style-type: none"> <li>✓ Data is accessible only for admin</li> <li>✓ Admin can't assign license</li> <li>✓ Maximum timeline 90 days</li> </ul>
4. Deprovisioned	<ul style="list-style-type: none"> <li>✓ Ultimate stage</li> <li>✓ Data is deleted</li> <li>✓ Azure AD is removed</li> <li>✓ Can't be accessible again even if buyer would like to pay again</li> </ul>

## 7. What is the difference between Tenant, Subscription and Licenses?

Tenant	Subscription	License
✓ House/container for items or features of any organization like users, domain,.	✓ whereas subscription is like a package	✓ where every subscription has some licenses. License is a monthly per-user subscription.

When a user buys a subscription he specifies the number of licenses that he needs based on how many people he has in his organization. After buying the subscription he can create the accounts for people of his organization, and then assign a license for each person. As per the change of organizational need a user can buy more licenses to accommodate new people or reassign the license to others when someone leaves the organization.

## 8. Name the types of Licenses in Microsoft 365

Business	Basic	\$ 5.00 / Monthly	
	Standard	\$ 12.5.00 / Monthly	
	Premium	\$ 20.00 / Monthly	
Enterprise	E3	\$ 32.00 / Monthly	
	E5	\$ 57.00 / Monthly	Extra Security Features
	F3	\$ 10.00 / Monthly	Only for mobile apps

## 9. How many channels are there to purchase Microsoft 365? Explain the differences?

Channels	Description
✓ <a href="http://www.microsoft365.com">www.microsoft365.com</a> ✓ <a href="http://www.office365.com">www.office365.com</a>	✓ From Microsoft webpage ✓ Need global credit card
✓ Partner/Reseller	✓ purchase from the people who are directly working with Microsoft

# W-1, D-2

1. WHAT IS DNS AND DNS HOSTING PROVIDER? WHAT IS NAMESERVER?

<b>DNS</b>	<ul style="list-style-type: none"><li>• Phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses.</li><li>• DNS translates domain names to IP addresses so browsers can load Internet resources.</li><li>• DNS is very important and adding an enigmatic dot (ex. www.facebook.com.) at the end of domain name by adding memory cache.</li><li>• Operating System will ask Resolving Name Server (RNS) to find the domain to get the root, then RNS sends all to TLD and TLD to Authoritative Name Server (ANS) to find the actual IP for this domain.</li></ul>
<b>DNS Hosting Provider</b>	<ul style="list-style-type: none"><li>• DNS hosting is a type of network service that provides domain name system resolution services.</li><li>• It builds, operates and provisions domain name servers, which are used and integrated with domain name registrars, Web hosting services and Internet service providers (ISP).</li><li>• Host companies and Internet Service Providers interact with the Central Registry on a regular schedule to get updated DNS information.</li></ul>
<b>Nameserver</b>	<ul style="list-style-type: none"><li>• Handling queries regarding the location of a domain name's various services.</li><li>• Fundamental part of the Domain Name System (DNS).</li><li>• Allow using domains instead of IP addresses.</li><li>• Help web browsers and another services access in the domain's DNS records.</li></ul>

# W-1, D-2

## 2. WHAT IS DOMAIN? WHAT IS TXT, MX, SRV, SPF, A AND CNAME RECORDS?

<b>Domain</b>	<ul style="list-style-type: none"><li>• A domain name is an identification string that defines a realm of administrative autonomy, authority or control within the Internet.</li><li>• It represents an Internet Protocol (IP) resource, such as a personal computer used to access the Internet, a server computer hosting a web site, or the web site itself or any other service communicated via the Internet.</li><li>• Domain names are formed by the rules and procedures of the Domain Name System (DNS). Any name registered in the DNS is a domain name.</li><li>• Domain names are organized in subordinate levels (subdomains) of the DNS root domain, which is nameless. The first-level set of domain names are the top-level domains (TLDs), including the generic top-level domains (gTLDs), such as the prominent domains com, info, net, edu, and org, and the country code top-level domains (ccTLDs).</li></ul>
<b>DNS Records</b>	
<b>TXT</b>	<ul style="list-style-type: none"><li>• This can be edited to include any additional information about the domain that isn't currently listed.</li><li>• These records aren't used to direct any traffic. Instead they're used to provide needed information to outside sources.</li><li>• Used to verify the domain (recommended).</li></ul>
<b>MX</b>	<ul style="list-style-type: none"><li>• This refers to any mail servers that might be used in accordance with your domain.</li></ul>
<b>SRV</b>	<ul style="list-style-type: none"><li>• SRV (Service) record points one domain to another domain name using a specific destination port.</li><li>• Allow specific services, such as VOIP or IM, to be directed to a separate location.</li></ul>
<b>SPF</b>	<ul style="list-style-type: none"><li>• A powerful email authentication method.</li><li>• SPF (Sender Policy Framework) are used by many email systems to help identify if email is coming from a trusted source.</li><li>• Helping filter out spam or messages pretending to be from your domain (called spoofing).</li></ul>

## W-1, D-2

<b>A</b>	<ul style="list-style-type: none"><li>• A record (Address Record) refers to the actual IP address that's associated with the Domain.</li><li>• It points a domain or subdomain to an IP address. For example, you can use it for store.website.com or blog.website.com and point it to where you have your store.</li><li>• As an example, an A Record is used to point a logical domain name, such as "google.com", to the IP address of Google's hosting server, "74.125.224.147".</li></ul>
<b>CNAME</b>	<ul style="list-style-type: none"><li>• A CNAME (Canonical Name) points one domain or subdomain to another domain name.</li><li>• Allow to update one record each time, regardless of how many Host Records need to resolve to that IP address.</li><li>• These records point www.example.com to example.com, imap.example.com to mail.example.com, and docs.example.com to ghs.google.com.</li><li>• The first record allows the domain to resolve to the same server with or without the www subdomain.</li><li>• The second record allows you to use an alternative subdomain for email hosting and delivery.</li></ul>

### 3. REGISTER NEW DOMAIN (FREE OR PAID).

<ul style="list-style-type: none"><li>• Please <a href="#">click here</a></li></ul>
<ul style="list-style-type: none"><li>• Please go to -<a href="#">Services &gt; Register a New Domain</a></li></ul>
<ul style="list-style-type: none"><li>• Please write down the desired domain &amp; check availability.</li></ul>
<ul style="list-style-type: none"><li>• If the domain is available, you will see in the next page and choose any of the free domains.</li></ul>
<ul style="list-style-type: none"><li>• Please go to -</li><li>• <a href="#">Get in Now</a> &gt; then select the domain and click <a href="#">Checkout</a></li></ul>
<ul style="list-style-type: none"><li>• Please choose the best option for you - (12 Months @ free) and click <a href="#">Continue</a>.</li></ul>

## W-1, D-2

- |                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>You will see that there is no charge for this domain and you can choose your email/google/facebook to sign up here.</li></ul>                        |
| <ul style="list-style-type: none"><li>Whatever you select, they will send you the verification email.</li></ul>                                                                            |
| <ul style="list-style-type: none"><li>Please check the email and click the link in the email to get this form. Please fill up details carefully and click <b>Complete Order</b>.</li></ul> |
| <ul style="list-style-type: none"><li>Sign in to your account and please go to -<br/><b>Services &gt; My Domains</b></li></ul> <p>Enjoy your Free Domain for 12 Months fully free</p>      |

### 4. HOW TO CHECK WHERE DOMAIN IS HOSTED?

There are several ways to check where the domain is hosted. But the best way to use WHOIS Lookup page provided by ICANN, a non-profit organization that compiles domain information. Another way is to go directly to [www.whois.net](http://www.whois.net) and search the desired domain for details. All the processes to check where domain is hosted given below:

- |                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>Please go to <a href="https://www.lookup.icann.org">https://www.lookup.icann.org</a></li></ul>                                                                               |
| <ul style="list-style-type: none"><li>Please enter the dejsired website</li></ul>                                                                                                                                  |
| <ul style="list-style-type: none"><li>Please scroll down to check the details of the page including the location &amp; contacts. There are a lot of information available related to the website domain.</li></ul> |

### 5. WHY DO WE NEED TO ADD A COMPANY DOMAIN?

<b>Brand</b>	It creates brand value of the company and customer can easily rely on this particular company.
<b>Verified Email</b>	If a company has a specific domain, they can create verified email for the employees and it ensures that the employee only get the email from the company. For example, a university has their own website and the associated faculty members have their email related to the University domain. Any students around the world would easily

## W-1, D-2

	recognize the faculty members by looking his email account, which can really be helpful for the students/teachers.
<b>Walk-in Business</b>	If you decide to register a domain name that matches the concept of your business, you might draw Web surfers in search of that topic. For instance, a dropshipping store that registered <a href="http://www.shadmart.com">www.shadmart.com</a> might get visitors looking for dropshipping in their own country.
<b>Easy to Remember</b>	It is easy to remember the company name through domain name.
<b>SEO</b>	This allows a company to boost their business around the world and eventually, those who are interested with company's product/services can contact with them. If any customer search in bing/google/yahoo, they will get the company profile, which may help the customer for taking decision whether they will take the products/service from that particular company or not.

### 6. ADDING A DOMAIN TO THE TRIAL TENANT.

Steps for adding a domain -

- Adding a domain
- Verify a domain
- Choose Online Services
- Update DNS Records

- Please go to -  
<https://admin.microsoft.com>

Please go to -  
*Settings > Domains*

- Please go to - *Add domain*

- Please input the domain which you created earlier from [www.freenom.com](http://www.freenom.com)

- You will find two options here to verify the domain -



## W-1, D-2

*TXT Record*

*MX Record*

*TXT Record is recommended because if you have done any mistake in the process it will not hamper other services such as Exchange Online, SharePoint etc.*

*You will see there a TXT value. Please copy the value and go to DNS hosting management.*

- Please go to the DNS hosting Provider. Here it is freenom recommended by Microsoft for free domain.*

*Please go to -*

*[Services > My Domains > Manage Domains](#)*

- Please go to -*

*[Manage Freenom DNS](#)*

- Copy the TXT Records in the paste here and click [Save Changes](#).*

- Please wait 10-15 minutes after adding the TXT records in the DNS management and then please go to -*

*[Verify > Continue in the next page](#)*

- Now you will see MX, CNAME, SPF Records.*

- Please add MX, CNAME, SPF Records in the manage freenom DNS and click [Save Changes](#).*

- Please wait 10-15 minutes and click Continue in the Microsoft Admin Center Domain Add Stage. Domain is added successfully.*

### 7. WHAT IS MX RECORD OF A DOMAIN? HOW TO CHECK MX, SPF RECORDS FOR DOMAIN?

An MX-record is a type of resource record in the Domain Name System (DNS). This is the system that, among other indicates to what specific IP address emails need to be sent. The

## W-1, D-2

MX-record contains the host name of the computer(s) that handle the emails for a domain and a prioritization code.

### Through Command Prompt (MX Records)

- Please open a command prompt.
- Please type "**nslookup**" then press Enter.
- Please Type "**set q=mx**" then press Enter to get the MX value.
- Please type any domain name that you want to know the MX value. You will see the details there.

### Through Command Prompt (SPF Records)

- Please Type -  
"**nslookup -type=txt**" a space, and then the domain/host name. e.g. "**nslookup -type=txt facebook.com**"

8. WHAT SERVICES CAN BE ASSIGNED DURING DOMAIN VERIFICATION PROCESS?

- Exchange online
- Skype for business
- MDM-mobile device management for office 365

9. HOW TO REMOVE A DOMAIN? IF THERE ARE NO ACTIVE USERS AND GROUPS USING THIS DOMAIN AND THE DOMAIN CAN STILL NOT BE REMOVED, WHAT ELSE YOU NEED TO CHECK?

### Remove a Domain

Please go to -

[Settings > Domains](#)

## W-1, D-2

Select the Domain and Click -

*Remove Domain*

*If there are no dependencies it will be deleted.*

**Remove a Domain with Dependencies even if there are no active users and groups using this domain**

- If the domain is set as default it will not be deleted.
- Users, Groups & Resources need to be removed manually before deleted

10. HOW MANY DOMAINS CAN BE ADDED IN MICROSOFT 365 TENANT? IS IT POSSIBLE TO ADD A DOMAIN IN MICROSOFT 365, IF IT IS ALREADY ADDED TO ANOTHER SERVICE PROVIDER?

<b>Maximum Domain in Microsoft 365</b>	<ul style="list-style-type: none"><li>• 900 domains in a single subscription.</li></ul>
<b>Add a Domain if it is already added to another service provider</b>	<ul style="list-style-type: none"><li>• It is not possible.</li><li>• If we want to add in the tenant then we must delete from the previous tenant</li></ul>

11. HOW TO FIND URLS AND IPs USED BY THE MICROSOFT 365? WHAT ARE THEY USED FOR?

<b>Steps</b>	<b>Flow Process</b>
<ul style="list-style-type: none"><li>• Please <a href="#">click here</a> and scroll down to check the URLs &amp; IPs used by Microsoft 365</li></ul>	
<ul style="list-style-type: none"><li>• Please scroll down to the page and check URLs &amp; IPs for the specific Microsoft 365 Services. Here, it is Exchange Online</li></ul>	

**Necessity of the URLs & IPs:** If sometimes the link mentioned in the green boxes are not working then we can tell ISP to allow all the IPs related to that link and from the next time the desired link will work. It is necessary for proper functioning of exchange online. Thus, these IPs are crucial to troubleshoot the exchange online problem.

## W-1, D-2

### 12. IF I PUT WRONG MX RECORDS, WHAT WILL HAPPEN?

The mail will not be sent. We will see the error after sending the email.

### 13. WHY DO WE RECOMMEND TXT RECORDS TO VERIFY THE DOMAIN RATHER THAN CHOOSING MX RECORDS?

If we make any mistake during txt records entry, it will not affect other services such as Exchange Online. As MX records is used for Exchange Online, if we choose MX records to verify the domain and make a mistake then we can't send email through this domain.

### 14. WHAT ARE THE THINGS WE NEED TO CONSIDER DURING MX RECORDS CHECKUP?

MS Preference -

- ✓ If the value is lower, that mail exchange server will get the highest priority but if there is any problem of sending/receiving any email using that server, then this will try to the next lowest valued MX preference mail exchange server.
- ✓ For example, there are 3 mail exchange servers (MX preference 10, 20, 30) for a specific domain. At first, it will try value 10 mail exchange server and if not working then 20, accordingly 30.

### 15. IS THERE ANY OTHER WAY TO CHECK DNS RECORDS EXCEPT CMD?

- ✓ [www.mxtoolbox.com](http://www.mxtoolbox.com)
- ✓ Put Domain name > choose MX lookup/TXT > check details.

### 16. HOW CAN I CHECK THE SPF VERSION AND WHY IT IS TXT RECORDS?

- ✓ Suppose "v=spf1 redirect=\_spf.facebook.com" is the facebook's spf records.
- ✓ This is 1<sup>st</sup> version - means only one spf records available.
- ✓ SPF is itself a txt record.

# W-1 D-3

## 1. HOW TO USE POWERSHELL TO CONNECT TO MICROSOFT 365?

1. Please Search "PowerShell" in the Windows Search and Run as Administrator.

2. Please type -

**"\$Cred = Get-Credential"** and press **Enter** and you will see the Credential Box for information. Please enter the username and password.

3. Please type -

**"Set-ExecutionPolicy RemoteSigned"** and press **Enter** and when you will see a request please type **"A"** and press **Enter** again.

[N.B. Once you connected you do not need to type this command again]

4. Please type -

**"Install-Module MSOnline"** and press **Enter**. Type **"Y"** and then type **"A"** and press **Enter**.

[N.B. Once you connected you do not need to type this command again]

**"Import-Module MSOnline"** and press **Enter**. Type **"Y"** and then type **"A"** and press **Enter**.

**"Connect-MSOLService"** and press **Enter**. You will see sign in option.

5. Please provide your username and password again to connect Microsoft 365 Admin Center.

Then Please type -

**"Get-Msoluser"** and press **Enter** to check whether the connection is working perfectly. If the PowerShell is connected you will see the Active User list below.

# W-1 D-3

## 2. COMMON POWERSHELL COMMANDS.

<i>Reference</i>	<a href="https://docs.microsoft.com/en-us/powershell/module/msonline/?view=azureadps-1.0">https://docs.microsoft.com/en-us/powershell/module/msonline/?view=azureadps-1.0</a>
<i>Common For</i>	Microsoft 365 PowerShell V 1.0
<b>Add-MsolAdministrativeUnitMember</b>	Adds a member to an administrative unit.
<b>Add-MsolForeignGroupToRole</b>	Adds a security group from a partner tenant to a Role in this tenant.
<b>Add-MsolGroupMember</b>	Adds a member to an existing security group.
<b>Add-MsolRoleMember</b>	Adds a member to an administrator role.
<b>Add-MsolScopedRoleMember</b>	Adds a member to an administrative unit-scoped role.
<b>Confirm-MsolDomain</b>	Verifies a custom domain.
<b>Confirm-MsolEmailVerifiedDomain</b>	Confirms ownership of an unmanaged tenant.
<b>Connect-MsolService</b>	Initiates a connection to Azure Active Directory.
<b>Convert-MsolDomainToFederated</b>	Converts the domain from using standard authentication to using single sign-on.
<b>Convert-MsolDomainToStandard</b>	Converts the domain from using single sign-on (also known as identity federation) to using standard authentication.
<b>Convert-MsolFederatedUser</b>	Updates a user in a domain that was recently converted from single sign-on.
<b>Disable-MsolDevice</b>	Disables a device object in Azure Active Directory.
<b>Enable-MsolDevice</b>	Enables a device object in Azure Active Directory.
<b>Get-MsolAccountSku</b>	Returns all the SKUs for a company.
<b>Get-MsolAdministrativeUnit</b>	Retrieves administrative units from Azure AD.
<b>Get-MsolAdministrativeUnitMember</b>	Gets members of an administrative unit.
<b>Get-MsolAllSettingTemplate</b>	Gets all the directory setting templates that a tenant owns.
<b>Get-MsolAllSettings</b>	Gets all directory settings object associated with tenant or group/user/service principal/application/device.
<b>Get-MsolCompanyAllowedDataLocation</b>	Get the current allowed data locations of a company from Azure Active Directory.
<b>Get-MsolCompanyInformation</b>	Retrieves company-level information.
<b>Get-MsolContact</b>	Gets contacts from Azure Active Directory.
<b>Get-MsolDevice</b>	Gets an individual device, or a list of devices.
<b>Get-MsolDeviceRegistrationServicePolicy</b>	Gets the Azure Active Directory device registration service settings.
<b>Get-MsolDirSyncConfiguration</b>	Gets the directory synchronization settings.
<b>Get-MsolDirSyncFeatures</b>	Gets the status of identity synchronization features for a tenant.

## W-1 D-3

### 3. HOW TO VERIFY IF YOU ARE CONNECTED TO MICROSOFT 365 USING POWERSHELL?

*When PowerShell is connected to Microsoft 365, we need to check any of the normal commands of PowerShell to verify the connection.*

*To Do that Please type -*

***"Get-Msoluser"** and press Enter to check whether the connection is working perfectly. If the PowerShell is connected you will see the Active User list below.*

*[N.B. This command is used to get the list of the User in the tenant]*

### 4. EXPLAIN THE DIFFERENCE BETWEEN MICROSOFT 365 POWERSHELL AND AZURE AD POWERSHELL?

Microsoft 365 PowerShell	Azure AD PowerShell
1. The MSOnline Module, with its *-MSOL* cmdlets, was the first Windows PowerShell Module for Azure Active Directory.	1. Its full name is Azure Active Directory PowerShell for Graph.
2. Less Functionalities	2. More Functionalities than Microsoft 365 PowerShell
3. Microsoft refers to this module as version 1.0. MSOnline is the old module, which can still provide functionality that is not yet available in the AzureAD module.	3. Microsoft refers to this module as version 2.0.
4. MSOnline module will be deprecated when all of the functionality has been migrated to the newer module called AzureAD.	4. The AzureAD module, and its dependencies, can be installed and updated using PowerShellGet from the PowerShell Gallery.
5. PowerShell Commands - <b>Install-Module MSOnline</b> <b>Import-Module MSOnline</b>	5. PowerShell Commands - <b>Install-Module AzureAD</b> <b>Import-Module AzureAD</b>

## W-1 D-3

### 5. HOW TO CONNECT TO EXCHANGE ONLINE USING POWERSHELL?

Connect to Exchange Online PowerShell with Basic Authentication	
Reference	<a href="https://docs.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps">https://docs.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps</a>
Steps	Flow Process
1. Please type - <b>"Set-ExecutionPolicy RemoteSigned"</b>	
2. Please type - <b>"\$UserCredential = Get-Credential"</b>	
3. Please type Session command - <b>"\$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential \$UserCredential -Authentication Basic -AllowRedirection"</b>	
4. Please type - <b>"Import-PSSession \$Session -DisableNameChecking"</b>	
5. To check the Connection, please type - <b>"Get-Mailbox"</b> and press <b>Enter</b> and there will be a list of mailboxes available in the tenant. If there is no error, Exchange Online is connected successfully.	

Exchange Online PowerShell with Modern Authentication using V2 module	
Reference	<a href="https://docs.microsoft.com/en-us/powershell/exchange/exchange-online-powershell-v2?view=exchange-ps">https://docs.microsoft.com/en-us/powershell/exchange/exchange-online-powershell-v2?view=exchange-ps</a>
<p>Please type -</p> <p><b>"Install-PackageProvider -Name NuGet -Force"</b> and press <b>Enter</b>.</p> <p>Please type -</p> <p><b>"Install-Module -Name PowerShellGet -Force"</b> and press <b>Enter</b>.</p> <p>Please type -</p> <p><b>"Update-Module -Name PowerShellGet"</b> and press <b>Enter</b>.</p> <p>It will update <b>NuGet</b> and <b>PowerShellGet</b></p>	



## W-1 D-3

1. Please type -

**"Set-ExecutionPolicy RemoteSigned"** and press **Enter**.

2. Please type -

**"Install-Module -Name ExchangeOnlineManagement"** and press **Enter**.

3. Please type -

**"Update-Module -Name ExchangeOnlineManagement"** and press **Enter**.

4. AS I have MFA enabled Account -

Please type -

**"Connect-ExchangeOnline -UserPrincipalName <UPN> -ShowProgress \$true"** and press **Enter**. You will see a dialogue box where enter the username and

[N.B. Here <UPN> is your tenant account. Please write down your tenant account]

N.B. If it isn't MFA enabled account then please use these 2 commands -

**"\$UserCredential = Get-Credential"**

**"Connect-ExchangeOnline -Credential \$UserCredential -ShowProgress \$true"**

5. Connection check -

**"Get-EXOMailbox"** and press **Enter**. You will see a list of mailboxes created in the exchange online. It means that you are connected successfully.

## W-1 D-3

### 6. HOW TO VERIFY IF YOU ARE CONNECTED TO EXCHANGE ONLINE SUCCESSFULLY OR NOT?

- Please refer to this answer in the Question-5 last portion.
- Connect to Exchange Online PowerShell with Basic Authentication -
  - ✓ Please type - "**Get-Mailbox**" and press Enter and there will be a list of mailboxes available in the tenant. If there is no error, Exchange Online is connected successfully.
- Use the Exchange Online PowerShell with Modern Authentication using V2 module -
  - ✓ Please type "**Get-EXOMailbox**" and press Enter. You will see a list of mailboxes created in the exchange online. It means that you are connected successfully.

### 7. WHY DO WE NEED TO VERIFY THE CONNECTION OF MS 365 AND AZURE AD POWERSHELL?

- ✓ Check the connection working perfectly.
- ✓ Once PowerShell is connected, it is possible to run all the commands that are available.

### 8. WHY DO YOU NEED POWERSHELL?

- ✓ Reveal additional information that you cannot see with the Microsoft 365 admin center
- ✓ Configure features and settings only possible with Office 365 PowerShell
- ✓ Perform bulk operations
- ✓ Filtering data
- ✓ Print or save data
- ✓ Manage across services

### 9. WHO CAN HAVE ACCESS POWERSHELL CONNECTION?

- Only Admin
- Suppose, Exchange Admin can have access only in Exchange Online. Global Admin has all admin access.
- User can't have access in PowerShell connection

## W-1 D-3

### 10. EXPLAIN THE SESSION COMMAND OF THE EXCHANGE ONLINE CONNECTION.

✓ `$Session = New-PSSession`

`-ConfigurationName` Microsoft.Exchange [N.B. Exchange Online connection]

`-ConnectionUri` <https://outlook.office365.com/powershell-liveid/>  
[N.B. URL link for the connection]

`-Credential` \$UserCredential [N.B. take the user credential from the first command]

`-Authentication` Basic [N.B. this command is for basic authentication method. There is another method of V-2.0 using Exchange Online Management]

`-AllowRedirection` [N.B. it will allow redirecting to the link above]

✓ There are 5 positional parameters available in the command, e.g. - ConfigurationName

### 11. IF I DON'T FIND DOMAIN IN SETTINGS, WHAT WILL I DO?

✓ There is another navigation – Admin Center > Setup > Domain

### 12. WHAT IS REQUIRED FOR EXCHANGE ONLINE CONNECTION?

✓ .NET Framework

✓ Windows Remote Management (winrm)

✓ Download framework from office.com

## W-1, D-4

### 1. How to create users in Microsoft 365?

Steps
<p>1. Please go – <a href="https://admin.microsoft.com">admin.microsoft.com</a></p> <p>2. Then go to – <b>Users &gt; Active users &gt; Add a user</b></p>
<p>3. Set up the Basic -</p> <p><b>Display Name</b> and <b>Username</b> are must to create a user. After filling up all info click <b>Next</b></p> <p>[N.B. Here Auto-generate password is chosen and user need to change the password during first time sign-in process]</p>
<p>4. Assign Product License-</p> <p>Here you need to assign product License for the User. It is possible to create an unlicensed user by choosing the 2<sup>nd</sup> option.</p> <p>5. If required you need to fill up the Profile Info given below of that page, which is not mandatory.</p>
<p>6. Roles –</p> <p>You can provide roles here as <b>User</b> or <b>Admin</b>. If you choose admin, you have to select the admin access type from below. Click <b>Next</b>.</p>
<p>7. You will get user credential in the next page.</p> <ul style="list-style-type: none"><li>• <b>Display name</b></li><li>• <b>Username</b></li><li>• <b>Password</b></li></ul>

## W-1, D-4

### 2. HOW TO CREATE BULK USERS?

Steps
1. Please go – <a href="https://admin.microsoft.com">admin.microsoft.com</a>
2. Then go to – <b>Users &gt; Active users &gt; Add multiple users</b>
3. Please download a CSV file with header and sample user information.
4. Fill up and change accordingly.
5. <b>Browse</b> and <b>Upload</b> the file.
6. <b>Verify</b> the file and click <b>Next</b>
7. Select <b>Sign-in allowed</b>
8. Select the <b>License</b>
9. Click <b>Next</b>
10. <b>Download results</b> to see the user credential.
11. If you want to get results to your email, you may select the checkbox and type the desired email.
12. Click <b>Close without sending</b>

### 3. How to assign the license to the user?

Steps
1. Please go – <a href="https://admin.microsoft.com">admin.microsoft.com</a>
2. Then go to – <b>Users &gt; Active users &gt; Select</b> the User whom you want to assign the License
3. Please go to -  <b>Licenses and Apps &gt; Select</b> the Licenses that are available to the tenant > <b>Save changes</b>
4. The changes have been saved.
5. Please Go Back and a License is assigned already under the user

## W-1, D-4

### 4. How to create single-user & bulk user with PowerShell?

#### Creating Single User using PowerShell

1. Please open Windows PowerShell as Administrator and connect PowerShell to MS 365
2. Please type – **Get-MsolAccountSku** and press **Enter** to get the License Assignment for the next command.
3. Please type – **New-MsolUser -DisplayName "type name" -FirstName "type first name" -LastName "type last name" -UserPrincipalName <UPN> -UsageLocation US -LicenseAssignment <type license type>**  
  
[N.B. you need to type display name, first name, last name, UPN as user email address using your domain and at last type the license.]
4. To check the user, please type “**Get-Msoluser**” and **Enter**. You will see the user is added to your tenant.

#### Creating Bulk User Using Powershell

1. At first, we have to create a CSV file using the heading of –
  - **DisplayName**
  - **FirstName**
  - **LastName**
  - **Display Name**
  - **User Principal Name**
  - **UsageLocation**
  - **AccountSkuld**
2. Please open Windows PowerShell as Administrator and connect PowerShell to MS 365
3. Please type – **Import-Csv -Path "input\_path\_name" | foreach {New-MsolUser -DisplayName \$\_.DisplayName -FirstName \$\_.FirstName -LastName \$\_.LastName -UserPrincipalName \$\_.UserPrincipalName -UsageLocation \$\_.UsageLocation -LicenseAssignment \$\_.AccountSkuld} | Export-Csv -Path "output\_path\_name"**
4. To check the user, please type “**Get-Msoluser**” and **Enter**. You will see the users are added to your tenant.
5. Please check the output CSV file to check the **username** and **password** of the new users.

## W-1, D-4

5. Besides using excel to create a CSV file, are there any other ways to do it?

### Creating Single User using PowerShell

1. Please open **Notepad** from Windows Start Menu.
2. Please type – **User Name, First Name, Last Name, Display Name, Job Title, Department, Office Number, Office Phone, Mobile Phone, Fax, Address, City, State or Province, ZIP or Postal Code, Country or Region**. This is the heading line.
3. Press **Enter** and type the information for the first user in chronological sequence as same as the heading sequence such as first type User Name, then First Name and so on. Please remember that every value should be separated by comma (,).
4. You may add the unlimited number of lines for unlimited users.
5. **Save** the notebook and change the file name extension from “**txt**” to “**csv**”.

6. What information can be set to create new users with PowerShell?

### Creating Single User using PowerShell

Command – `New-MsolUser -DisplayName “display name” -FirstName “first name” -LastName “last name” -UserPrincipalName <sign-in name> -UsageLocation <ISO 3166-1 alpha-2 country code> -LicenseAssignment <licensing plan name> [-Password <Password>]`

### Creating Bulk User Using Powershell

```
Import-Csv -Path <Input CSV File Path and Name> | foreach {New-MsolUser -DisplayName $_.DisplayName -FirstName $_.FirstName -LastName $_.LastName -UserPrincipalName $_.UserPrincipalName -UsageLocation $_.UsageLocation -LicenseAssignment $_.AccountSkuld [-Password $_.Password]} | Export-Csv -Path <Output CSV File Path and Name>
```

- ✓ DisplayName
- ✓ FirstName
- ✓ LastName
- ✓ Password
- ✓ User Principal Name
- ✓ UsageLocation
- ✓ AccountSkuld

## W-1, D-4

Property name	Required?	Description
DisplayName	Yes	<ul style="list-style-type: none"><li>✓ This is the display name that's used in Office 365 services.</li><li>✓ For example, MD Samiul Islam.</li><li>✓ Inside the inverted comma (" ")</li></ul>
UserPrincipalName	Yes	<ul style="list-style-type: none"><li>✓ Used to sign in to Microsoft 365 services.</li><li>✓ For example, samiulengineer@novoir.onmicrosoft.com.</li></ul>
FirstName	No	<ul style="list-style-type: none"><li>✓ First Name inside the inverted comma (" ")</li></ul>
LastName	No	<ul style="list-style-type: none"><li>✓ Last Name inside the inverted comma (" ")</li></ul>
LicenseAssignment	No	<ul style="list-style-type: none"><li>✓ Licensing plan for Microsoft 365, which is assigned to the user account.</li><li>✓ No need to assign a license to a user when you create the account, but the account requires a license to access Microsoft 365 services. You have 30 days to license the user account after you create it.</li></ul>
Password	No	<ul style="list-style-type: none"><li>✓ If you don't specify a password, a random password is assigned to the user account, and the password is visible in the results of the command.</li><li>✓ If you specify a password, it needs to be 8 to 16 ASCII text characters from any three of the following types: lowercase letters, uppercase letters, numbers, and symbols.</li></ul>
UsageLocation	No	<ul style="list-style-type: none"><li>✓ This is a valid ISO 3166-1 alpha-2 country code.</li><li>✓ For example, US for the United States, and FR for France.</li></ul>

### 7. What is shared mailbox

- ✓ Shared mailboxes are used when multiple people need access to the same mailbox, such as company information or support email address, reception desk, or other function that might be shared by multiple people.
- ✓ Shared mailboxes can receive external emails if the administrator has enabled this.
- ✓ Users with permissions to the group mailbox can send as or send on behalf of the mailbox email address if the administrator has given that user permissions to do that.
- ✓ Can use 50 GB and upgradable depending on administrative permission.



## **W-1, D-4**

8. Describe types of 'groups' in Microsoft 365 and its function.

Group Name	Description
1. Office 365	<ul style="list-style-type: none"><li>✓ Used for collaboration between users, both inside and outside the company.</li><li>✓ It can be configured for dynamic membership in Azure Active Directory, allowing group members to be added or removed automatically based on user attributes such as department, location, title, etc.</li><li>✓ It can be accessed through mobile apps such as Outlook for iOS and Outlook for Android.</li><li>✓ Group members can send as or send on behalf of the group email address if this has been enabled by the administrator.</li></ul>
2. Distribution	<ul style="list-style-type: none"><li>✓ Used for sending notifications to a group of people.</li><li>✓ Members can receive the external email if enabled by the administrator.</li><li>✓ Used to broadcast information to a set group of people.</li></ul>
3. Security	<ul style="list-style-type: none"><li>✓ Used for granting access to resources such as SharePoint sites.</li><li>✓ Members can make administration easier because you need only administer the group rather than adding users to each resource individually.</li><li>✓ Security groups can contain users or devices. Creating a security group for devices can be used with mobile device management services, such as Intune.</li><li>✓ Security groups can be configured for dynamic membership in Azure Active Directory, allowing group members or devices to be added or removed automatically based on user attributes such as department, location, or title; or device attributes such as operating system version.</li></ul>
4. Mail-enabled security	<ul style="list-style-type: none"><li>✓ Can send email to each other.</li><li>✓ Used for granting access to resources such as SharePoint.</li><li>✓ Emailing notifications to those users.</li><li>✓ Mail-enabled security groups function the same as regular security groups, except that they cannot be dynamically managed through Azure Active Directory and cannot contain devices.</li></ul>
• Navigation to the Groups	<b>Admin Center &gt; Groups &gt; Add a Group</b>

## W-1, D-5

1. What are the Admin Roles? Detailed descriptions and limitations of roles.

Admin Roles	Description	Limitation
1. Global Admin	<ul style="list-style-type: none"><li>✓ Access to most management features</li><li>✓ Reset passwords for all users</li><li>✓ Add and manage domains</li><li>✓ Signed up person automatically becomes a Global admin.</li></ul>	✓ Recommended maximum 2-4 Global Admins
2. Exchange Admin	<ul style="list-style-type: none"><li>✓ View and manage your user's -<ul style="list-style-type: none"><li>○ Mailboxes</li><li>○ Microsoft 365 groups</li><li>○ Exchange Online</li></ul></li><li>✓ Recover deleted items in a user's mailbox</li><li>✓ Set up "Send As" &amp; "Send on behalf" delegates</li></ul>	✓ Can't access as Admin to other Services
3. Global Reader	<ul style="list-style-type: none"><li>✓ View admin features and settings in admin centers that the global admin can view.</li></ul>	✓ The global reader admin can't edit any settings.
4. Group Admin	<ul style="list-style-type: none"><li>✓ Create, edit, delete and restore Microsoft 365 groups</li><li>✓ Create and update group creation, expiration, and naming policies</li><li>✓ Create, edit, delete and restore Azure Active Directory security groups</li></ul>	
5. HelpDesk Admin	<ul style="list-style-type: none"><li>✓ Reset passwords</li><li>✓ Force users to sign out</li><li>✓ Manage service requests</li><li>✓ Monitor service health</li></ul>	✓ Can only help non-admin users and users assigned these roles: Directory reader, Guest inviter, Helpdesk admin, Message center reader, and Reports reader.
6. Service Admin	<ul style="list-style-type: none"><li>✓ Open and manage service requests</li><li>✓ View and share message center posts</li></ul>	

## **W-1, D-5**

<b>7. SharePoint Admin</b>	<ul style="list-style-type: none"><li>✓ manage the SharePoint Online admin center.</li><li>✓ Create and delete sites</li><li>✓ Manage site collections and global SharePoint settings</li></ul>	✓ Limited to SharePoint Service only
<b>8. Teams Service Admin</b>	<ul style="list-style-type: none"><li>✓ Manage the Teams admin center</li><li>✓ Manage meetings</li><li>✓ Manage conference bridges</li><li>✓ Manage all org-wide settings, including federation, teams upgrade, and teams client settings</li></ul>	✓ Limited to Teams Service only
<b>9. User Admin</b>	<ul style="list-style-type: none"><li>✓ Add users and groups</li><li>✓ Assign licenses</li><li>✓ Manage most users' properties</li><li>✓ Create and manage user views</li><li>✓ Update password expiration policies</li><li>✓ Manage service requests</li><li>✓ Monitor service health</li><li>✓ Assigned the following roles: Directory reader, Guest inviter, Helpdesk admin, Message center reader, Reports reader.</li><li>✓ Manage usernames</li><li>✓ Delete and restore users</li><li>✓ Reset passwords</li><li>✓ Force users to sign out</li><li>✓ Update (FIDO) device keys</li></ul>	
<b>10. Office Apps Admin</b>	<ul style="list-style-type: none"><li>✓ Use the Office cloud policy service to create and manage cloud-based policies for Office</li><li>✓ Create and manage service requests</li><li>✓ Manage the What's New content that users see in their Office apps</li><li>✓ Monitor service health</li></ul>	✓ Limited to Office Apps

## W-1, D-5

### 2. What are the resources?

Resources	Description
Rooms & Equipment	<ul style="list-style-type: none"><li>✓ <b>Microsoft 365 Admin Center &gt; Resources &gt; Rooms &amp; Equipment</b></li><li>✓ Can create for specific room mailbox e.g. conference, meeting room.</li><li>✓ Can create for specific equipment mailbox e.g. printer, projector.</li><li>✓ Used for booking purpose for a specific time through outlook,</li><li>✓ Anyone can book the room or equipment.</li><li>✓ Delegates are dealing with all of that and admin can choose the delegates</li></ul>
Sites	<ul style="list-style-type: none"><li>✓ <b>Microsoft 365 Admin Center &gt; Resources &gt; Sites</b></li><li>✓ Used for SharePoint Access</li><li>✓ Can share files, make collaboration with the team members</li></ul>

### 3. A short overview of Billing & Payment methods. How to check how many subscriptions or licenses a tenant has?

Billing	Description
Billing & Payment Methods	<ul style="list-style-type: none"><li>✓ In the Billing section of Microsoft 365 Admin Center, we can see current services and licenses that we are using</li><li>✓ Possible to assign the license to the user</li><li>✓ Possible to add the payment method and auto transaction</li><li>✓ Add more licenses</li><li>✓ Check transaction history</li><li>✓ Receive Billing statement/notification</li></ul>
<ol style="list-style-type: none"><li>1. Microsoft 365 Admin &gt; <b>Billing &gt; Licenses</b></li><li>2. Assign/Unassign the licenses from here</li></ol>	

## W-1, D-5

4. What is the Password Expiration Policy?
5. How to set up password expiration policy?

<b>Password Expiration Policy</b>	✓ Policy for changing login password after a certain period due to security purpose.
<ul style="list-style-type: none"><li>✓ Microsoft 365 Admin Center &gt; ① <b>Settings</b> &gt; ② <b>Org Settings</b> &gt; ③ <b>Security &amp; Privacy</b> &gt; ④ <b>Password expiration policy</b> &gt; select ⑤ Set user password to expire after a number of days &gt; Fill up details &amp; ⑥ Save changes</li><li>✓ Days before password expires –</li><li>✓ Default = <b>90 days</b>, possible to set between <b>14 - 730 days</b></li><li>✓ Days before a user is notified about expiration – Default = <b>14 days</b>, possible to set between <b>1 - 30 days</b></li></ul>	

6. How to add/modify organization information?

<ul style="list-style-type: none"><li>✓ Please go to – Microsoft 365 Admin Center &gt;</li><li>✓ ① <b>Settings</b> &gt; ② <b>Org Settings</b> &gt; ③ <b>Organization Profile</b> &gt; ④ <b>Organization Information</b> &gt; Fill up detail &amp; ⑤ Save changes</li></ul>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7. What is Partner Relationship?

<b>Partner Relationship</b>	<ul style="list-style-type: none"><li>✓ To manage a customer's service or subscription on their behalf, the customer must grant you administrator permissions for that service.</li><li>✓ To get administrator permissions from a customer, email them a reseller relationship request.</li><li>✓ After the customer approves your request, you'll be able to log on to the service's admin portal and manage the service on the customer's behalf.</li><li>✓ Your customers can find out which of their partners have admin privileges to their tenant from within the Office 365 admin portal.<ul style="list-style-type: none"><li>○ The customer needs to sign in to the Office 365 admin portal as a Global admin.</li><li>○ Select <b>Settings</b> &gt; <b>Partner relationships</b></li><li>○ On the Partner relationships page, the customer will see a list of the partners with whom they work and those that have been granted delegated administration privileges to their tenant.</li></ul></li></ul>
-----------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## W-1, D-5

8. What are the usage reports? How to check usage reports in Microsoft 365 Admin Center?

<ul style="list-style-type: none"><li>✓ How people in the business organization are using Microsoft 365 services. For example, you can identify who is using a service a lot and reaching quotas, or who may not need a Microsoft 365 license at all.</li><li>✓ Reports are available for the last 7 days, 30 days, 90 days, and 180 days. Data won't exist for all reporting periods right away. The reports become available within 48 hours.</li><li>✓ For example – if we consider about Email activity report we can see sent, received, read, meeting created, Meeting interacted, user mailbox. We can easily detect that the user behaviour and email responding criteria by looking at the reports.</li></ul>
<p>1. Please go to –</p> <ul style="list-style-type: none"><li>✓ Reports &gt; Usage to check the usage reports for the last 7 days, 30 days, 90 days, 180 days for different services.</li></ul>

9. How to check the Productivity score?

<ul style="list-style-type: none"><li>✓ Productivity Score</li></ul>	<ul style="list-style-type: none"><li>✓ Give insights that transform how work gets done.</li><li>✓ Provide you visibility into how your organization works</li><li>✓ Identify where you can enable improved experiences so people can reach their goals.</li><li>✓ Actions to update skills and systems so everyone can do their best work.</li><li>✓ This score reflects your organization's performance across measures of employee and technology experiences.</li></ul>
<p>2. Please go to – <a href="https://www.admin.microsoft.com">www.admin.microsoft.com</a> &gt; Reports &gt; Productivity Score</p>	

10. What is service health? How to check if there is any service incident is going on?

<ul style="list-style-type: none"><li>✓ Service Health</li></ul>	<ul style="list-style-type: none"><li>✓ Shows the current status of the service and details about service disruptions and outages.</li><li>✓ Planned maintenance information is available on the Message Center.</li></ul>
<ul style="list-style-type: none"><li>✓ Please go to – <a href="https://www.admin.microsoft.com">www.admin.microsoft.com</a> &gt; Health &gt; Service Health</li></ul>	

## **W-1, D-5**

11. How to check if there is any update/planned change for any products?

1. Please go to – [www.admin.microsoft.com](http://www.admin.microsoft.com) > Health > Message center
2. The primary way to inform about the update of the Microsoft 365 services though there are other ways.
3. Possible to get an email notification as a weekly digest

12. How many ways to assign admin roles?

You can assign users to a role in 2 different ways:

- ✓ Please go to the –
  - **Users > Active users > Select a user > Manage roles > Admin center access > Save changes**
- ✓ Please go to –
  - **Roles > select the role > Assign admins > Add > Select Members > Save**

13. After changing the role, how long it will take maximum to update the system?

- ✓ It will take maximum 24 hours but in most of the cases it works within a short time.

14. What is delegate for rooms & equipments?

- ✓ One of the people added to the Delegates will be responsible for accepting or declining meeting requests that are sent to the room mailbox.
- ✓ If you assign more than one resource delegate, only one of them has to act on a specific meeting request.

15. How to purchase a new service from the tenant?

- ✓ Please go to –
  - **Admin Center > Billing > Purchase Services > Choose your desired services**

16. How many ways to assign the license for the user?

There are 2 ways to assign the license –

- ✓ **Users > Active users > Select the user > Licenses and apps > Select licenses > Save changes**
- ✓ **Billing > Licenses > Select License > Select Users > Assign license**

# W-2, D-1

## 1. What is MFA? How to enable it?

<b>MFA</b>	<ul style="list-style-type: none"><li>✓ Known as 2-step verification</li><li>✓ Recommended for Admin</li><li>✓ Only Global admin can enable/disable the MFA</li><li>✓ Uses password &amp; additional verification method for sign in -<ul style="list-style-type: none"><li>○ Something you have with you that is not easily duplicated, such as a smartphone.</li><li>○ Something you uniquely and biologically have, such as your fingerprints, face, or other biometric attributes.</li></ul></li></ul> <p>By default, both Microsoft 365 and Office 365 support MFA for user accounts using:</p> <ul style="list-style-type: none"><li>✓ A text message sent to a phone that requires the user to type a verification code.</li><li>✓ A phone call.</li><li>✓ The Microsoft Authenticator smartphone app.</li></ul>
<b>Set up Multi-Factor Authentication (MFA)</b>	
1. Please log in to admin center and go to – <b>Users &gt; Active users &gt; Multi-factor authentication</b>	
2. A new window will open in a new tab, where you will see a list of users available in the tenant. Please select the desired user to enable the MFA. Please click <b>Enable</b>	
3. A new prompt window will open and please click <b>enable multi-factor auth</b>	
4. Now MFA is enabled, but need to enforce now. Please click <b>Enforce</b>	
5. A prompt window will open. Please click - <b>enforce multi-factor auth</b>	
6. Please click – <b>Manage user settings</b>  There you will find 3 new settings available. If you want you can configure here be selecting and <b>Save</b> .	



# W-2, D-1

## 2. What is App Password? How to create an app password?

<i>App Password</i>	<ul style="list-style-type: none"><li>✓ App passwords are auto-generated</li><li>✓ Should be created and entered once per app.</li><li>✓ Limit of 40 passwords per user. If you try to create one after that limit, you'll be prompted to delete an existing password before being allowed to create the new one.</li></ul>
<b>Set up App Password</b>	
1. Please log in to admin center and go to – <b>Admin centers &gt; Azure Active Directory</b>	
2. A new window will open in a new tab.  Please go to – <b>Users &gt; All users (Preview)</b>  where you will see a list of users available in the tenant. Please click the desired user.	
3. Please scroll down and Click – <b>Authentication methods</b>	
4. A new window will open.  Please click – <b>Access Panel Profile</b>	
5. Please click - <b>Additional security verification</b>	
6. Please click – <b>App passwords</b>	
7. A new prompt window will open, where you need to put a suitable name and click <b>Next</b>	
8. You will see a password will generate. Please click <b>copy password to clipboard</b> and save it in another place. Click <b>close</b>	
9. You will see that a list of passwords that you have created.	

## W-2, D-1

### 3. What is Exchange Online in Microsoft 365?

<i>Exchange Online</i>	<ul style="list-style-type: none"><li>✓ Microsoft Exchange Online is a hosted version of Exchange Server.</li><li>✓ Cloud-based service.</li><li>✓ Gives users access to email, calendar, contacts, and tasks from PCs, the web, and mobile devices.</li><li>✓ Integrates fully with Active Directory, enabling administrators to use group policies, as well as other administration tools, to manage Exchange Online features across their environment.</li><li>✓ Email is hosted on servers that support multiple customers simultaneously.</li><li>✓ Accessible to users on a wide range of devices from inside a corporate network or over the internet.</li></ul>
------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4. How to access Exchange Online Admin Center? What is the URL to access EXO Admin Center?

Exchange Online Admin Center URL	<a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a>
<p>1. Please go to –</p> <p>Admin center and Click <b>Exchange</b> under the Admin centers located at the left pane</p>	
<p>2. A new tab will be opened and you will see a list of features available in the left pane. A total of 11 features are available.</p> <p>(DaRPeCOP MaMoPUH)</p>	

## W-2, D-1

### 5. Familiarize with the navigations of EAC.

1. Dashboard	✓ Overview of the admin center.
2. Recipients	✓ View and manage your mailboxes, groups, resource mailboxes, contacts, shared mailboxes, and mailbox migrations.
3. Permissions	✓ Manage administrator roles, user roles, and Outlook on the web policies.
4. Compliance management	✓ Manage In-Place eDiscovery & Hold, auditing, data loss prevention (DLP), retention policies, retention tags, and journal rules.
5. Organization	✓ Manage organization sharing and apps for Outlook
6. Protection	✓ Manage malware filters, connection filters, content filters, outbound spam, and quarantine for your organization.
7. Mail flow	✓ Manage rules, message tracing, accepted domains, remote domains, and connectors.
8. Mobile	✓ Manage the mobile devices that you allow to connect to your organization. ✓ Manage mobile device access and mobile device mailbox policies.
9. Public folders	✓ Manage public folders and public folder mailboxes.
10.Unified messaging	✓ Manage Unified Messaging (UM) dial plans and UM IP gateways.

## W-2, D-1

6. What do you understand by EXO limits?

Mailbox Storage Limits		
Features	Business (Basic, Standard, Premium)	Enterprise (E3, E5)
✓ User Mailbox	50 GB	100 GB
✓ Archive Mailbox	50 GB	✓ Initially 100 GB ✓ Auto Expanding Archiving On another 10 GB and again 10 GB upto 1 TB
✓ Shared Mailbox	✓ 50 GB (Without License) ✓ 100 GB (EO Plan-2 License) ✓ 100 GB (EO Plan-1 with Exchange Online Archiving add-on license)	✓ 50 GB (without License) ✓ 100 GB (E3, E5 License)
✓ Resource Mailbox	✓ 50 GB (without License) ✓ 100 GB (E3, E5 License)	✓ 50 GB (without License) ✓ 100 GB (E3, E5 License)
✓ Site Mailbox	50 GB	50 GB
✓ Public Folder Mailbox	50 GB	100 GB
✓ Group Mailbox	50 GB	50 GB

Address Book Limits		
Features	Business (Basic, Standard, Premium)	Enterprise (E3, E5)
✓ Address list limit	1000	1000
✓ Offline address book (OAB) limit	250	250
✓ Address book policies (ABP) limit	250	250
✓ Global address lists limit	250	250

Receiving & Sending Limits		
Features	Business (Basic, Standard, Premium)	Enterprise (E3, E5)
✓ Messages received	3,600 message/hour	3,600 message/hour
✓ Sending Recipient rate limit	10,000 recipients/day	10,000 recipients/day
✓ Sending Recipient limit	1,000 recipients	1000 recipients
✓ Sending Recipient proxy address limit	400	400
✓ Message rate limit	30 messages/minute	30 messages/minute

## W-2, D-1

Message Limits		
Features	Business (Basic, Standard, Premium)	Enterprise (E3, E5)
✓ Message size limit – Outlook for windows & MAC	✓ 150 MB (default 25 MB) ✓ Possible 33% encoding increase	✓ 150 MB (default 25 MB) ✓ Possible 33% encoding increase
✓ Message size limit - OWA	✓ 112 MB (default 25 MB) ✓ Possible 33% encoding increase	✓ 112 MB (default 25 MB) ✓ Possible 33% encoding increase
✓ Message size limit - migration	150 MB (default 25 MB)	150 MB (default 25 MB)
✓ Message size limit - Outlook for iOS and Android	33 MB	33 MB
✓ Subject length limit	250 Characters	250 Characters
✓ File attachments limit	250 Attachments	250 Attachments
✓ File attachment size limit - Outlook for windows & MAC	150 MB	150 MB
✓ File attachment size limit – OWA	112 MB 2 GB (One Drive Attachment)	112 MB 2 GB (One Drive Attachment)
✓ File attachment size limit - Outlook for iOS and Android	33 MB	33 MB
✓ Embedded message depth limit	30 embedded messages	30 embedded messages

Retention Limits		
Features	Business (Basic, Standard, Premium)	Enterprise (E3, E5)
✓ Deleted Items folder retention period	No limit	No limit
✓ Retention period for items removed from the Deleted Items folder	Default 14 days Max 30 days	Default 14 days Max 30 days
✓ Junk Email folder retention period	30 days	30 days

## W-2, D-1

### 7. What is the Exchange Online deployment types?

Deployment Types	Description
1. Cloud-only Deployment	<ul style="list-style-type: none"><li>✓ All user mailboxes hosted in Exchange Online.</li><li>✓ Exchange Online service isn't connected with an on-premises Exchange organization</li></ul>
2. Exchange hybrid Deployment	<ul style="list-style-type: none"><li>✓ Some user mailboxes hosted in an on-premises Exchange organization and some user mailboxes hosted in Exchange Online.</li><li>✓ Available for Microsoft Exchange 2003, Exchange 2007, Exchange 2010 and Exchange 2013 on-premises organizations.</li><li>✓ Offers organizations the ability to extend the feature-rich experience and administrative control they have with their existing on-premises Microsoft Exchange organization to the cloud.</li></ul>

### 8. Why do we need MFA?

- ✓ To provide more security for the account.
- ✓ Microsoft recommends to enable MFA for all types of admins and not required for users.
- ✓ Protecting the sensitive data to prevent various attacks designed to gain access to the data and the account itself.
- ✓ Office 365 MFA is critically important to limiting unlawful access to the world's most popular SaaS (software as a Service) business system.

### 9. Is there any other way to change app password in Additional Security Verification?

- ✓ Please login to- <https://outlook.office365.com>  
<https://admin.microsoft.com>  
<https://outlook.office365.com/ecp>
- ✓ Click Top right corner, where you will see you **My account**
- ✓ **Overview** > under Security Info **Additional Security Verification** > **App passwords** > **Create**

### 10. Why do we need App Passwords?

- ✓ If Microsoft service or device that you use that doesn't support two-step verification codes.
- ✓ Face issues using older apps or devices (like **Windows Phone 8, Xbox 360, Outlook 2010**) that don't support two-step verification.
- ✓ Users are facing problem if they want to enable MFA and want to use old apps.

## W-2, D-1

11. Which kind of options you will find during MFA enabling?

- ✓ Enable
- ✓ Enforce
- ✓ Manage Settings
  - Require selected users to **provide** contact methods again
  - **Delete** all existing app passwords generated by the selected users
  - **Restore** multi-factor authentication on all remembered devices

12. What is modern Authentication?

- ✓ Modern authentication in Exchange Online enables authentication features like multi-factor authentication (MFA), smart cards, certificate-based authentication (CBA), and third-party SAML identity providers. Modern authentication is based on the Active Directory Authentication Library (ADAL) and OAuth 2.0.
- ✓ When you enable modern authentication in Exchange Online, Windows-based Outlook clients that support modern authentication (Outlook 2013 or later) use modern authentication to connect to Exchange Online mailboxes.
- ✓ When you disable modern authentication in Exchange Online, Windows-based Outlook clients that support modern authentication use basic authentication to connect to Exchange Online mailboxes.

13. How to enable/disable modern authentication?

- ✓ Microsoft 365 Admin Center – <https://admin.microsoft.com>
- ✓ **Settings > Org settings > Services > Modern authentication**

## W-2, D-2

1. What are the recipients? Mention all the recipients of EAC.

<b>Recipients in Exchange Online Admin Center</b>	<ul style="list-style-type: none"><li>• View and manage your mailboxes, groups, resource mailboxes, contacts, shared mailboxes, and mailbox migrations.</li></ul>
<ul style="list-style-type: none"><li>• There are 6 recipients options available –</li></ul> <p><b>(mg rc sm)</b></p> <ol style="list-style-type: none"><li>1. Mailboxes</li><li>2. Groups</li><li>3. Resources</li><li>4. Contacts</li><li>5. Shared</li><li>6. Migration</li></ol>	

2. How many types of groups are there in EXO? Mention the difference between those groups.

<b>Group Name</b>	<b>Description</b>
1. Office 365	<ul style="list-style-type: none"><li>✓ Used for collaboration between users, both inside and outside the company.</li><li>✓ It can be configured for dynamic membership in Azure Active Directory, allowing group members to be added or removed automatically based on user attributes such as department, location, title, etc.</li><li>✓ It can be accessed through mobile apps such as Outlook for iOS and Outlook for Android.</li><li>✓ Group members can send as or send on behalf of the group email address if this has been enabled by the administrator.</li></ul>
2. Distribution	<ul style="list-style-type: none"><li>✓ Used for sending notifications to a group of people.</li><li>✓ Members can receive the external email if enabled by the administrator.</li><li>✓ Used to broadcast information to a set group of people.</li></ul>
3. Dynamic Distribution	<ul style="list-style-type: none"><li>✓ Same as distribution groups</li><li>✓ Membership list for dynamic distribution groups is calculated each time a message is sent to the group, based on the filters and conditions that you define.</li></ul>



## W-2, D-2

	<ul style="list-style-type: none"> <li>✓ When an email message is sent to a dynamic distribution group, it's delivered to all recipients in the organization that match the criteria defined for that group.</li> </ul>
4. Mail-enabled security	<ul style="list-style-type: none"> <li>✓ Can send email to each other.</li> <li>✓ Used for granting access to resources such as SharePoint.</li> <li>✓ Emailing notifications to those users.</li> <li>✓ Mail-enabled security groups function the same as regular security groups, except that they cannot be dynamically managed through Azure Active Directory and cannot contain devices.</li> </ul>
<p>✓ Navigation to the Groups –</p> <p>Please login to EAC to –  <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a></p> <p>Then, recipients &gt; groups</p>	

### 3. How to create O365 Group as normal user?

Creating office 365 group as normal user	
From Outlook Client	✓ Groups > New Group
From OWA	✓ Groups > New Group > Groups Name > Create

### 4. What are the resources in EAC? Explain the difference between room & equipment mailboxes.

Resources	<ol style="list-style-type: none"> <li>1. Room Mailbox</li> <li>2. Equipment Mailbox</li> </ol>
-----------	-------------------------------------------------------------------------------------------------

## W-2, D-2

Room Mailbox	Equipment Mailbox
<ul style="list-style-type: none"> <li>✓ A room mailbox is a resource mailbox that's assigned to a physical location, such as a conference room, an auditorium, or a training room.</li> <li>✓ With room mailboxes, users can easily reserve these rooms by including room mailboxes in their meeting requests. When they do this, the room mailbox uses options you can configure to decide whether the invite should be accepted or denied.</li> <li>✓ To create a room mailbox, you need to be an administrator who's a member of either the –               <ul style="list-style-type: none"> <li>○ Organization Management or</li> <li>○ Recipient Management role groups.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>✓ An equipment mailbox is a resource mailbox assigned to a resource that's not location specific, such as a portable computer, projector, microphone, or a company car.</li> <li>✓ After an administrator creates an equipment mailbox, users can easily reserve the piece of equipment by including the corresponding equipment mailbox in a meeting request.</li> <li>✓ You can use the Exchange admin center (EAC) and the Exchange Management Shell to create an equipment mailbox or change equipment mailbox properties.</li> </ul>

### 5. What is the difference between mail contact and mail user?

Mail Contact	Mail user
✓ In Exchange Online organizations, mail users are similar to mail contacts. Both have external email addresses and both contain information about people outside your Exchange Online organization that can be displayed in the shared address book and other address lists.	
✓ A mail contact hasn't logon credentials in your Microsoft 365 organization and can access resources.	✓ However, unlike a mail contact, a mail user has logon credentials in your Microsoft 365 organization and can access resources.
✓ You manage mail contacts in the Exchange admin center (EAC) or in PowerShell (Exchange Online PowerShell in organizations with Exchange Online mailboxes; standalone Exchange Online Protection (EOP)).	✓ You manage mail users in the Exchange admin center (EAC) or in PowerShell (Exchange Online PowerShell in organizations with Exchange Online mailboxes).
✓ In Exchange Online organizations, mail contacts are mail-enabled objects that contain information about people who exist outside your organization. Each mail contact has an external email address.	✓ In Exchange Online organizations, mail users are mail-enabled objects that contain information about people who exist inside your organization. Each mail user has an internal email address.
✓ Can't add in the distribution group.	✓ Can add in the group

## W-2, D-2

6. How many types of mailboxes are there?

- ✓ User Mailbox
- ✓ Group Mailbox
- ✓ Resource Mailbox
- ✓ Contact Mailbox
- ✓ Shared Mailbox

7. How to access shared mailbox? Is it possible to send emails from shared mailbox?

Access Shared Mailbox from OWA	
Group Name	Description
<p>1. Please log in to – <a href="http://www.outlook.office365.com">www.outlook.office365.com</a></p> <p>2. Please click at the right top corner, there you will see an option <b>Open another mailbox</b> – click and enter the shared mailbox and <b>Open</b>.</p> <p>3. The shared mailbox will be opened in the new tab as a new mailbox.</p>	

Access Shared Mailbox from Outlook Client	
<p>✓ Please open <b>Outlook Client</b></p> <p>Please go to the top left corner and click File</p>	
<p>✓ In the Info page go to Account Settings</p>	
<p>✓ Please select the email address and press Change</p>	
<p>✓ Please go to – More Settings</p>	
<p>✓ In the <b>Advanced</b> tab please click <b>Add</b> and type your shared mailbox and press <b>OK</b>.</p> <p>Your shared mailbox is now enrolled in the outlook client. You can send and receive the email message in the shared mailbox anytime in the outlook client.</p>	

## W-2, D-2

8. What is mailbox usage limit? How to check it? How to Convert Regular Mailbox to Shared Mailbox and vice versa?

Checking Mailbox Usage Limit	
Group Name	Description
Mailbox Usage Limit	<ul style="list-style-type: none"><li>✓ The amount of mailbox storage available is determined by the mailbox type and the user's subscription license.</li><li>✓ Administrators can reduce maximum mailbox sizes per user or globally.</li></ul>
<p>✓ Please go to – <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a></p> <p>✓ Then click –</p> <p>① recipients &gt; ② mailboxes &gt; ③ select the users and double click on it &gt; ④ Then go to mailbox usage &gt; ⑤ check the mailbox usage</p>	
Convert Regular Mailbox to Shared	
Group Name	Description
<p>✓ Please go to – <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a></p> <p>✓ Then click –</p> <p>① recipients &gt; ② mailboxes &gt; ③ select and double click on the user &gt; ④ at right side menu under the Convert to Shared Mailbox, click Convert &gt; ⑤ press Yes</p>	
Convert Shared to Regular	
Group Name	Description
<p>✓ Please go to – <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a></p> <p>✓ Then click –</p> <p>① recipients &gt; ② shared &gt; ③ select and double click on the user &gt; ④ at right side menu under the Convert to Regular Mailbox, click Convert &gt; ⑤ press Yes</p>	
<p>When you press Yes, we will see a prompt message that we need to assign license and reset the password from Microsoft 365 admin center after creating regular mailbox as we need license and password to use this mailbox.</p>	

## W-2, D-2

9. Explain about mailbox features.

<b>Mailbox Features</b>		✓ <b>Only available in EXO user mailbox and shared mailbox</b>
<b>Navigation</b>		✓ EXO Admin Center > recipients > mailbox > select & double-click on the mailbox > mailbox features ✓ EXO Admin Center > recipients > mailbox > select & double-click on the mailbox > mailbox features
<b>3 Options Available</b>	<b>Policy</b>	<b>(ShaRRA)</b> 1. Sharing Policy 2. Role Assignment Policy 3. Retention Policy 4. Addressbook Policy
	<b>Email Connectivity</b>	1. Outlook on the Web 2. IMAP (Internet Message Access Protocol) 3. POP3 (Post Office Protocol) 4. MAPI (Outlook Client – Message Application Programming Interface) 5. Litigation Hold 6. Archiving
	<b>Mail Flow</b>	1. Delivery Options (forwarding option, maximum recipients) 2. Message Size Restrictions (maximum sent/receive message size) 3. Message Delivery Restrictions (Accept/Reject Message)

10. Comparison of mailboxes, resources, shared options.

<b>mailboxes</b>	<b>resources</b>	<b>shared</b>
general	general	general
<b>mailbox usage</b>		<b>mailbox usage</b>
contact information		contact information
organization		organization
email address	email address	email address
<b>mailbox features*</b>		<b>mailbox features*</b>
member of		member of
Mailtip	Mailtip	Mailtip
<b>mailbox delegation</b> (send as. Send on behalf, Full access)	<b>mailbox delegation</b> (send as. Send on behalf, Full access)	<b>mailbox delegation</b> (send as, Full access)
	<b>booking delegates</b> (responsible for accept/decline booking request)	
	<b>booking option</b> (max booking lead times – set 0 for only today, max duration – set 0 for unlimited)	

## W-2, D-2

### 11. Comparison of different groups in EXO.

Office 365	Distribution	Dynamic Distribution	Mail-enabled security
general	general	general	general
ownership	ownership	ownership	ownership
membership	membership	Membership (based on criteria)	membership
delivery management (accept/reject)	delivery management (allow internal or external sender)	delivery management (allow internal or external sender)	delivery management (allow internal or external sender)
group delegation (send as, send on behalf)	group delegation (send as, send on behalf)	group delegation (send as, send on behalf)	group delegation (send as, send on behalf)
	membership approval		membership approval
	message approval		message approval
	email option		email option
	Mailtip		Mailtip

### 12. Comparison among “Send As”, “Send on behalf” and “Full access”

Send As	Send on behalf	Full access
<ul style="list-style-type: none"> <li>✓ Allows the delegate to send messages as if they came directly from the mailbox or group.</li> <li>✓ There's no indication that the message was sent by the delegate.</li> <li>✓ Doesn't allow to read the contents of the mailbox.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Allows the delegate to send messages from the mailbox or group.</li> <li>✓ The From address of these messages clearly shows that the message was sent by the delegate ("&lt;Delegate&gt; on behalf of &lt;MailboxOrGroup&gt;").</li> <li>✓ Doesn't allow the delegate to read the contents of the mailbox.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Allows the delegate to open the mailbox, and view, add and remove the contents of the mailbox.</li> <li>✓ Doesn't allow the delegate to send messages from the mailbox.</li> </ul>

### 13. As there is limit of sending email to maximum recipient (default 500), can I send to one group of 5000 members?

This limit is only applicable for the To, Cc, Bcc recipient email addresses. So, you can send easily to that group as this group is taken only 1 mailbox recipient.

### 14. What is Group Delegation?

Select responsible person to send email as if his own mailbox, send on behalf. Thus, someone is responsible for the group. There are 2 options available – “send as” & “send on behalf”

## W-2, D-2

### 15. What is Mailbox Delegation?

Mailbox delegation is similar to group delegation except this one is for user mailboxes, resources and shared.

### 16. Why we do not have Security group in Exchange Online?

Security group members are not allowed to send email to each other. On the other hand, Mail-Enabled Security members are able to send email among the members. Perhaps, Exchange Online service is only dealing with message/email sending/receiving. That is the reason, Security group is not required in EXO.

### 17. If I don't have EXO license, but I am a member of a group. Can I send email?

No, you can't, because EXO is dealing with email message sending/receiving. We must need EXO license whether as Business, Enterprise license or standalone EXO Plan-1/2 license.

### 18. Why there isn't "Sites" option in the "Resources" in EAC?

"**Sites**" option is available in Microsoft 365 Admin center under the "**Resources**" because it is necessary for SharePoint service, where you can create site link to share the files using SharePoint.

### 19. Why do we need to reset password and assign license after converting shared mailbox to regular mailbox?

A user needs license to use the services and shared mailbox doesn't have password but a user needs password to access the mailbox.

### 20. Why can I not add external user in shared mailbox?

To access the shared mailbox, you need a regular mailbox of an organization. External user doesn't have regular mailbox – for that reason external users are not allowed to be a member of shared mailbox.

### 21. What services are included in the Exchange Online?

- ✓ Access to email, calendar, contacts, and tasks from PCs, the web, and mobile devices.
- ✓ It integrates fully with Active Directory, enabling administrators to use group policies, as well as other administration tools, to manage Exchange Online features across their environment.
- ✓ Policy, Compliance, DLP, Auditing, Journaling etc.

### 22. What will happen if anyone exceeds the limit of sending limits 30 messages/minute?

The user may be blocked temporarily or permanently.

## W-2, D-3

1. What is Role-based permissions or Role Based Access Control (RBAC)?
2. Define Administrative roles.
3. Define End-user roles.

<b>Role-Based Permission</b>	<ul style="list-style-type: none"><li>✓ In Exchange Online, the permissions that you grant to administrators and users are based on management roles.</li><li>✓ A role defines the set of tasks that an administrator or user can perform.</li><li>✓ A large set of pre-defined roles known as RBAC (Role-Based Access Control), which are in the role group section</li><li>✓ 2-types of rules – administrative and end-user rules.</li><li>✓ For example, a help desk admin has to perform a set of roles to deal with the users' daily activities e.g. reset password, available user options. A help desk admin doesn't need to perform another administrative task.</li><li>✓ We can compare this as same as physical office e.g. a Regulatory Officer used to perform only regulatory-related jobs and IT officer needs to perform his duty related to IT.</li></ul>
<b>Administrative Roles</b>	<ul style="list-style-type: none"><li>✓ Can be assigned to administrators or specialist users.</li><li>✓ Manage a part of the Exchange Online organization, such as recipients.</li></ul> <p>Somehow Microsoft 365 online and Exchange online overlap each other in terms of roles -</p> <ul style="list-style-type: none"><li>✓ First, users who are Global Administrators or Service Administrators in Microsoft Online are automatically assigned to the Organization Management role group in Exchange Online.</li><li>✓ Second, users who are Help Desk Administrators in Microsoft Online are automatically assigned to the Help Desk role group in Exchange Online.</li></ul>
<b>End-user Roles</b>	<ul style="list-style-type: none"><li>✓ Assigned by using role assignment policies</li><li>✓ Manage aspects of their mailboxes and distribution groups that they own.</li><li>✓ End-user roles begin with the prefix "<b>My</b>".</li></ul>
Some role groups are pre-defined. We can add members to the role groups.	
Default Roles applied for all, if we change this role settings it will be applied to all user. If we want to create specific roles for specific users, then we need to create custom roles and applied to the users/groups from the recipient	



## W-2, D-3

4. Function of Outlook Web App mailbox policies. (Try all the available OWA policies)

Inbox Rules Check
Initially, the rules can be set.
Please login to – <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a>
Navigate to – ① <b>permission</b> > ② <b>Outlook We App policies</b> > ③ <b>OwaMailboxPolicy-Default</b> > ④ <b>untick inbox rules</b> > ⑤ <b>press Save</b>
Please login to – <a href="http://www.outlook.office365.com">www.outlook.office365.com</a>
Navigate to – Top right corner <b>Gear Settings Icon</b> > <b>View all outlook Settings</b> > <b>Mail</b>

Direct File Access Check
From the <b>file access</b> , if we uncheck this option, users will unable to open the attachment from OWA.

5. Perform below practical steps:

Assign one user with eDiscovery management
Please login to – <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a>
Navigate to – ① <b>permission</b> > ② <b>admin roles</b> > ③ double-click on the <b>Discovery Management</b> > ④ under the <b>Members</b> section click plus “+” sign > ⑤ select the user > ⑥ <b>press OK</b>

## W-2, D-3

### Create one User role and assign to one user.

Please login to –

<https://outlook.office365.com/ecp>

Navigate to –

① **permission** > ② **user roles** > ③ section click **plus “+”** sign > ④ write down Policy Name > ⑤ select end-user rules > ⑥ press **Save**

✓ It will take some time to create new user roles.

✓ When new role is created please navigate to –

① **recipients** > ② **mailboxes** > ③ double-click on the user > ④ select the **Role assignment policy** > ⑤ press **Save**

### Create OWA policy for - Disable user access on features for Themes and inbox rules.

Please login to –

<https://outlook.office365.com/ecp>

Navigate to –

① **permission** > ② **Outlook Web App policies** > ③ double-click on the OwaMailboxPolicy-Default > ④ uncheck **Inbox Rules** and **Themes** > ⑤ press **Save**

✓ Initially, there is a **Theme** option in Settings in OWA

✓ After unchecking the OWA policies for Themes there is no option for **Theme** in Settings

## 6. How to disable or enable OWA features for users?

- ✓ Please login to – <https://outlook.office365.com/ecp>
- ✓ Navigate to – **permission** > **Outlook We App policies** > *double-click on the OwaMailboxPolicy-Default* > **features**
- ✓ Here you will find different options for check or uncheck the options in different categories e.g. Communication Management, Information Management, User Experience, Time Management.
- ✓ For example, if we uncheck **Inbox rules** under the Information Management category, users will not be able to see the Rule option in the OWA.
- ✓ We can create custom OWA policy and assign this policy for the specific user.

## W-2, D-3

Restricting User to Enter the Account in OWA	
Disable & Enable OWA feature for users	
Please login to – <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a>	
Navigate to – ① recipients > ② mailboxes > ③ select & double-click on the user > ④ click <b>Enable/Disable</b> > ⑤ press <b>Save</b>	
✓ Press <b>Yes</b>	
✓ After disabling the OWA features for the user/users. User can't log in anymore from the web. He/she will get this error message.	

### 7. What are Inbox rules?

<b>Inbox Rule</b>	<ul style="list-style-type: none"><li>✓ An action that Outlook Web App runs automatically on incoming or outgoing messages.</li><li>✓ From the outlook client, we can also create rules. (Navigate to - <b>Rules</b> &gt; <b>Create Rule</b>)</li><li>✓ For example, a rule can be created to move all emails to trash if the email comes from any advertisement agency.</li></ul>
-------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 8. What is eDiscovery?

- ✓ The eDiscovery feature provides a single place for administrators, compliance officers, and other authorized users to conduct a comprehensive investigation into Microsoft 365 user activity. Security officers with the appropriate permissions perform searches and place holds on content.
- ✓ Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases.

### 9. What is the command for Outlook Web App policies?

- ✓ New-OwaMailboxPolicy -Name <policy name>
- ✓ Get-OwaMailboxPolicy

## W-2, D-3

### 10.Explain Details about EXO Permission.

Permission	admin roles	Compliance Management	Name	
		Discovery Management	.....	
		Organization Management	Roles	
		Help Desk		
		Security Administrator	Members	
		.....		
	user roles	Default Role Assignment Policy	Contact information	
			Profile information	
			Distribution groups	
			Distribution group memberships	
			Other roles	
	Outlook Web App Policies	OWAMailboxPolicy-Default	general	
			features	Communication management (Linkedin...)
				Information management (Inbox Rules...)
				User experience (Themes...)
				Time management (Calendar...)
			file access	○ Direct file access
			offline access	○ Always ○ Private computer ○ Never

### 11. How to verify that disabling OWA access is working?

When user try to log in to the account, he will get an error message – “protocol disabled”

### 12.How to create inbox rules?

- ✓ <https://outlook.office365.com> > **Settings** (Gear sign) > **View all Outlook settings** > **Mail** > **Rules** > **Add new rule** (condition, action, exception)
- ✓ Outlook client > **Home** > **Rules** > **Create Rule**

## **W-2, D-3**

### 13. How to disable OWA access for user mailbox?

- ✓ <https://outlook.office365.com> > recipients > mailboxes > select & double-click on the mailbox > mailbox features > under email connectivity – Outlook on the web – Disable
- ✓ <https://outlook.office365.com> > recipients > mailboxes > properties at right side > under Email Connectivity – Outlook on the web – Disable

## W-2, D-4

### 1. What is an In-place hold and Litigation Hold?

<b>In-place hold</b>	<ul style="list-style-type: none"><li>✓ Hold all mailbox data for a user indefinitely or until when the hold is removed.</li><li>✓ Hold mailbox based on criteria or query parameter.</li><li>✓ To perform this, you need to be a member of <b>Discovery Management</b>.</li></ul> <p>Includes a new model that allows you to specify the following parameters:</p> <ul style="list-style-type: none"><li>✓ <b>What to hold:</b> You can specify which items to hold by using query parameters such as keywords, senders and recipients, start and end dates, and also specify the message types such as email messages or calendar items that you want to place on hold.</li><li>✓ <b>How long to hold:</b> You can specify a duration for items on hold.</li></ul>
<b>Litigation Hold</b>	<ul style="list-style-type: none"><li>✓ Hold entire mailbox without any criteria for a certain period or indefinite time</li><li>✓ Duration is calculated from the date a mailbox item is received or created. If a duration isn't set, items are held indefinitely or until the hold is removed.</li></ul>

### 2. How to put mailbox/mailboxes on litigation hold? Perform putting mailbox on litigation hold using PowerShell.

Put Mailbox Litigation Hold from EAC
<p>Please login to –</p> <p><a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a></p> <p>Please navigate to –</p> <p>① <b>recipients</b> &gt; ② <b>mailboxes</b> &gt; ③ select &amp; double-click on the user &gt; ④ <b>mailbox features</b> &gt; ⑤</p> <p>Under Litigation Hold option, click <b>Enable</b></p>
<p>⑥ You may give a value in the <b>Litigation hold duration (days)</b> box if you want to hold the mailbox for a certain period. If you leave this empty, the mailbox will be held for an indefinite time.</p> <p>⑦ press <b>Save</b></p>
<p>You will see <b>Litigation hold</b> is enabled now. The system will take some time (240 mins maximum) to execute the settings to that mailbox. ⑧ press <b>Save</b></p>

## W-2, D-4

### Put Mailbox Litigation Hold using PowerShell

Please open PowerShell as administrator –

Place a mailbox on Litigation Hold please type command –

**Set-Mailbox <UPN> -LitigationHoldEnabled <\$true/\$false>**

If you want to place all mailboxes on Litigation Hold then –

**# Set-Mailbox <UPN> -LitigationHoldEnabled <\$true/\$false> -LitigationHoldDuration <duration period (days)>**

To verify that the litigation hold commands working perfectly –

**Get-Mailbox <UPN> | Format-List LitigationHold\***

To verify that the litigation hold commands working perfectly –

**Get-Mailbox -ResultSize Unlimited -Filter "RecipientTypeDetails -eq 'UserMailbox'" | Format-Table Name,LitigationHold\***

### 3. What licenses are required for this feature?

#### License Required for Litigation Hold

- ✓ Standalone Exchange Online Plan-2
- ✓ Standalone Exchange Online Plan-1 + Auto Archiving Add-ins
- ✓ Enterprise (E3, E5) – included with EXO Plan-2

### 4. How to enable In-Place Archive from Admin Centre & PowerShell?

### Put Mailbox Litigation Hold from EAC

Please login to –

<https://outlook.office365.com/ecp>

Please navigate to –

① **recipients** > ② **mailboxes** > ③ select & double-click on the user > ④ **mailbox features** > ⑤ Under Archiving option, click **Enable** > ⑥ press **Save**

You can confirm from the mailboxes option. You will see **Mailbox Type** is now set to **User (Archive)**

## W-2, D-4

### Enable In-place Archive from PowerShell

Please open PowerShell as administrator –

Enable Archiving mailbox please type command –

**Enable-Mailbox <UPN> -Archive**

Verify the Archiving Command working Successfully -

**Get-Mailbox <UPN> | Format-List Name,RecipientTypeDetails,PrimarySmtpAddress,\*Archive\***

### 5. What is Auditing? How many types of Auditing are there?

- ✓ Use audit logging to troubleshoot configuration issues by tracking specific changes made by admins.
- ✓ Help to meet regulatory, compliance, and litigation requirements.

Exchange Online provides two types of audit logging:

- ✓ **Administrator** audit logging records any action, based on an Exchange Online PowerShell cmdlet, performed by an admin.
- ✓ **Mailbox** audit logging records when a mailbox is accessed by an admin, a delegated user, or the person who owns the mailbox.

1. **Run a non-owner mailbox access report:** Use this report to find mailboxes that have been accessed by someone other than the person who owns the mailbox.
2. **Export mailbox audit logs:** When mailbox audit logging is enabled for a mailbox, Exchange Online stores a record of actions performed on mailbox data by non-owners in the mailbox audit log, which is stored in a hidden folder in the mailbox being audited. Exchange Online saves the search results in an XML file and attaches it to an email message.
3. **Run an administrator role group report:** Use this report to search for changes made to administrator role groups.
4. **Run an in-place discovery and hold report:** Use this report to find mailboxes that have been put on, or removed from, In-Place Hold.
5. **Run a per-mailbox litigation hold report:** Use this report to find mailboxes that were put on, or removed from, litigation hold.
6. **Run the admin audit log report:** Use this report to view entries from the administrator audit log. Instead of exporting the administrator audit log, which can take up to 24 hours to receive in an email message, you can run this report in the EAC.



## W-2, D-4

7. **Export the administrator audit log:** Any action performed by an admin that's based on an Exchange Online PowerShell cmdlet that doesn't begin with the verbs Get, Search, or Test is logged in the administrator audit log. Exchange Online saves them in an XML file and attaches it to an email message.
8. **Run the external admin audit log report:** Actions performed by Microsoft datacenter administrators or delegated admins are logged in the administrator audit log. Use the external admin audit log report to search for and view the actions that administrators outside your organization performed on the configuration of your Exchange Online organization.

### 6. What is Journaling and why we use it?

<b>Journaling</b>	<ul style="list-style-type: none"><li>✓ Recording all inbound and outbound emails for the regulatory purpose</li><li>✓ Help organization respond to legal, regulatory, and organizational compliance requirements by recording inbound and outbound email communications.</li></ul>
<b>Reason for Using</b>	<ul style="list-style-type: none"><li>✓ To meet an increasing number of regulatory and compliance requirements, many organizations must maintain records of communications that occur when employees perform daily business tasks.</li></ul>

### 7. Explain the steps to enable Journaling.

Put Mailbox Litigation Hold from EAC
<p>Please login to –</p> <p><a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a></p> <p>Please navigate to –</p> <p>① <b>compliance management</b> &gt; ② <b>journal rules</b> &gt; ③ click “+” sign &gt; ④ press <b>Save</b></p> <p>Here 3 options are available to change –</p> <ol style="list-style-type: none"><li>1. Journaling Mailbox</li><li>2. Journal Recipient</li><li>3. Journal Rule Scope</li></ol> <p>Here, you will see a new journal entry.</p>

## W-2, D-4

### 8. Option in Compliance Management in EAC?

(InAD ReReJ)

- ✓ in-place eDiscovery & hold
- ✓ auditing
- ✓ data loss prevention
- ✓ retention policies
- ✓ retention tags
- ✓ journal rules

### 9. Which admin roles is required to perform litigation hold?

In permission > Admin roles > Discovery management

### 10. Which admin role is required to perform auditing?

In permission > Admin roles > Compliance Management

### 11. Who can be the Journaling Mailbox?

- ✓ Mail user
- ✓ Mail contact
- ✓ External user

### 12. What are the 3 things required for journal rules and Journal rule scope?

- ✓ Journaling Mailbox (whom we send journal reports)
- ✓ Journaling Recipient (which mailbox we want to record)
- ✓ Journal Rule Scope
  - Internal Message
  - External Message
  - All Message

### 13. Why do we need set **Send undeliverable journal reports to** before set journal rules?

If the system can't send the records of inbound and outbound message to Journaling mailbox then the report will go to the Send undeliverable journal reports to (email address).

## W-2, D-5

1. Why do we need to setup OrgSharing?
2. What is Individual Sharing Policy?

<b>Organization Sharing</b>	<ul style="list-style-type: none"><li>✓ To share calendar information with an external business partner.</li><li>✓ Microsoft 365 or Office 365 admins can set up an organization relationship with another Microsoft 365 and Office 365 organization or with an Exchange on-premises organization.</li><li>✓ One-to-one relationship between businesses to allow users in each organization to view calendar availability information.</li><li>✓ Allow you to enable federated sharing with another federated Exchange organization for the purpose of sharing calendar free/busy information between users in both organizations.</li><li>✓ Requiring a federation trust with the Microsoft Federation Gateway, organization relationships are one-to-one relationships between two Exchange organizations, not a relationship between individual users in the Exchange organizations.</li></ul> <p>Three options –</p> <ul style="list-style-type: none"><li>✓ Domain</li></ul> <p>There are two levels of access that you can specify:</p> <ul style="list-style-type: none"><li>✓ Calendar Free/busy information with time only</li><li>✓ Calendar Free/busy information with time, subject, and location</li></ul> <ul style="list-style-type: none"><li>✓ Everyone / specified security group (mail-enabled security group)</li></ul>
<b>Individual Sharing Policy</b>	<ul style="list-style-type: none"><li>✓ Sharing policies provide user-established, people-to-people sharing of both calendar and contact information with different types of external users.</li><li>✓ Sharing policies allow your users to share both their free/busy and contact information (including the Calendar and Contacts folders) with recipients in other external federated Exchange organizations.</li><li>✓ For recipients that aren't in an external federated organization or are in non-Exchange organizations, sharing policies allow people-to-people sharing of their calendar information with anonymous users through the use of Internet Calendar Publishing.</li></ul> <p>Three Options –</p> <ul style="list-style-type: none"><li>✓ Sharing with specific domain or all domain</li></ul> <p>There are three levels of access that you can specify:</p> <ul style="list-style-type: none"><li>✓ Free/busy information with time only</li><li>✓ Free/busy information with time, subject, and location</li><li>✓ Free/busy information, including time, subject, location, and title</li></ul> <ul style="list-style-type: none"><li>✓ Share your contacts folder</li></ul>

## W-2, D-5

3. What are the ways to Add or Remove Add-ins for organization?

<b>Add Add-ins</b>	There are three ways to add add-ins – <ul style="list-style-type: none"><li>I. Add from AppSource</li><li>II. Add from URL</li><li>III. Add from file</li></ul>
<b>Remove Add-ins</b>	<ul style="list-style-type: none"><li>✓ Please go to – <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a></li><li>✓ Please navigate to – <b>Organization &gt; add-ins &gt; select the add-in &gt; click recycle bin sign</b></li></ul>

4. What is mobile devices access in EAC > Mobile for?

5. What is mobile device mailbox policies?

<b>Mobile Device Access</b>	Default Exchange ActiveSync Access Settings -  <ul style="list-style-type: none"><li>I. Connection Settings – (Allow, Block, Quarantine-Decide later)<ul style="list-style-type: none"><li>✓ Allow synchronization with mobile devices that aren't managed by rules or personal exemptions.</li></ul></li><li>II. Quarantine Notification Email Message -<ul style="list-style-type: none"><li>✓ You haven't selected any administrators to receive quarantine email messages.</li></ul></li><li>III. Text to include in messages sent to users whose mobile device is in quarantine, blocked, or in the process of being identified:<ul style="list-style-type: none"><li>✓ No custom text is added to messages sent to users by Exchange ActiveSync</li></ul></li></ul>
<b>Mobile Device Mailbox Policies</b>	<ul style="list-style-type: none"><li>✓ Can create mobile device mailbox policies to apply a common set of policies or security settings to a collection of users.</li></ul> Different policy settings that can be applied – <ul style="list-style-type: none"><li>I. Allow simple passwords</li><li>II. Require an alphanumeric password</li><li>III. Require encryption on device</li><li>IV. Minimum password length</li><li>V. Number of sign-in failure before device is wiped</li><li>VI. Require sign-in after the device has been inactive for (minutes)</li><li>VII. Enforce password lifetime (days):</li><li>VIII. Password recycle count</li></ul>

## W-2, D-5

### 6. How to add or remove devices in Quarantine?

- ✓ Please go to – <https://outlook.office365.com/ecp>
- ✓ Please navigate to – **Mobile > mobile device access** > click mobile + sign

### 7. What is a public folder and public folder mailbox?

- ✓ Designed for shared access and provide an easy and effective way to collect, organize, and share information with other people in your workgroup or organization.
- ✓ Help organize content in a deep hierarchy that's easy to browse.
- ✓ Users will see the full hierarchy in Outlook, which makes it easy for them to browse for the content they're interested in.

There are two types of public folder mailboxes –

#### **Primary hierarchy mailbox:**

- ✓ Writable copy of the public folder hierarchy.
- ✓ Copied to all other public folder mailboxes, but these will be read-only copies.

#### **Secondary hierarchy mailboxes:**

- ✓ Contain public folder content as well and a read-only copy of the public folder hierarchy.

### 8. What is retention in Exchange Online?

<b>Retention</b>	<ul style="list-style-type: none"><li>✓ Applied to content or data to make sure we do not delete it before a specified date.</li><li>✓ For example, a contract might need to be kept for seven years to comply with a regulation. We would first need to identify the document as a contract, and then apply the contract retention policy, which would ensure we keep the contract for seven years.</li></ul>
------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## W-2, D-5

9. What are retention tags? How many types of retention tags are there? Explain briefly.

<b>Retention Tags</b>	<b>Retention tags:</b> <ul style="list-style-type: none"><li>✓ Apply retention settings to folders and individual items such as e mail messages and voice mail.</li><li>✓ This specify how long a message remains in a mailbox and the action to be taken when the message reaches the specified retention age.</li><li>✓ When a message reaches its retention age, it's moved to the user's In Place Archive or deleted.</li></ul>
<b>Types of Retention Tags</b>	<ul style="list-style-type: none"><li>✓ Default Policy Tag (DPT)<ul style="list-style-type: none"><li>○ Applied automatically to entire mailbox</li></ul></li><li>✓ Retention Policy Tag (RPT)<ul style="list-style-type: none"><li>○ Applied automatically to a default folder</li></ul></li><li>✓ Personal Tag (PT)<ul style="list-style-type: none"><li>○ Applied by users to items and folders</li></ul></li></ul>

10.How MRM works for retention Policy?

<b>MRM</b>	<ul style="list-style-type: none"><li>✓ Messaging Record Management</li><li>✓ Accomplished by using retention tags and retention policies.</li></ul>
<b>How it works</b>	<ol style="list-style-type: none"><li>Create Retention Tags (DPT, RPT, PT)</li><li>Create Retention Policies</li><li>Link Retention Policies to Retention Tags</li><li>Apply Retention Policies (to mailbox)</li><li>The Managed Folder Assistant Processes Mailbox<ol style="list-style-type: none"><li>Runs on mail servers</li><li>Applies retention settings on mailbox items</li><li>Takes retention action on specified time</li></ol></li></ol> <p>[N.B. From GUI it will take 7 days to apply the retention settings, by comparing with PowerShell which will affect immediately]</p> <ol style="list-style-type: none"><li>Mailbox Processed<ol style="list-style-type: none"><li>DPT &amp; RPT are applied to mailbox &amp; default folders</li><li>PT is available to Outlook client/OWA, from where users can apply</li></ol></li></ol>

## W-2, D-5

	Applied	Applied by	Available actions	Details
<b>Default Policy Tag (DPT)</b>	<ul style="list-style-type: none"> <li>✓ Automatically to entire mailbox</li> <li>✓ Applies to untagged items, which are mailbox items that don't have a retention tag applied directly or by inheritance from the folder.</li> </ul>	Administrator	<ul style="list-style-type: none"> <li>✓ Delete and allow recovery</li> <li>✓ Permanently delete</li> <li>✓ Move to archive</li> </ul>	<ul style="list-style-type: none"> <li>✓ Users can't change DPTs applied to a mailbox.</li> </ul>
<b>Retention Policy Tag (RPT)</b>	<ul style="list-style-type: none"> <li>✓ Automatically to a default folder</li> <li>✓ Default folders are folders created automatically in all mailboxes.</li> <li>✓ For example: <ul style="list-style-type: none"> <li>○ Inbox</li> <li>○ Drafts</li> <li>○ Sent Items</li> <li>○ Outbox</li> <li>○ Junk Email</li> <li>○ Deleted Items</li> <li>○ Archive</li> <li>○ Calendar</li> <li>○ RSS Feeds</li> </ul> </li> </ul>	Administrator	<ul style="list-style-type: none"> <li>✓ Delete and allow recovery</li> <li>✓ Permanently delete</li> </ul>	<ul style="list-style-type: none"> <li>✓ Users can't change the RPT applied to a default folder.</li> </ul>
<b>Personal Tag (PT)</b>	<ul style="list-style-type: none"> <li>✓ Manually to items and folders</li> <li>✓ Users can automate tagging by using Inbox rules to either move a message to a folder that has a particular tag or to apply a personal tag to the message.</li> </ul>	Users	<ul style="list-style-type: none"> <li>✓ Delete and allow recovery</li> <li>✓ Permanently delete</li> <li>✓ Move to archive</li> </ul>	<ul style="list-style-type: none"> <li>✓ Allow your users to determine how long an item should be retained.</li> <li>✓ For example, the mailbox can have a DPT to delete items in seven years, but a user can create an exception for items such as newsletters and automated notifications by applying a personal tag to delete them in three days.</li> </ul>

## W-2, D-5

### 11. What is MRM and How it works?

Messaging records management (MRM) is the records management technology in Exchange Server that helps organizations **manage email lifecycle** and **reduce the legal risks** associated with email.

Deploying MRM can help your organization in several ways:

- ✓ Meet Business Requirement
- ✓ Meet legal and regulatory requirements
- ✓ Increase user productivity
- ✓ Improve storage management

### 12. What are the actions you can take in retention policy?

Retention Action	DPT	I. Delete & Allow Recovery II. Permanently Delete III. Move to Archive
	RPT	I. Delete & Allow Recovery II. Permanently Delete
	PT	I. Delete & Allow Recovery II. Permanently Delete III. Move to Archive

### 13. Why multiple retention tags in one policy are not recommended to apply in retention policies?

They can contradict with each another.

### 14. How to assign retention policy to a user?

EAC > recipient > double click on the user > mailbox features > Mobile Devices > Disable/Enable Exchange Active Sync

### 15. How many days it will take to activate after assigning policy?

7-days from GUI and Immediately from PowerShell (Start-ManagedFolderAssistant -Identify <mailbox>)



## **W-2, D-5**

16.How to enable/disable Exchange Active Sync?

**EAC** > **recipient** > double click on the user > **mailbox features** > under Email Connectivity category **Retention policy** > select the policy > **Save** (take 7-days to apply)

## W-3, D-1

1. What is EOP? Explain the purpose of EOP.

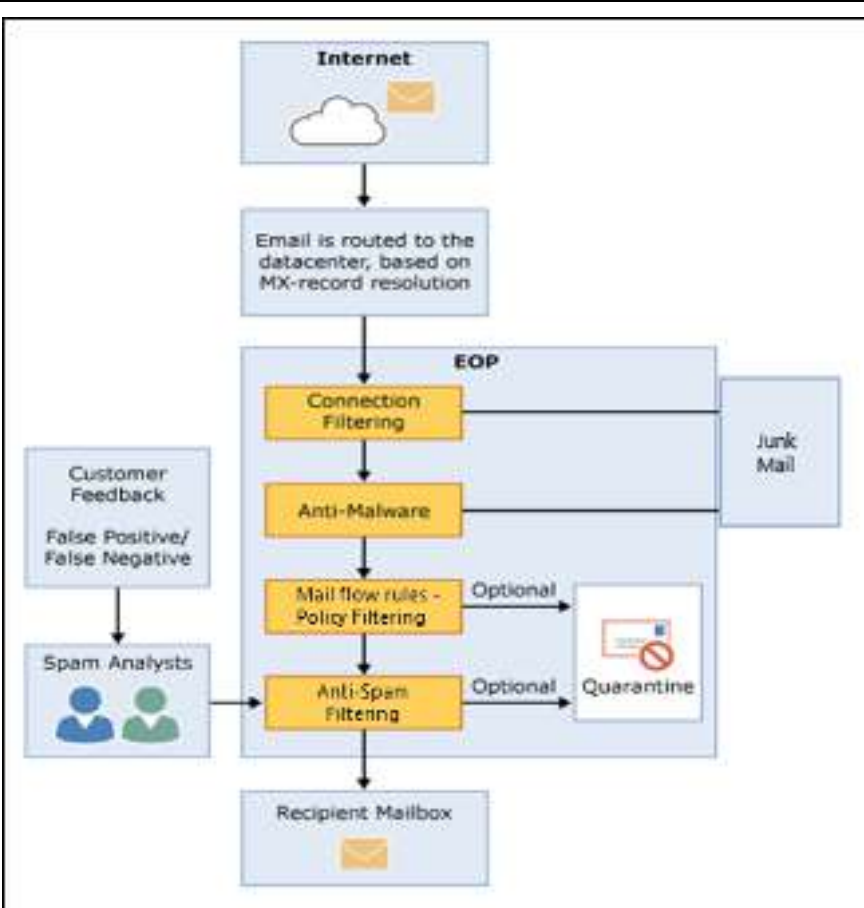
EOP	<ul style="list-style-type: none"><li>✓ EOP stands for Exchange Online Protection</li><li>✓ Exchange Online Protection (EOP) is the cloud-based filtering service that helps protect your organization against spam and malware.</li><li>✓ EOP is included in all Microsoft 365 organizations with Exchange Online mailboxes.</li></ul>
Purpose of EOP	<ul style="list-style-type: none"><li>✓ Inbound spam detection</li><li>✓ Outbound spam detection</li><li>✓ Backscatter protection</li><li>✓ Bulk mail filtering</li><li>✓ Malicious URL block-lists</li><li>✓ Anti-phishing protection</li><li>✓ Anti-spoofing protection</li></ul>

2. What does EOP protect and filter Microsoft 365 inbound mail?

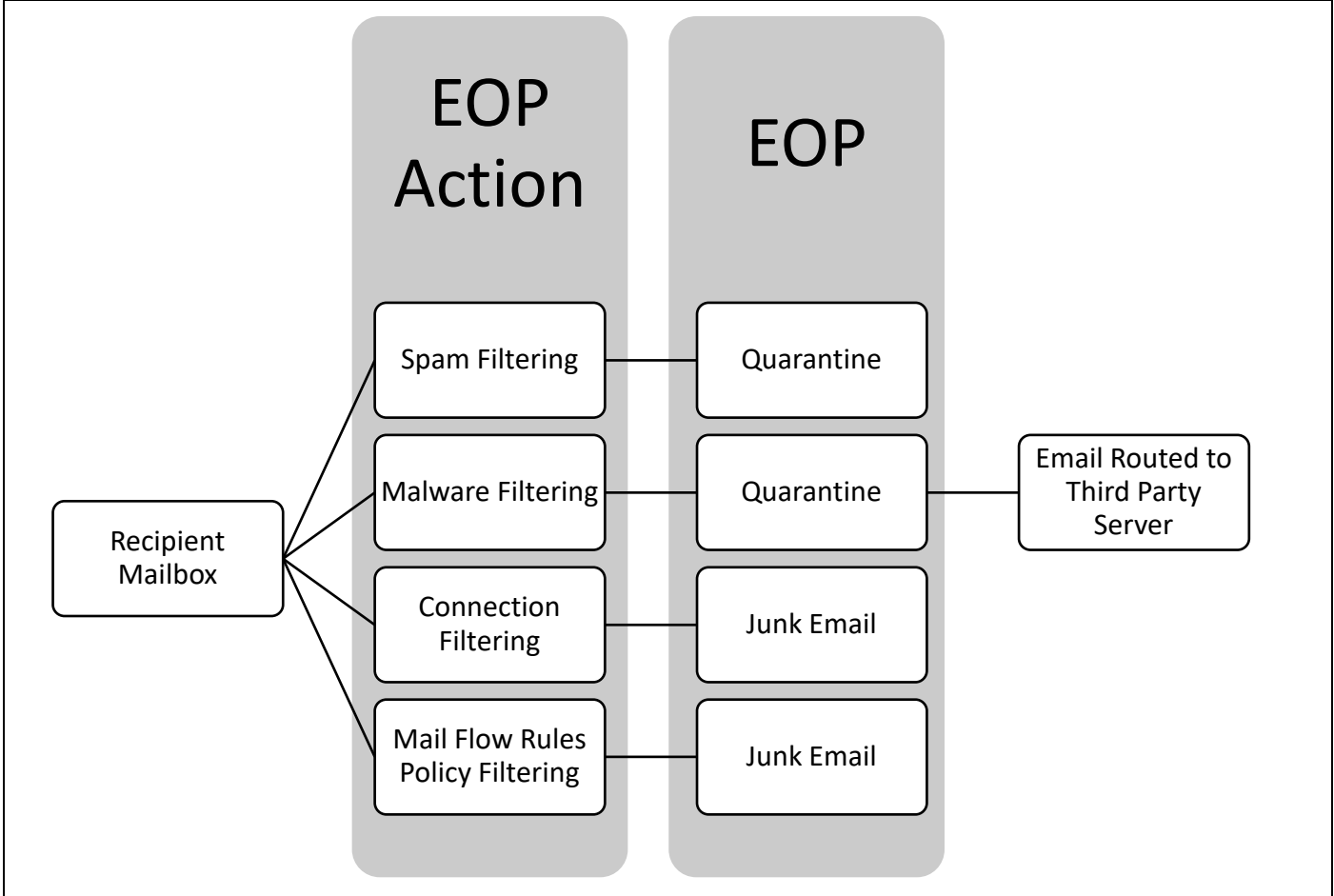
EOP for Inbound Email
<ol style="list-style-type: none"><li>I. Initially, email messages are routed to the data center based on MX-record resolution.</li><li>II. Incoming message initially passes through <b>Connection Filtering &amp; Malware Filtering</b> which checks the sender's reputation and inspects the message for malware. The majority of spam is stopped at this point and deleted by EOP and send the email to Junk Email.</li><li>III. Messages continue through <b>Mail flow rules policy filtering</b>, where messages are evaluated against custom mail flow rules/transport rules that have been created or enforced from a template. For example, you can have a rule that sends a notification to a manager when mail arrives from a specific sender. Data loss prevention (DLP) checks also occur at this point.</li><li>IV. Next, messages pass through <b>Spam Filtering</b>. A message that's determined to be spam can be sent to a user's Junk Email folder or the quarantine, among other options.</li><li>V. After a message passes all of these protection layers successfully, it's delivered to the recipient.</li><li>VI. Customers can give feedback whether the messages are False Positive or False Negative.</li></ol>

W-3, D-1

Overall Scenario  
for EOP of  
Inbound Email



EOP for Outbound Email



## W-3, D-1

3. How does Malware filtering work? How to block any attachment in inbound mail?

<b>Malware Filtering</b>	<ul style="list-style-type: none"><li>✓ Built-in Function -<ul style="list-style-type: none"><li>○ EOP provides built-in malware and spam filtering capabilities that help protect inbound and outbound messages from malicious software and help protect the network from spam transferred through email.</li><li>○ Admins do not need to set up or maintain the filtering technologies, which are enabled by default. However, admins can make company-specific filtering customizations.</li></ul></li><li>✓ Custom Function –<ul style="list-style-type: none"><li>○ EOP offers multilayered protection that's designed to catch all known malware.</li><li>○ Messages transported through the service are scanned for malware (viruses and spyware). If malware is detected, the message is deleted.</li><li>○ Notifications may also be sent to senders or admins when an infected message is deleted and not delivered.</li><li>○ You can also choose to replace infected attachments with either default or custom messages that notify the recipients of the malware detection.</li></ul></li></ul>
<b>Custom Settings</b>	<ul style="list-style-type: none"><li>I. Malware Detection Response</li><li>II. Common Attachment Types Filter</li><li>III. Malware Zero-hour Auto Purge</li><li>IV. Notifications</li><li>V. Administrator Notifications</li><li>VI. Customize Notifications</li></ul>
<b>Block Attachment in Inbound Email for All users</b>	
<p>Please go to – <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a></p> <p>Please navigate to –</p> <p>① <b>protection</b> &gt; ② <b>malware filter</b> &gt; ③ double click on the <b>Default</b> &gt; ④ <b>settings</b> &gt; ⑤ Under <b>Common Attachment Types Filter</b>, choose <b>on</b> &amp; select any file type that you want to block &gt; ⑥ press <b>Save</b></p>	

## W-3, D-1

### 4. How to block or allow any IP?

Allow or Block IP for All users	
Please go to – <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a>	
Please navigate to –	
① <b>protection</b> > ② <b>connection filter</b> > ③ double click on the <b>Default</b> > ④ <b>connection filtering</b> > ⑤ By clicking “+” sign you can allow or block IP/IP ranges > ⑥ press <b>Save</b>	
<b>Enable Safe list</b>	This is the list of trusted partners. By checking you are allowing all IP’s from trusted partners of Microsoft. It will never be detected as spam.

### 5. How to block or allow any sender or domain? How long messages are retained in quarantine by default? Is the duration changeable?

Block or Allow Sender or Domain for all users	
Please go to – <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a>	
Please navigate to –	
① <b>protection</b> > ② <b>spam filter</b> > ③ double click on the <b>Default</b> > ④ <b>block lists</b> > ⑤ By clicking “+” sign you can block sender or domain > ⑥ press <b>Save</b>	
In the very next option <b>allow lists</b> – by clicking “+” sign you can also allow sender or domain	
How long messages are retained in quarantine by default -  <b>15 Days (max 30 days)</b>	
Change the Duration	
Please go to – <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a>	
Please navigate to –	
① <b>protection</b> > ② <b>spam filter</b> > ③ double click on the <b>Default</b> > ④ <b>spam and bulk actions</b> > ⑤ Under <b>Quarantine</b> , please type the desired dasys in <b>Retain Spam for (days)</b> > ⑥ press <b>Save</b>	

## W-3, D-1

### 6. How to filter messages based on language or country or regions?

#### Filter Messages Based on Language or Country for all Users

Please go to – <https://outlook.office365.com/ecp>

Please navigate to –

① **protection** > ② **spam filter** > ③ double click on the **Default** > ④ **international spam** > ⑤ Check the box for enabling filter for languages & countries and select the languages and countries that you would like to block > ⑥ press **Save**

### 7. Explain the different ways of mail auto-forwarding.

#### Mail Auto Forwarding from EAC

Please go to – <https://outlook.office365.com/ecp>

Please navigate to –

① **recipients** > ② **mailboxes** > ③ double click on the user mailbox that you want to enable the Mail Auto Forwarding > ④ **mailbox features** > ⑤ Under the **Mail Flow category, Delivery Options** click **View details**

⑥ **Enable forwarding** > ⑦ if you want to keep a copy of that email to the mailbox please check this, otherwise leave it > ⑧ **Browse** > ⑨ select the forwarding email > press **OK**

From now on, if anyone sends an email to that user, that email message will be forwarded to forwarding email.

#### Mail Auto Forwarding from OWA

Please go to – <https://outlook.office365.com>

Please navigate to – ① **settings** (gear sign) > ② **View all Outlook settings**

③ **Mail** > ④ **Forwarding** > ⑤ **Enable forwarding** & write down the email where you want to forward > ⑥ if you want to keep a copy of that email to the mailbox please check this, otherwise leave it > ⑦ press **Save**

## W-3, D-1

Mail Auto Forwarding from Outlook Client	
Please open Outlook Client.	
Please navigate to – ① <b>Rules</b> > ② <b>Create Rule</b>	
Please press – ③ <b>Advanced Options</b>	
④ please select any condition > ⑤ change the parameter accordingly by clicking this > ⑥ press <b>Next</b>	
⑦ select <b>forward it to people or public group</b> > change the forwarding email accordingly by clicking this > ⑨ press <b>Next</b>	
Please press <b>Next</b> again	
Press <b>Finish</b> to save the rule. This rule will work as Auto Forwarding.	

### 8. How to Analyze Message Header.

<b>Message Header from OWA</b>	✓ <a href="https://outlook.office365.com">https://outlook.office365.com</a> > select the message > right click on the message > <b>view message details</b>
<b>Message Header from Outlook Client</b>	✓ Open outlook client > double click on the message > <b>File</b> > <b>Properties</b> > <b>Internet Headers</b>

### 9. What is spam confidence level (SCL)?

SCL	Definition	Default action
-1	<ul style="list-style-type: none"> <li>✓ The message skipped spam filtering.</li> <li>✓ For example, the message is from a safe sender, was sent to a safe recipient, or is from an email source server on the IP Allow List</li> </ul>	Deliver the message to the recipients' inbox.
0, 1	✓ Spam filtering determined the message was not spam.	Deliver the message to the recipients' inbox.
5, 6	✓ Spam filtering marked the message as Spam	Deliver the message to the recipients' Junk Email folder.
9	✓ Spam filtering marked the message as High confidence spam	Deliver the message to the recipients' Junk Email folder.

## W-3, D-1

10.Explain the features of EAC Protection.

Protection (MaCoS)	malware filter	<ul style="list-style-type: none"> <li>✓ Default</li> <li>✓ Custom (+)</li> </ul>	<div>Settings</div> <div>Applied to (only for Custom)</div>	<ul style="list-style-type: none"> <li>✓ Malware Detection Response (Inform the Recipient)</li> <li>✓ Common attachment Types Filter</li> <li>✓ Malware Zero Hour Auto Purge</li> <li>✓ Notification (Sender/Administrator)</li> </ul> <ul style="list-style-type: none"> <li>✓ Recipient</li> <li>✓ Domain</li> </ul>
	connection filter	Default	Connection filtering	<div>IP Allow List</div> <div>IP Block List</div> <div>Enable Safe List (trusted senders IP list)</div>
	spam filter	<ul style="list-style-type: none"> <li>✓ Default</li> <li>✓ Custom (+)</li> </ul>	Spam and Bulk Actions	<ul style="list-style-type: none"> <li>✓ Spam (what to do – move junk email)</li> <li>✓ High Confidence Spam (what to do – move junk email)</li> <li>✓ Bulk Email (7 Default)</li> <li>✓ Quarantine (15 Default/30 Max)</li> </ul>
			Block lists	<ul style="list-style-type: none"> <li>✓ Sender</li> <li>✓ Domain</li> </ul>
			Allow Lists	<ul style="list-style-type: none"> <li>✓ Sender</li> <li>✓ Domain</li> </ul>
			International spam	<ul style="list-style-type: none"> <li>✓ Language</li> <li>✓ Country or Region</li> </ul>
			Advanced options	<ul style="list-style-type: none"> <li>✓ SPF</li> <li>✓ NDR</li> <li>✓ .....</li> <li>✓ Test Mode Option</li> </ul>
			Applied to (only for Custom)	<ul style="list-style-type: none"> <li>✓ Recipient</li> <li>✓ Domain</li> </ul>
	outbound filter			
	quarantine	(All Quarantine Messages)		
	action center			
	dkim	(Accepted Domain list)	<ul style="list-style-type: none"> <li>✓ Enable</li> <li>✓ Disable</li> </ul>	



## W-3, D-2

1. What are the actions towards an email when it is marked as spam? How can an end user find the quarantined emails back?

<b>Actions towards an email when it is marked as spam</b>	Move message to the junk email folder - <ul style="list-style-type: none"><li>✓ Add X-header</li><li>✓ Prepend subject line with text</li><li>✓ Redirect message to the email address</li><li>✓ Delete message</li><li>✓ Quarantine message</li></ul>
-----------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Quarantine Email Retrieve by End-user
<ul style="list-style-type: none"><li>✓ Please go to – <a href="https://protection.office.com">https://protection.office.com</a></li><li>✓ Please navigate to – <b>Threat management &gt; Review</b></li><li>✓ Here, you will find a list of Quarantine message from where you can retrieve the message.</li></ul>

2. How to get message header from Outlook & OWA?


Message Header from Outlook Client
<ul style="list-style-type: none"><li>✓ Please open Outlook Client and select the inbox message, which you would like to check the message header.</li></ul>
<ul style="list-style-type: none"><li>✓ Double click on that message</li></ul>
<ul style="list-style-type: none"><li>✓ Please click <b>Properties</b></li></ul>
<ul style="list-style-type: none"><li>✓ There you will find one box named – <b>Internet headers</b></li><li>✓ This is the message header of that particular message. You can copy from here.</li></ul>
Message Header from OWA
<ul style="list-style-type: none"><li>✓ Please go to – <a href="https://outlook.office365.com">https://outlook.office365.com</a></li><li>✓ Select and right click on the inbox message, which you would like to check the message header.</li><li>✓ Please click <b>View message details</b></li></ul>
<ul style="list-style-type: none"><li>✓ This is the message header of that particular message. You can copy from here.</li></ul>

## W-3, D-2

3. What will happen to the message header if the email was marked as spam by advanced spam filter options?

<b>Message Header for ASF</b>	<p>Enabling one or more of the ASF settings is an aggressive approach to spam filtering. You can't report messages that are filtered by ASF as false positives. ASF add extra field of X-CustomSpam if the message was detected by ASF.</p> <p>✓ <b>The specific X-CustomSpam:</b> X-header fields that are added to messages as described in this topic.</p>
-------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

4. What are DKIM and DMARC?

DKIM	
<ul style="list-style-type: none"><li>✓ Domain Keys Identified Mail (DKIM)</li><li>✓ Ensure that destination email systems trust messages sent outbound from the custom domain.</li><li>✓ You should use DKIM in addition to SPF and DMARC to help prevent spoofers from sending messages that look like they are coming from your domain.</li><li>✓ DKIM lets you add a digital signature to outbound email messages in the message header.</li><li>✓ A private key is used to encrypt the header in your domain's outgoing email and then publish a public key to the domain's DNS records that receiving servers can then use to decode the signature. They use the public key to verify that the messages are really coming from you and not coming from someone spoofing your domain.</li><li>✓ Microsoft 365 automatically sets up DKIM for its initial onmicrosoft.com domain.</li></ul>	
<ul style="list-style-type: none"><li>✓ At first case, DKIM and SPF both have passes as the email comes from authorized mail server.</li><li>✓ At second case, DKIM have passed because it relies on public key cryptography to authenticate and not just IP addresses,</li></ul>	
 <p>The diagram illustrates two scenarios of email authentication. In the first scenario, a message is sent from the Contoso.com Mail server (IP address #1) to the Woodgrovebank.com Mail server. The message has a DKIM signature, and both SPF and DKIM checks pass. In the second scenario, a message is sent from the Woodgrovebank.com Mail server (IP address #25) to the Outlook.com Mail server. The message has a DKIM signature, but the SPF check fails while the DKIM check passes.</p>	

## W-3, D-2

### DMARC

- ✓ Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- ✓ Works with SPF and DKIM to authenticate mail senders and ensure that destination email systems trust messages sent from your domain.
- ✓ Implementing DMARC with SPF and DKIM provides additional protection against spoofing and phishing email.
- ✓ DMARC helps receiving mail systems determine what to do with messages sent from your domain that fail SPF or DKIM checks.

### How DMARC works for Outbound Message

- ✓ **Mail From" address:** Identifies the sender and specifies where to send return notices if any problems occur with the delivery of the message, such as non-delivery notices. This appears in the envelope portion of an email message and is not usually displayed by your email application. This is sometimes called the **5321.MailFrom address** or the **reverse-path address**.
- ✓ **"From" address:** The address displayed as the From address by your mail application. This address identifies the author of the email. That is, the mailbox of the person or system responsible for writing the message. This is sometimes called the **5322.From address**.
- ✓ SPF uses a DNS TXT record to provide a list of authorized sending IP addresses for a given domain. Normally, SPF checks are only performed against the 5321.MailFrom address. This means that the 5322.From address is not authenticated when you use SPF by itself. This allows for a scenario where a user can receive a message which passes an SPF check but has a spoofed 5322.From sender address. Here DMARC check fail and detected the message as spam but spf fail to detect as SPF only checks 5321.Mail From Address.

text

```
S: Helo woodgrovebank.com
S: Mail from: phish@phishing.contoso.com
S: Rcpt to: astobes@tailspintoys.com
S: data
S: To: "Andrew Stobes" <astobes@tailspintoys.com>
S: From: "Woodgrove Bank Security" <security@woodgrovebank.com>
S: Subject: Woodgrove Bank - Action required
S:
S: Greetings User,
S:
S: We need to verify your banking details.
S: Please click the following link to verify that we have the right information for your account.
S:
S: https://short.url/woodgrovebank/updateaccount/12-121.aspx
S:
S: Thank you,
S: Woodgrove Bank
S: ,
```

## W-3, D-2

### How DMARC works for Inbound Message

- ✓ If you configured SPF, then the receiving server performs a check against the Mail from address phish@phishing.contoso.com. If the message came from a valid source for the domain phishing.contoso.com then the SPF check passes. Since the email client only displays the From address, the user sees that this message came from security@woodgrovebank.com. With SPF alone, the validity of woodgrovebank.com was never authenticated.
- ✓ When you use DMARC, the receiving server also performs a check against the From address. In the example above, if there is a DMARC TXT record in place for woodgrovebank.com, then the check against the From address fails.

### 5. Set up DKIM with your tenant.

<p>1. <b>Publish CNAME</b> records in the Custom Domain in <b>DNS Management</b></p> <p>[N.B. to get the domainGUID you need to find MX records and get the mail server]</p>	<ul style="list-style-type: none"> <li>✓ <b>Host name:</b> selector1._domainkey <b>Value:</b> selector1-&lt;domainGUID&gt;._domainkey.&lt;initialDomain&gt; <b>TTL:</b> 3600</li> <li>✓ <b>Host name:</b> selector2._domainkey <b>Points to address or value:</b> selector2-&lt;domainGUID&gt;._domainkey.&lt;initialDomain&gt; <b>TTL:</b> 3600</li> </ul>
<p>2. <b>Enable DKIM</b></p>	<ul style="list-style-type: none"> <li>✓ Please go to – <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a></li> <li>✓ Please navigate to – ① <b>protection</b> &gt; ② <b>dkim</b> &gt; ③ select the custom domain &gt; ④ <b>Enable</b></li> <li>✓ Now, DKIM is enabled.</li> </ul>

### 6. How to enable DMARC.

<p>1. <b>Identify</b> valid sources of mail for your domain</p>	<ul style="list-style-type: none"> <li>✓ If you have already set up SPF then you have already gone through this exercise. However, for DMARC, there are additional considerations. When identifying sources of mail for your domain there are two questions you need to answer: <ul style="list-style-type: none"> <li>○ What IP addresses send messages from my domain?</li> <li>○ For mail sent from third parties on my behalf, will the 5321.MailFrom and 5322.From domains match?</li> </ul> </li> </ul>
<p>2. Set up <b>SPF</b> for your domain</p>	<ul style="list-style-type: none"> <li>✓ Update the SPF records according to the IP address.</li> </ul>

## W-3, D-2

3. Set up <b>DKIM</b> for your custom domain	<ul style="list-style-type: none"> <li>✓ Publish given DKIM CNAME records in the DNS Management of the DNS hosting provider.</li> <li>✓ Enable DKIM from EAC protection.</li> </ul>
4. Update <b>DMARC</b> TXT record in the DNS management	<ul style="list-style-type: none"> <li>✓ <code>_dmarc.&lt;domain&gt; TTL IN TXT "v=DMARC1; p=policy; pct=100"</code></li> <li>✓ domain is the domain you want to protect. By default, the record protects mail from the domain and all subdomains. For example, if you specify <code>_dmarc.contoso.com</code>, then DMARC protects mail from the domain and all subdomains, such as <code>housewares.contoso.com</code> or <code>plumbing.contoso.com</code>.</li> <li>✓ TTL should always be the equivalent of one hour. The unit used for TTL, either hours (1 hour), minutes (60 minutes), or seconds (3600 seconds), will vary depending on the registrar for your domain.</li> <li>✓ pct=100 indicates that this rule should be used for 100% of email.</li> <li>✓ policy specifies what policy you want the receiving server to follow if DMARC fails. You can set the policy to <b>none</b>, <b>quarantine</b>, or <b>reject</b>.</li> </ul>

### 7. How would EOP check and deal with DKIM authentication result?

Dealing with DKIM by EOP for Inbound message	
✓	Exchange Online Protection (EOP) and Exchange Online support inbound validation of DKIM messages.
✓	DKIM is a method for validating that a message was sent from the domain it says it originated from and that it was not spoofed by someone else. It ties an email message to the organization responsible for sending it. DKIM verification is automatically used for all messages sent over IPv6 communications.
✓	Microsoft 365 also now supports DKIM when mail is sent over IPv4.
✓	DKIM validates a digitally signed message that appears in the DKIM-Signature header in the message headers. The result of a DKIM-Signature validation is stamped in the Authentication-Results header which conforms with <b>RFC 7001</b> (Message Header Field for Indicating Message Authentication Status).
✓	Authentication-Results: <code>&lt;domain&gt;; dkim=pass (signature was verified) header.d=example.com</code>

## W-3, D-2

### Dealing with DKIM by EOP for Outbound message

- ✓ DKIM lets you add a digital signature to outbound email messages in the message header.
- ✓ SPF adds information to a message envelope but DKIM actually encrypts a signature within the message header. When you forward a message, portions of that message's envelope can be stripped away by the forwarding server. Since the digital signature stays with the email message because it's part of the email header.

#### Example of DKIM and SPF work together:

- ✓ In this example, if you had only published an SPF TXT record for your domain, the recipient's mail server could have marked your email as spam and generated a false positive result. The addition of DKIM in this scenario reduces false positive spam reporting. Because DKIM relies on **public key cryptography** to authenticate and not just IP addresses, DKIM is considered a much stronger form of authentication than SPF. We recommend using both SPF and DKIM, as well as DMARC in your deployment.
- ✓ DKIM uses a **private key** to insert an encrypted signature into the message headers. The signing domain, or outbound domain, is inserted as the value of the **d= field in the header**. The verifying domain, or recipient's domain, then use the d= field to look up the public key from DNS and authenticate the message. If the message is verified, the DKIM check passes.



#### 8. What is SPF? Why do we need SPF?

- ✓ SPF is an email authentication system, which indicates that users are sending from an authorized mail server.
- ✓ An SPF TXT record is a DNS record that helps prevent spoofing and phishing by verifying the domain name from which email messages are sent.
- ✓ SPF validates the origin of email messages by verifying the IP address of the sender against the alleged owner of the sending domain.

## W-3, D-2

### 9. What is email authentication/email validation system?

- ✓ Email authentication is a group of standards that tries to stop spoofing (email messages from forged senders).
- ✓ In Microsoft 365 organizations with mailboxes in Exchange Online, and standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, EOP uses these standards to verify inbound email:
  - SPF (Sender Policy Framework)
  - DKIM (Domain Keys Identified Mail)
  - DMARC (Domain based Message Authorization, Reporting & Conformance)

### 10. What is SPF enforcement rule for the last segment?

- ✓ **-all**
  - Indicates hard fail.
  - If you know all of the authorized IP addresses for your domain, list them in the SPF TXT record and use the -all (hard fail) qualifier.
  - Also, if you are only using SPF, that is, you are not using DMARC or DKIM, you should use the -all qualifier.
  - Recommended to use always this qualifier.
- ✓ **~all**
  - Indicates soft fail.
  - If you're not sure that you have the complete list of IP addresses, then you should use the ~all (soft fail) qualifier.
  - Also, if you are using DMARC with p=quarantine or p=reject, then you can use ~all. Otherwise, use -all.
- ✓ **?all**
  - Indicates neutral.
  - This is used when testing SPF.
  - Not recommended to use this qualifier in your live deployment.

### 11. Explain the SPF record with Example.

- ✓ **v=spf1 ip4:192.168.0.1 ip4:192.168.0.2 include:spf.protection.outlook.com -all**
  - **v=spf1** is required.
  - **ip4** indicates that you are using IP version 4 addresses. **ip6** indicates that you are using IP version 6 addresses. If you are using **ip6** IP addresses, replace ip4 with ip6 in the examples in this article. You can also specify IP address ranges using CIDR notation, for example ip4:192.168.0.1/26.
  - IP address is the IP address that you want to add to the SPF TXT record. Usually, this is the IP address of the outbound mail server for your organization. You can list multiple outbound mail servers.
  - domain name is the domain you want to add as a legitimate sender.

## W-3, D-2

- If you are fully using EXO then the SPF record will be – **v=spf1 include:spf.protection.outlook.com -all**

12.What is initial domain? Do we need to set up SPF, DKIM, DMARC for initial domain?

- ✓ The domain I got when I register in the tenant is known as initial domain. (onmicrosoft.com)
- ✓ For initial domain, you don't need to set up these email authentication systems. SPF, DKIM, DMARC are required for custom domain after adding the domain in the tenant.

13.Which type of records are SPF, DKIM, DMARC?

Email Authentication	DNS Record Type	When to Add in DNS Management	Process
SPF	TXT	During adding Domain Process (in step-2)	✓ Publish SPF record in DNS Management of Domain provider
DKIM	CNAME	During DKIM Enable	✓ <b>Publish</b> two CNAME records in DNS Management of Domain provider ✓ <b>Enable</b> from <b>Protection &gt; dkim</b>
DMARC	TXT	After SPF & DKIM Set Up	✓ Check all <b>IP</b> from my email server ✓ Update <b>SPF</b> record ✓ <b>DKIM</b> set up ✓ Publish <b>DMARC</b> records in DNS Management of Domain provider

14.How to get Domain GUID?

- ✓ Domain GUID is the same as the MX record for your custom domain that appears before mail.protection.outlook.com. For example, MX record for the domain contoso.com is **contoso-com.mail.protection.outlook.com**, the domainGUID is then **contoso-com**.



## W-3, D-3

### 1. What is the Transport Rule? What are the components of transport Rule?

<b>Mail Flow Rules or Transport Rules</b>	<ul style="list-style-type: none"><li>✓ Similar to the Inbox rules that are available in Outlook and Outlook on the web.</li><li>✓ The main difference is mail flow rules take action on messages while they're in transit, and not after the message is delivered to the mailbox.</li><li>✓ Mail flow rules contain a richer set of conditions, actions &amp; exceptions, which provides the flexibility to implement many types of messaging policies.</li></ul>
<b>Components of Transport Rule</b>	<ul style="list-style-type: none"><li>✓ <b>Conditions:</b> Identify the messages that you want to apply the actions to. If there are no conditions or exceptions, the rule is applied to all messages.</li><li>✓ <b>Actions:</b> Specify what to do to messages that match the conditions in the rule, and don't match any of the exceptions. There are many actions available, such as rejecting, deleting, or redirecting messages, adding additional recipients, adding prefixes in the message subject, or inserting disclaimers in the message body.</li><li>✓ <b>Exceptions:</b> Optionally identify the messages that the actions shouldn't apply to. The same message identifiers that are available in conditions are also available in exceptions. Exceptions override conditions and prevent the rule actions from being applied to a message, even if the message matches all of the configured conditions.</li><li>✓ <b>Properties:</b> Specify other rules settings that aren't conditions, exceptions or actions. For example, when the rule should be applied, whether to enforce or test the rule and the period when the rule is active.</li></ul>

## W-3, D-3

### 2. How to encrypt a message?

When you need to protect the privacy of an email message, encrypt it. Encrypting an email message in Outlook means it's converted from **readable plain text** into **scrambled cipher text**. Only the recipient who has the **private key** that matches the **public key** used to encrypt the message can **decipher** the message for reading. Any recipient without the corresponding private key, however, sees **indecipherable** text. Outlook supports two encryption options:

- ✓ **S/MIME encryption** - To use S/MIME encryption, the sender and recipient must have a mail application that supports the S/MIME standard. Outlook supports the S/MIME standard
- ✓ **Microsoft 365 Message Encryption (Information Rights Management)** - To use Microsoft 365 Message Encryption, the sender must have Microsoft 365 Message Encryption, which is included in the **Office 365 Enterprise E3 license**.

#### Encrypt a Message for Single User from Outlook Client

- ✓ Please open outlook client
- ✓ Please navigate to –  
① **New Email** > ② **File** > ③ **Properties** > ④ **Security Settings** > ⑤ Check on - **Encrypt Message Contents & Attachments** > ⑥ press **OK**

#### Encrypt all Outbound Messages from Outlook Client

- ✓ Please open outlook client
- ✓ Please navigate to – **File** > **Option** > **Trust Center** > **Trust Center Settings** > **Email Security** > Check on – **Encrypt contents & attachments for outgoing messages**

### 3. How to apply disclaimers?

#### An Example of Disclaimer

- ✓ A climate change scientist writing an editorial or opinion piece that involves the topic of climate change may include a disclaimer saying that the opinions are his own and not that of his employer.

- ✓ Please go to – <https://outlook.office365.com/ecp>
- ✓ Please navigate to – ① **mail flow** > ② **rules** > ③ click “+” > ④ **Apply disclaimers**

- ✓ Then –  
⑤ type a suitable name  
⑥ **Apply the rule if** such as **the sender is located** - **inside the organization**  
⑦ **Do the following** such as **forward the message for approval to** – a mailbox  
⑧ **Except if** required.  
⑨ Set **Audit this rule with severity level**

At last, **choose a mode for this rule**, Select **Enforce** to turn on the disclaimer immediately, or select **Test without Policy Tips** to put a message in the message tracking log instead of adding the disclaimer.

- ⑩ Press **Save**

## W-3, D-3

4. How to bypass spam filtering? In which scenarios we must bypass EOP filtering?

✓ Please go to – <https://outlook.office365.com/ecp>

✓ Please navigate to – ① **mail flow** > ② **rules** > ③ click “+” > ④ **Bypass spam filtering**

✓ Then –

⑤ **Apply the rule if** such as **the sender is located - inside the organization**

⑥ **Do the following** such as **Set the spam confidence level (SCL) to – a mailbox**

⑦ **Except if required.**

⑧ Set **Audit this rule with severity level**

⑨ At last, **choose a mode for this rule**, Select **Enforce** to turn on immediately, or select **Test without Policy Tips** to put a message in the message tracking log instead of adding the rule.

⑩ Press **Save**

### Scenarios to Bypass EOP Filtering

- ✓ To bypass spam filtering in Office 365 for clean mail that is being sent from any trusted organization or person.
- ✓ In most cases, email passing through external organizations/persons and then double scanned by Office 365 will cause issues.
- ✓ Although not critical, in most scenarios, the double scan will result in legitimate emails being dumped into the Outlook junk folder. This can be avoided with a simple bypass filter.
- ✓ When we are supposed to work with third party webserver in that case mainly bypass filter needs. Like by using the IP allow list you are allowing all email from that web server's IP address to bypass your spam filters. In effect, you're trusting the web hosting company to prevent other customers who are also on the shared hosting server from spamming or phishing your users. It's unlikely that the web hosting company will be able to prevent that. Furthermore, any insecurity in the web form itself could lead to abuse.
- ✓ So, to enhance your protection without opening yourself up to a new risk, you can use a mail flow rule instead. The mail flow rule is configured to ensure that mail from the web server is still subject to spam filtering if it doesn't have the specific characteristics of the sales contact form emails.

## W-3, D-3

### 5. What is EOP trace?

<b>EOP Trace</b>	<ul style="list-style-type: none"><li>✓ Offers many different reports that can help to determine the overall status and health of your organization. Some reports are available in the Microsoft 365 admin center, while others are available in the Exchange admin center (EAC).</li><li>✓ The message trace feature in the EAC lets you, as an administrator, follow email messages as they pass through the EOP.</li><li>✓ Helps to determine whether a targeted email message was <b>received</b>, <b>rejected</b>, <b>deferred</b>, or <b>delivered</b> by the service.</li><li>✓ Shows what <b>actions</b> have occurred to the message before reaching its final status.</li><li>✓ <b>Obtaining detailed information</b> about a specific message lets you efficiently answer your user's questions, troubleshoot mail flow issues, validate policy changes, and alleviates the need to contact technical support for assistance.</li></ul>
------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 6. How to do message trace in EAC?

<ul style="list-style-type: none"><li>✓ Please go to – <a href="https://outlook.office365.com/ecp">https://outlook.office365.com/ecp</a></li><li>✓ Please navigate to – <b>mail flow &gt; message trace</b></li></ul>
<ol style="list-style-type: none"><li>1. <b>Date range</b> – Select <b>Custom</b> to get the report</li><li>2. <b>Time zone</b> - Select your local timezone</li><li>3. <b>Start/End Date &amp; Time</b> - The difference must be greater than 7 days to get the report (#8 option)</li><li>4. <b>Delivery Status</b> - Choose any – All, Delivered, Failed, Expanded</li><li>5. <b>Message ID</b> - Possible to get from MHA</li><li>6. <b>Sender</b> - Mailbox or wildcard</li><li>7. <b>Recipient</b> - Mailbox or wildcard</li><li>8. <b>Include message events and routing details with report</b> - Check this</li><li>9. <b>Report title</b> - Set a suitable report name</li><li>10. <b>Notification email address</b> - Email address where the report will be sent (inside organization mailbox)</li><li>11. Press <b>Search</b></li></ol>
You will see a prompt window that your <b>message trace has been submitted</b> . It will take some time to generate the report.

## W-3, D-3

7. What is the accepted domain? Define all type of accepted domains.

Accepted Domain	<ul style="list-style-type: none"><li>✓ SMTP name spaces (also known as address spaces) that are configured in an Exchange organization to receive email messages.</li><li>✓ For example, my company registered the domain contoso.com, and you configured a mail exchanger (MX) record in your Internet DNS for contoso.com, you need to configure contoso.com as an accepted domain in your Exchange organization to accept messages that are addressed to @contoso.com recipients.</li></ul>
Types of Accepted Domain	<ul style="list-style-type: none"><li>✓ <b>Authoritative domains:</b><ul style="list-style-type: none"><li>○ Recipients (in particular, mailboxes) are configured with email addresses in these domains.</li><li>○ The Exchange organization accepts messages that are addressed to recipients in these domains and is responsible for generating non-delivery reports (also known as NDRs or bounce messages) for non-existent recipients.</li></ul></li><li>✓ <b>Relay domains:</b><ul style="list-style-type: none"><li>○ The Exchange organization accepts messages that are addressed to recipients in relay domains but aren't responsible for generating NDRs for non-existent recipients.</li><li>○ Instead, Exchange (with additional configuration) relays the messages to messaging servers that are external to the Exchange organization.</li><li>○ Relay domains can be internal (for domains that you control) or external (for domains that you don't control).</li></ul></li></ul>

8. What is Remote domain? Which features are included in Remote domain?

	<ul style="list-style-type: none"><li>✓ <b>Organizational setting</b> that allows controlling certain message types such as “Out of Office” and “Non-Delivery Reports”.</li><li>✓ In 4 cases we may need a remote domain –<ul style="list-style-type: none"><li>i. Don't allow to forward messages to recipients in other domains.</li><li>ii. You work with an organization that you don't want to receive automatic messages.</li><li>iii. You have a business partner that's outside your organization, and you'd like that partner to receive the same out-of-office replies as those received by people inside your organization.</li><li>iv. Your users frequently send email to a company that supports limited email formats, and you'd like to make sure all emails sent to that organization are sent in a format that they can read.</li></ul></li></ul>
Features in Remote Domain	<ul style="list-style-type: none"><li>✓ Out-of-office messages</li><li>✓ Automatic replies</li><li>✓ Automatic forwards</li><li>✓ Delivery reports</li><li>✓ Non-delivery report</li><li>✓ Meeting forward notifications</li></ul>

## W-3, D-3

### 9. What do connectors do? How to set up a connector?

<b>Connector</b>	<ul style="list-style-type: none"><li>✓ <b>Collection of instructions</b> that customize the way your <b>email flows to and from</b> your Microsoft 365 or Office 365 organization.</li><li>✓ Most Microsoft 365 and Office 365 organizations don't need connectors for regular mail flow.</li><li>✓ Only necessary for the hybrid environment.</li></ul>
<b>Set up Connector</b>	<p>We need connectors for 4 scenarios –</p> <ul style="list-style-type: none"><li>i. Standalone EOP subscription.</li><li>ii. Some of the mailboxes are on on-premises email servers, and some are in Exchange Online.</li><li>iii. All of the mailboxes are in Exchange Online, but you need to send email from sources in your on-premises organization.</li><li>iv. You frequently exchange sensitive information with business partners, and you want to apply security restrictions.</li></ul> <p>These 4 options are available to set up connectors (<b>From &amp; To</b>) -</p> <ul style="list-style-type: none"><li>✓ Office 365</li><li>✓ Your Organization Email Server</li><li>✓ Partner Organization</li><li>✓ Internet</li></ul>

### 10. How old and recent message can be traced?

- ✓ Messages less than 4 hours old might not be available.
- ✓ Messages older than 90 days are unavailable.

### 11. When mail flow works?

Before delivered to user mailbox in EOP stage.

## W-3, D-3

12.Explain the features of mail flow.

<b>Mail Flow</b>  <b>(RuMU ARC)</b>	<b>Rules</b>	<ul style="list-style-type: none"> <li>✓ Apply disclaimers</li> <li>✓ Bypass filter</li> <li>✓ Restrict messages by sender or recipient</li> <li>✓ .....</li> </ul>	<ul style="list-style-type: none"> <li>✓ Apply this rule if</li> <li>✓ Do the following</li> <li>✓ Except if</li> <li>✓ Audit this rule with severity level</li> <li>✓ Choose a mode for this rule</li> <li>✓ Stop Processing more rules</li> <li>✓ .....</li> </ul>
	<b>Message trace</b>	Date Range	<ul style="list-style-type: none"> <li>○ Past 48 hours (summary trace)</li> <li>○ Past 24 hours (summary trace)</li> <li>○ Past 7 days (summary trace)</li> <li>○ Custom (only for EOP trace)</li> </ul>
		Time zone	
		Start/End Date & Time	
		Delivery Status	<ul style="list-style-type: none"> <li>○ All</li> <li>○ Delivered</li> <li>○ Failed</li> <li>○ Expanded</li> </ul>
		Message ID	
		Recipient	
		Sender	
		(only Activate when duration is more than 7 days & date range set custom)	
		<ul style="list-style-type: none"> <li>✓ Include message events &amp; routing details with report (looking for a small number of messages)</li> </ul>	
		Direction	<ul style="list-style-type: none"> <li>○ All</li> <li>○ Inbound</li> <li>○ Outbound</li> </ul>
		Report title	
		Notification email address	
	<b>URL trace</b>		
	<b>Accepted domains</b>		
	<b>Remote domains</b>	Default	<ul style="list-style-type: none"> <li>✓ Out of Office automatic replies</li> <li>✓ Automatic replies</li> <li>✓ Automatic Forwarding</li> <li>✓ Delivery report</li> <li>✓ Non-delivery report</li> <li>✓ Meeting Forward Notification</li> </ul>
	<b>Connectors</b>	<ul style="list-style-type: none"> <li>✓ From</li> <li>✓ To</li> </ul>	<ul style="list-style-type: none"> <li>✓ Office 365</li> <li>✓ Your Organization's email server</li> <li>✓ Partner Organization</li> <li>✓ Internet</li> </ul>

## W-3, D-4

### 1. What is HRDP?

<b>HRDP</b>	<ul style="list-style-type: none"><li>✓ High Risk Deliver Pool</li><li>✓ All outbound messages from Microsoft 365 datacenter servers that's determined to be spam or that exceeds the sending limits of the service or outbound spam policies are sent through the HRDP.</li><li>✓ Separate IP address pool for outbound email that's only used to send "low quality" messages (for example, spam and backscatter).</li><li>✓ Helps prevent the normal IP address pool for outbound email from sending spam.</li><li>✓ The normal IP address pool for outbound email maintains the reputation sending "high quality" messages, which reduces the likelihood that these IP address will appear on IP block lists.</li><li>✓ The very real possibility that IP addresses in the high-risk delivery pool will be placed on IP block lists remains, but this is by design. Delivery to the intended recipients isn't guaranteed, because many email organizations won't accept messages from the HRDP.</li></ul>
<b>Scenario for HRDP Outbound email</b>	<pre>graph LR; Sender[Sender (EXO Server)] --&gt; EOP[EOP]; EOP --&gt; HQM[High Quality Message]; EOP --&gt; LQM[Low Quality Message]; HQM --&gt; NIP[Normal IP Address Pool (Safe IP List)]; NIP --&gt; TPES[Third Party email server]; TPES --&gt; Recipient[Recipient]; LQM --&gt; HRDP[HRDP (e.g. NDR backscatter, spam)]; HRDP --&gt; IBLR[IP Block List Remains]; TPES -.-&gt; Not guaranteed Delivery from HRDP  IBLR</pre>

### 2. What is NDR? How to deal with NDRs?

<b>NDR</b>	<ul style="list-style-type: none"><li>✓ NDR means Non-Delivery Reports.</li><li>✓ When you sent a mail and it faced a problem delivering, Microsoft 365 or office 365 let you know by sending a mail.</li><li>✓ The email you receive is the <b>delivery status notification</b>, also knows as a DSN or bounce message.</li><li>✓ The most common type is called a non-delivery report (NDR).</li><li>✓ NDR can be caused by something as simple as a typo in an email address.</li><li>✓ NDRs include an error code by something that indicates why your email wasn't delivered.</li></ul>
------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



## W-3, D-4

<b>Deal with NDRs</b>	<ul style="list-style-type: none"> <li>✓ <b>Office 365 logo -</b> This indicates that Microsoft 365 or Office 365 generated the NDR. The logo doesn't mean that Microsoft 365 or Office 365 was responsible for the error. This tells which messaging endpoints or services are involved in the email transaction, which is not always clear in older style</li> <li>✓ <b>Cause –</b> This section provides the reason that the message wasn't delivered.</li> <li>✓ <b>Fix-it owner indicator –</b> This section provides an at-a-glance view of the issue and who needs to fix it. The image shows the three basic parties in a Microsoft 365 or Office 365 email transaction: the sender, Microsoft 365 or Office 365, and the recipient. The area marked in red is where the problem usually must be fixed.</li> <li>✓ <b>How to fix it –</b> This section is designed for the end-user or the email sender who receives the NDR. It explains how to fix the issue.</li> <li>✓ <b>More info for email admins -</b> This section provides a detailed explanation of the problem and solution along with technical details and a link to a web-based article that has detailed reference information.</li> <li>✓ <b>Message hops -</b> This section contains times and system references for the message, which allows an admin to follow the message's hops or server-to-server path. With this info, an admin might quickly spot problems between message hops.</li> </ul>
-----------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 3. How to reduce inbound spam emails? Which actions can be taken by admins and end-users?

<b>Actions Taken by Admin</b>	<ul style="list-style-type: none"> <li>✓ Configure <b>Common Attachment Types Filter</b> from - <b>Protection &gt; Malware filter</b></li> <li>✓ Configure <b>IP Allow/Block List</b> from - <b>Protection &gt; Connection filter</b></li> <li>✓ Configure <b>Spam &amp; Bulk Actions</b> from - <b>Protection &gt; Spam filter</b></li> <li>✓ Configure <b>Email domain allow/block list</b> from - <b>Protection &gt; Spam filter</b></li> <li>✓ Configure <b>International Spam</b> from - <b>Protection &gt; Spam filter</b></li> <li>✓ Configure <b>Advanced Options</b> from - <b>Protection &gt; Spam filter</b></li> <li>✓ Configure Mail flow rules from - <b>Mail flow &gt; Rules</b></li> </ul>
<b>Actions Taken by User</b>	<ul style="list-style-type: none"> <li>✓ Configure <b>Inbox rules</b></li> <li>✓ Train the filter by reporting junk email/safe email</li> <li>✓ Never respond to spam</li> <li>✓ Don't use email address publicly to register any unknown websites</li> </ul>

## W-3, D-4

4. A certain email was bounced back with "Access Denied: Recipient address rejected". What does it mean?

✓ <b>Bounced Back with "Access Denied"</b>	<ul style="list-style-type: none"><li>✓ Check the MX record from DNS Management</li><li>✓ Check whether the Domain is healthy</li><li>✓ Check Hybrid Environment configuration</li><li>✓ Check service issues in Exchange Online</li></ul>
--------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

5. An end user reported of not receiving expected inbound emails, what should the administrator do to solve the problem?

✓ Check the message details by doing – <b>Message Trace</b>	<ul style="list-style-type: none"><li>✓ Login to <b>EAC &gt; mail flow &gt; message trace</b>.</li><li>✓ Set <b>date range</b> as " Past 48 hours" (Choose the closest date to the time that the missing message was sent)</li><li>✓ The message status is marked Delivered but when we see "quarantined", go to message details.</li><li>✓ Click on the edit icon and it will open a new window and show the message status. It Describes the issue. "How to Fix It" section gives the steps to resolve the issue.</li></ul>
----------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

6. What is Out of Office? How to enable it?

<ul style="list-style-type: none"><li>✓ Set a specific reply to send someone as a reply of his/her mail</li><li>✓ Maximum 1 reply for one specific user in a day</li><li>✓ For example: I am in leave or vacation. Now if anyone sends me a message, they will get this reply. They are now informed that I am in leave and currently not doing work.</li></ul>	
<ul style="list-style-type: none"><li>✓ Please open Outlook Client</li><li>✓ Please navigate to – <b>File &gt; Automatic Replies &gt; send automatic replies</b></li></ul>	
<ul style="list-style-type: none"><li>✓ Please go to – <a href="https://outlook.office365.com">https://outlook.office365.com</a></li><li>✓ Please navigate to – <b>Settings (Gear Sign) &gt; View all outlook settings &gt; Mail &gt; Automatic replies &gt; turn on Automatic replies on</b></li></ul>	

## W-3, D-4

### 7. How to confirm whether an email is being routed through HRDP or not?

- ✓ If the customer has an email header, Review the X -Forefront-Antispam-Report header or the X-Forefront-Antispam-Report-Untrusted header to locate DIR:OUT
- ✓ spam confidence level (SCL) entry of 5 to 9 to verify that it was treated as spam.

### 8. Troubleshooting to be performed to confirm why email is being routed via HRDP.

- ✓ Have the sender send a blank message with **just a signature** to see if it's still marked as spam. If the message is still marked as spam the signature may be the problem.
- ✓ Have the sender send a blank message with **no signature or disclaimer**. If the message is still marked as spam there may be a reputation problem with the sending domain
- ✓ Have the sender send the same message but with the **signature disabled**. If the message is still marked as spam the problem is likely in the message content.
- ✓ Check public reputation lists for the sending domain, or any URLs included in the message

### 9. Actions to be taken to prevent legitimate emails from being routed via HRDP

Collect the original sample of the email from the sender's sent item folder and submit the sample to our protection team following below steps:

- ✓ Create a new, blank email.
- ✓ Address the email to the Microsoft team that reviews messages at **not\_junk@office365.microsoft.com**
- ✓ Copy and paste the affected message into that email (as an attachment).
- ✓ Make sure all information, including mail header information is included
- ✓ Click Send.
- ✓ Allow 24 hours for the filters to be updated and in case the issue persists contact the Support team.

## W-3, D-5

### 1. What is SMTP/POP3/MAPI/IMAP/ActiveSync/Autodiscover?

<b>SMTP</b>	<ul style="list-style-type: none"><li>✓ <b>Simple Mail Transfer Protocol (SMTP)</b> is the standard protocol for sending emails across the Internet.</li><li>✓ Most e-mail systems that send mail over the Internet use <b>SMTP</b> to send messages from one server to another; the messages can then be retrieved with an e-mail client using either <b>POP</b> or <b>IMAP</b>.</li><li>✓ <b>SMTP</b> is generally used to send messages from a mail client to a mail server. This is why you need to specify both the <b>POP</b> or <b>IMAP</b> server and the <b>SMTP</b> server when you configure your e-mail application.</li></ul>
<b>POP3</b>	<ul style="list-style-type: none"><li>✓ <b>Post Office Protocol version 3 (POP3)</b> is a standard mail protocol used to receive emails from a remote server to a local email client.</li><li>✓ <b>POP3</b> allows you to download email messages on your local computer and read them even when you are offline.</li><li>✓ Messages are downloaded locally and removed from the email server.</li></ul>
<b>MAPI</b>	<ul style="list-style-type: none"><li>✓ <b>MAPI</b> stands for <b>Messaging Application Programming Interface</b>.</li><li>✓ <b>MAPI</b> is a proprietary Microsoft protocol that allows the Microsoft Outlook email client to fully utilize all of the features of an Exchange server including email, shared address books, calendars and public folders.</li><li>✓ When Outlook is configured as a <b>MAPI</b> client, also known as an Exchange client, email is stored in the cloud on Comcast's secure mail server with a copy on your computer.</li><li>✓ Messages retained in the cloud are accessible via webmail from any internet connected computer.</li><li>✓ With <b>MAPI</b>, you can move messages from the cloud into a local file on your computer called a <b>.PST</b> file, a process through which copies of messages are deleted from the cloud and stored on your computer.</li></ul>
<b>IMAP</b>	<ul style="list-style-type: none"><li>✓ The <b>Internet Message Access Protocol (IMAP)</b> is a mail protocol used for accessing email on a remote web server from a local client.</li><li>✓ <b>IMAP</b> is the most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers.</li><li>✓ <b>IMAP</b> allows simultaneous access by multiple clients. This is why <b>IMAP</b> is more suitable for you if you're going to access your email from different locations or if your messages are managed by multiple users.</li></ul>
<b>ActiveSync</b>	<ul style="list-style-type: none"><li>✓ Exchange <b>ActiveSync</b> is a proprietary protocol that syncs your mobile device with your Exchange mailbox, so you can access your email, calendar, contacts, tasks, and so much more.</li><li>✓ It is based on <b>XML</b> and communicates with a mobile device using <b>HTTP</b> or <b>HTTPS</b>.</li></ul>

## W-3, D-5

### Autodiscover

- ✓ Autodiscover is the feature that Outlook uses to obtain configuration information for servers to which it connects.
- ✓ Kind of DNS records (CNAME).
- ✓ Help us to configure email client.

## 2. What are the steps of Autodiscover? How to check Autodiscover?

### 1) SCP Lookup:

- ✓ SCP refers to **Service Connection Point**, which the clients of the service use the data in an SCP to locate, connect to, and authenticate an instance of your service.
- ✓ **SCP data return a path of the Autodiscover XML.**
- ✓ An attempt is then made to each URL that's returned by the SCP lookup to try to retrieve the Autodiscover payload.
- ✓ If fails to retrieve the payload, it is moved to root domain query.

### 2) HTTPS root domain query:

- ✓ In this step, Outlook builds a URL from the domain name of the initial address in the format of **https://<domain>/autodiscover/autodiscover.xml** and tries to retrieve the payload from the resulting URL.
- ✓ Because many root domains aren't configured for Autodiscover, Outlook purposefully silences any certificate errors that occur during the attempted retrieval.
- ✓ If this step doesn't acquire the payload, it is moved to the next step.

### 3) HTTPS Autodiscover domain query:

- ✓ In this step, Outlook create a URL from the domain name of the initial address in the format of **https://autodiscover.<domain>/autodiscover/autodiscover.xml** and tries to retrieve the payload from the resulting URL.
- ✓ Since it's a primary URL typically for Autodiscover data, it doesn't silence any certificate errors that occur during the attempted retrieval.
- ✓ If this step doesn't acquire the payload, it is moved to the next step.

### 4) Check for local XML file:

- ✓ In this step Outlook will check the local XML file, whether the file is found or not.
- ✓ If the payload is not retrieved, it is moved to the next step.

### 5) HTTP Redirect Method:

- ✓ In this step, outlook sends a request to the Autodiscover domain URL **http://autodiscover.<domain>/autodiscover/autodiscover.xml** and test for redirect responses.
- ✓ If an actual Autodiscover XML payload is returned and not a redirect, Outlook ignores the actual Autodiscover XML response because it was retrieved without the http security.
- ✓ If it's a valid redirect URL, Outlook follows the redirect and will try to retrieve a payload XML from the new URL.

## W-3, D-5

- ✓ Outlook will also look for harmful URL's in this step.
- ✓ If the payload is not retrieved, it is moved to the next step.

### 6) SRV Record query:

- ✓ In this step, Outlook will perform a DNS inquiry and it will check for the for the first record that uses https as its protocol.
- ✓ Then it tries to retrieve the payload from that URL.
- ✓ If the payload is not retrieved, it is moved to the next step.

### 7) Cached URL in the Outlook profile:

- ✓ In this step, outlook will check for the cached URL in the Outlook profile.
- ✓ This step is performed by the Outlook itself, if it finds any cached it will retrieve the payload
- ✓ If not then it is moved to the next step.

### 8) Direct Connect to Office 365:

- ✓ If Autodiscover is working and pointing to the correct server, Outlook should use it to find the mail server, so verify that it is working.
- ✓ Use the Remote Connectivity Analyzer to check your records.
- ✓ If Outlook is unable to reach Autodiscover, Outlook will attempt to find your mail server using the method Direct Connect.

## How to Check Auto Autodiscover through Outlook Client

- ✓ Please open Outlook client
- ✓ Click on the show hidden icons > press and hold down the **CTRL** key, and then right-click the Outlook icon in the system tray.
- ✓ A menu will appear and select **Test E-mail AutoConfiguration**
- ✓ Use Autodiscover should be checked by default. You can also check and uncheck the other options Use Guesscheck and Secure Guessmart Authentication checkboxes.
- ✓ Provide your email address and passwords and click on Test.
- ✓ The Result tab shows that the Autodiscover is detected. You can also check for log and XML details by clicking the tabs.

## How to Check Auto Autodiscover through Email Connectivity Analyser

- ✓ Please go to - <https://testconnectivity.microsoft.com/>
- ✓ Click on **Outlook Connectivity**
- ✓ A new window will appear. Provide the **Email address**, Microsoft account and **Password**.
- ✓ Click on **Use Autodiscover** to detect server settings and check on the terms.
- ✓ Then provide the captcha for verification and finally click on Perform Test.

## W-3, D-5

### 3. What is the purpose of Autodiscover?

<b>Purpose of Autodiscover</b>	<ul style="list-style-type: none"><li>✓ Helps to configure Email client</li><li>✓ Synchronize outlook client to Exchange Sync</li><li>✓ Free/Busy information in your calendar</li><li>✓ Out of office automatic response messages setup in Outlook.</li><li>✓ Proper syncing of Offline Address Book</li><li>✓ Folder Sharing with sending out the Sharing invitation.</li></ul>
--------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4. Test Autodiscover from <https://testconnectivity.Microsoft.com/> and read the generated report.

<ul style="list-style-type: none"><li>✓ Please go to - <a href="https://testconnectivity.microsoft.com/">https://testconnectivity.microsoft.com/</a></li><li>✓ Click on <b>Outlook Connectivity</b></li><li>✓ A new window will appear. Provide the <b>Email address</b>, Microsoft account and <b>Password</b>.</li><li>✓ Click on <b>Use Autodiscover</b> to detect server settings and check on the terms.</li><li>✓ Then provide the captcha for verification and finally click on Perform Test.</li></ul>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 5. What is SMTP Relay?

<b>SMTP Relay</b>	<ul style="list-style-type: none"><li>✓ SMTP relay let office 365 replays emails on behalf of you by using a connector.</li><li>✓ Configured with public IP address or a TLS certificate.</li><li>✓ Any email address including Office 365 mailboxes can send mail using an SMTP relay, as long as it uses a domain that is set up as your in-office 365</li><li>✓ Possible to use multi-factor authentication (MFA).</li><li>✓ Possible to send email to external recipients</li></ul>
-------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 6. Why do we need SMTP relay?

- ✓ An SMTP relay service is the best way to manage **batch sends** and **automated emails**.
- ✓ Sending over SMTP through a trusted 3rd party will help you ensure that you don't experience **deliverability issues** and that your mail keeps flowing to the inbox without any issues.

## W-3, D-5

### 7. What is the limitation of accessing email account through POP3, IMAP?

Limitation of Accessing email through POP3	<ul style="list-style-type: none"><li>✓ Multiple connection using same email address is not possible.</li><li>✓ POP3 stores the email on the local storage of the client.</li><li>✓ POP3 clients remove downloaded messages from the email server.</li><li>✓ Difficult to access email on multiple computers.</li><li>✓ POP3 can't synchronize multiple folders on the email server with multiple folders on the client computer.</li><li>✓ POP3 also doesn't support public folder access.</li></ul>
Limitation of Accessing email through IMAP	<ul style="list-style-type: none"><li>✓ Multiple connection is possible using same email address (20 connections per IP address).</li></ul>
Common Limitation	<ul style="list-style-type: none"><li>✓ For always-connected clients, the user might <b>configure the email application</b> to send and receive messages every set number of minutes.</li><li>✓ Each time opening Microsoft 365 email, user will experience a <b>delay</b> of several seconds.</li><li>✓ <b>Modern Authentication</b> will not work for legacy protocols, such as POP3 and IMAP4.</li><li>✓ Don't offer <b>rich email</b>, <b>calendaring</b>, and <b>contact management</b>, or other features that are available when users connect with Outlook, Exchange ActiveSync, Outlook on the web</li></ul>

### 8. Why do we SMTP?

- ✓ SMTP is used to **send emails**, so it only works for **outgoing emails**.
- ✓ To be able to send emails, you need to provide the correct SMTP server when you set up your email client.
- ✓ Unlike POP3 and IMAP, SMTP can't be used to retrieve and store emails.
- ✓ SMTP is also responsible for setting up communication between servers.

### 9. How to enable Autodiscover?

- ✓ MS Admin > Settings > Domain > DNS Records > Add
- ✓ From Domain Hosting Provider, DNS Management



## W-3, D-5

10. What are the methods to send mail using Microsoft 365? Know the differences of each method

There are three methods to send mail using Microsoft 365:

	(1) SMTP client submission	(2) Direct send	(3) SMTP relay
Features			
MFA	No	Uses	uses
Send to recipients in your domain(s)	Yes	yes	yes
Relay to internet via Microsoft 365	Yes.	No. Direct delivery only	yes
Bypasses antispam	Yes, if the mail is destined for one of your Microsoft 365 or Office 365 mailboxes	No. Suspicious emails might be filtered. We recommend a custom Sender Policy Framework (SPF) record.	No. Suspicious emails might be filtered. We recommend a custom SPF record. Redirect to HRDP
Supports mail sent from applications hosted by a third party	Yes	Yes. We recommend updating your SPF record to allow the third party to send as your domain	No
Saves to Sent Items folder	Yes	No	No
Requirements			
Open network port	Port 587 or port 25	Port 25	Port 25
Device or application server must support TLS	Required (1.2 & above)	Optional	Optional
Requires authentication	Microsoft 365 or Office 365 username and password required	None	One or more static IP addresses.
Limitations			
Throttling limits	10,000 recipients per day. 30 messages per minute.	Standard throttling is in place to protect Microsoft 365 or Office 365 Throttling limits	Reasonable limits are imposed. The service can't be used to send spam or bulk mail.

## **W-3, D-5**

11. What are the different methods to configure SMTP Relay?

<b>Configured with IP address-based connector</b>	<ul style="list-style-type: none"><li>✓ Obtain the public (static) IP address that the device or application with send from.</li><li>✓ A dynamic IP address isn't supported or allowed.</li><li>✓ You can share your static IP address with other devices and users, but don't share the IP address with anyone outside of your company.</li></ul>
<b>Configured with TLS Certificate based connector</b>	<ul style="list-style-type: none"><li>✓ Verify the subject name on the certificate used by the sending device or application.</li><li>✓ The common name (CN) or subject alternative name (SAN) in the certificate should contain a domain name that you have registered in Microsoft 365 or Office 365.</li><li>✓ Must create a certificate-based connector in Microsoft 365 or Office 365 with this same domain name to accept and relay emails coming from these devices, applications, or any other on-premises server.</li></ul>

## **W-4, D-1**

1. What is SARA tool? When we should use this tool?

<b>SARA</b>	<ul style="list-style-type: none"><li>✓ <b>Microsoft Support &amp; Recovery Assistant</b></li><li>✓ Run tests on your computer to figure out the problem.</li><li>✓ Can fix many of the issues for you or tell you how to fix them yourself.</li><li>✓ This tool will scan Office, Outlook, Dynamic 365 (the online version of Office), OneDrive, Skype for Business, and give you a clearer picture of what needs to be done to resolve your issue.</li></ul>
<b>Reason for Using SARA</b>	<ul style="list-style-type: none"><li>✓ New app by Microsoft, designed exclusively to resolve issues that occur in Office 365 products.</li><li>✓ Known as Virtual support agent.</li><li>✓ Easy to install.</li><li>✓ Give instruction the users the remedial steps, whenever necessary.</li><li>✓ Trusted tool from the house of Microsoft that will come handy whenever there is an issue on Office 365 products.</li></ul>

2. What is MS Booking? Which subscriptions of Microsoft have MS Booking?

<b>MS Booking</b>	<ul style="list-style-type: none"><li>✓ Scheduling tool and is part of the Microsoft Office family of products.</li><li>✓ Allows customers of small businesses and companies to book appointments with the company.</li><li>✓ Online and mobile app for small businesses who provide services to customers on an appointment basis.</li><li>✓ Examples of businesses include hair salons, dental offices, spas, law firms, financial services providers, consultants, and auto shops.</li></ul>
<b>Subscriptions for MS Booking</b>	<ul style="list-style-type: none"><li>✓ Microsoft 365 Business Standard</li><li>✓ Microsoft 365 Business Premium</li><li>✓ Microsoft 365 E3</li><li>✓ Microsoft 365 E5</li></ul>

## W-4, D-1

### 3. What are the steps to Reset Microsoft 365 Apps for enterprise activation state?

#### Step 1: Remove Office 365 license for subscription -based installations

- ✓ In an elevated command window, run the cd command based on your install location: `cd "C:\Program Files\Microsoft Office\Office16"`
- ✓ Run - `cscript ospp.vbs /dstatus`
- ✓ Find product key & Run - `cscript ospp.vbs /unpkey:<Last 5 of installed product key>`

#### Step 2: Remove cached identities in HKCU registry

- ✓ In Registry Editor, locate the following registry:  
**HKEY\_CURRENT\_USER\Software\Microsoft\Office\16.0\Common\Identity\Identities**
- ✓ Remove all identities under the Identities registry entry.

#### Step 3: Remove the stored credentials in Credential Manager

- ✓ Open **Control Panel > Credential Manager**
- ✓ Remove all **Windows credentials** listed for Office16 by selecting the drop-down arrow and Remove.

#### Step 4: Clear persisted locations

##### Credential Manager

- ✓ %appdata%\Microsoft\Credentials
- ✓ %localappdata%\Microsoft\Credentials
- ✓ %appdata%\Microsoft\Protect
- ✓ HKEY\_CURRENT\_USER\Software\Microsoft\Protected Storage System Provider

##### Office 365 activation tokens and identities

- ✓ %localappdata%\Microsoft\Office\16.0\Licensing
- ✓ %localappdata%\Microsoft\Office\Licenses (Microsoft 365 Apps for enterprise version 1909 or later)
- ✓ HKEY\_CURRENT\_USER\Software\Microsoft\Office\16.0\Common\Identity
- ✓ HKEY\_USERS\The user's SID\Software\Microsoft\Office\16.0\Common\Identity

##### Auto-Process

- ✓ The four steps above can be automated using **OLicenseCleanup.vbs**.
- ✓ Simply download and run the script with elevated privileges.

## W-4, D-1

### 4. What is ODT? How to use ODT to update or install O365?

#### ODT

- ✓ A command-line tool that you can use to download and deploy Click-to-Run versions of Office, such as Microsoft 365 Apps for enterprise, to your client computers.

#### Step 1: Create the configuration file

- ✓ When creating the configuration file, we recommend starting with an example file and updating it with the appropriate options for your environment. You can start by copying and pasting the example below into a text file, saving it with a name of your choosing, and then editing the XML elements and attributes to define the options you want.

#### Step 2: Run the ODT executable in configure mode

- ✓ From a command prompt, run the ODT executable in configure mode with a reference to the configuration file you saved. In the following example, the configuration file is named installconfig.xml:

```
<path>setup.exe /configure installconfig.xml
```

- ✓ You must have local administrator permissions on the client computer. You can run the executable from the client computer on which you want to install Office or you can put the ODT and the configuration file on a network share and run it from there. If you use a network share, make sure to pass the full network path for both the setup.exe and the configuration file to the command.

#### Step 3: Verify that installation was successful

- ✓ After running the command, you should see the Office installation start (unless you set display level to none). After installation is complete, the command prompt will display "Products configured successfully." If you run into problems, make sure you have the newest version of the ODT. You can also troubleshoot issues by reviewing the log files in the %temp% and %windir%\temp directories.

## W-4, D-1

5. In which scenario customer can use Microsoft Booking?

Microsoft Booking	<ul style="list-style-type: none"><li>✓ Microsoft Bookings is an <b>online</b> and <b>mobile app</b> for <b>small businesses</b> who provide services to customers on an appointment basis.</li><li>✓ Examples of businesses include hair salons, dental offices, spas, law firms, financial services providers, consultants, and auto shops.</li></ul>
Different Scenario of Microsoft Booking	<ul style="list-style-type: none"><li>✓ Online appointment booking</li><li>✓ Automated email confirmations</li><li>✓ Reminder emails</li><li>✓ Customizable notice periods</li><li>✓ Unique appointment scheduling webpage</li><li>✓ Service, date, time &amp; staff member selection</li><li>✓ Appointment rescheduling</li><li>✓ Booking cancellations</li><li>✓ Centralized booking calendar</li><li>✓ Appointment reassignment between staff members</li><li>✓ Day 'split view' for staff availability</li><li>✓ Colour-coding of staff</li><li>✓ Manual appointment creation</li><li>✓ Automatic contact creation</li><li>✓ Automatic calendar updates</li><li>✓ Outlook.com &amp; Google calendar integrations</li><li>✓ Real-time staff availability</li><li>✓ Directions to appointments</li></ul>

6. Why does Outlook keep prompting for password?

<ul style="list-style-type: none"><li>✓ Outlook is configured to prompt you for credentials</li><li>✓ Incorrect password cached in credential storage</li><li>✓ Required Authentication Settings for outgoing server and incoming server</li><li>✓ Outlook Anywhere is not configured to use <b>NTLM Authentication</b></li><li>✓ Corrupt Outlook profile</li><li>✓ Slow or unstable network connection</li><li>✓ Antivirus programs</li><li>✓ Shared calendars</li></ul>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## W-4, D-1

7. Customer is getting “Error 0x80070002” when starting outlook client. How to solve it?

Cause	<ul style="list-style-type: none"><li>✓ Corrupted PST file</li><li>✓ Conflict of the operating system compatibility</li></ul>
<ul style="list-style-type: none"><li>✓ By default, there are two locations where Outlook may create PSTs. You will need to check them manually, these are: <code>\AppData\Local\Microsoft\Outlook\</code> <code>\Documents\Outlook Files</code></li><li>✓ If any of these paths are inaccessible, you will get this error.</li><li>✓ Firstly, you have to open the Windows Documents folder and create the new folder by the name of “<b>Outlook PST</b>” Make sure while you are creating a file in this folder you also create a test file to check whether it is accessible or not.</li><li>✓ Now the folder will be created, once done, click on the windows explorer address bar to make a note of the complete path.</li><li>✓ Windows <b>Run</b> dialogue, type <b>Regedit</b> and click <b>Enter</b></li><li>✓ Windows Registry will be opened. The path has to be browsed: <code>HKEY_CURRENT_USER\Software\Microsoft\Office\</code></li><li>✓ Now the Outlook folder has to be opened whichever Outlook version you are using. For instance:<ul style="list-style-type: none"><li>○ Outlook 2007 = \12\</li><li>○ Outlook 2010 = \14\</li><li>○ MS Outlook 2013 = \15\</li><li>○ Outlook 2016 = \16\</li></ul></li><li>✓ The path will look something like this: <code>HKEY_CURRENT_USER\Software\Microsoft\Office\\Outlook</code></li><li>✓ Now do the right-click in the vacant area in the right panel and click on <b>New &gt; String Value</b>.</li><li>✓ Now name it <b>ForcePSTPath</b> and click <b>Enter</b>.</li><li>✓ You’ll notice this new value in the right panel. Right-click on it, and select <b>Modify</b>.</li><li>✓ Under “<b>Value data</b>” enter the complete location for the PST file you noted/created earlier.</li><li>✓ Click <b>OK</b> and then close the Registry editor window.</li></ul>	

## **W-4, D-1**

8. Outlook to crash or stop responding when used with Office 365. How to troubleshoot this issue?

### **Step1: Investigate possible issues caused by add-ins.**

- ✓ Exit Outlook.
- ✓ Open a **Run** dialogue box from the Start menu.
- ✓ Type **Outlook /safe**, and then click **OK**.
- ✓ If the issue is fixed, click **Options** on the **File** menu, and then click **Add-Ins**.
- ✓ Select **COM Add-ins**, and then click **Go**.
- ✓ Click to clear all the checkboxes in the list, and then click **OK**.
- ✓ Restart Outlook.
- ✓ If the issue doesn't occur, start adding the add-ins one at a time until the issue occurs.

### **Step2: Repair Office**

- ✓ Open Control Panel, and then click **Uninstall a program**.
- ✓ In the list of installed programs, right-click the entry for your Office installation, and then click **Change**, and then click **Online Repair**.

### **Step3: Run Outlook Diagnostics**

- ✓ Download **Microsoft Support and Recovery Assistant** for Office 365 (SaRA).
- ✓ On the first screen, select **Outlook**, and then select **Next**.
- ✓ Select any of the following options, as appropriate, and then select **Next**:
  - Outlook keeps hanging or freezing
  - Outlook keeps crashing with a message "Microsoft Outlook has stopped working."
- ✓ SaRA runs some diagnostic checks and returns possible solutions for you to use to try to fix Outlook connectivity issues.

### **Step4: Create a new Outlook Profile**

- ✓ Open Control Panel, and then click **Mail**.
- ✓ Click **Show Profiles**.
- ✓ Select the profile that you want to remove, and then click **Remove**.
- ✓ Click **Add**.
- ✓ In the **Profile Name** box, type a name for the new profile.
- ✓ Specify the user name, the primary SMTP address, and the password.
- ✓ Then, click **Next**.
- ✓ You may receive a message.
- ✓ In this message, click to select the **Don't ask me about this website again** checkbox, and then click **Allow**.
- ✓ When you're prompted, enter your login credentials, and then click **OK**.
- ✓ When Setup is finished, click **Finish**.



## W-4, D-2

### 1. How to create alert policies? What are those policies used for?

<b>Alert Policy</b>	<ul style="list-style-type: none"><li>✓ Use alert policies to <b>track user and admin activities</b>, malware threats, or data loss preventions, mail flow activities, permissions in your organization.</li><li>✓ After choosing the activity you want to be alerted on, refine the policy by adding conditions, deciding when to trigger the alert, and who should receive notifications.</li></ul>
<b>How Alert Policy Works</b>	
Please go to – <a href="https://protection.office.com">https://protection.office.com</a>	
Please navigate to – <b>Alerts &gt; Alert policies</b>	
<ul style="list-style-type: none"><li>✓ <b>Name your Alert</b></li></ul> Type the Name, Choose <b>Severity &amp; Category</b>	
<ul style="list-style-type: none"><li>✓ <b>Create alert settings</b></li></ul> Choose <b>activity is</b> and <b>Add condition</b> if required	
<ul style="list-style-type: none"><li>✓ <b>Set your recipients</b></li></ul> Type <b>send email notification</b> and set <b>Daily notification limit</b>	
<ul style="list-style-type: none"><li>✓ <b>Review your settings</b></li></ul>	

### 2. Assigning permission in SCC.

Please go to – <a href="https://protection.office.com">https://protection.office.com</a>
Please navigate to – <b>Permissions</b>
You will see a list of default permissions available. Click any one & scroll down. Click <b>Edit</b> under <b>Member</b> section
Click <b>Choose members</b> & add a member for this role.

## W-4, D-2

### 3. How to import .PST files?

<b>Roles required</b>	<ul style="list-style-type: none"><li>✓ You have to be assigned the <b>Mailbox Import Export role</b>, <b>Mail Recipients role</b> in Exchange Online. By default, this role is assigned to the <b>Organization Management</b> and <b>Recipient Management</b> roles groups.</li><li>Or,</li><li>✓ You have to be a global administrator in your organization.</li></ul>
<ul style="list-style-type: none"><li>✓ <b>Step 1: Copy the SAS URL and install AzCopy</b><ul style="list-style-type: none"><li>○ This URL is a combination of the <b>network URL</b> for the <b>Azure Storage location</b> in the Microsoft cloud for your organization and a <b>Shared Access Signature (SAS)</b> key.</li><li>○ This key provides you with the necessary permissions to upload PST files to your Azure Storage location.</li><li>○ Need to download <b>Azure AzCopy</b></li></ul></li><li>✓ <b>Step 2: Upload your PST files to Microsoft 365</b></li><li>✓ (Optional) <b>Step 3: View a list of the PST files uploaded</b></li><li>✓ <b>Step 4: Create the PST Import mapping file</b></li><li>✓ <b>Step 5: Create a PST Import job</b></li><li>✓ <b>Step 6: Filter data and start the PST Import job</b></li></ul>	
<ul style="list-style-type: none"><li>✓ You have to perform <b>Step 1 only once</b> to import PST files to Microsoft 365 mailboxes.</li><li>✓ Upload PST file must be less than 20 GB</li></ul>	

### 4. What is Submission explorer? How to submit emails?

<b>Submission Explorer</b>	<ul style="list-style-type: none"><li>✓ In Microsoft 365 organizations with mailboxes in Exchange Online, admins can use the Submissions portal in the Security &amp; Compliance Center to submit email messages, URLs, and attachments to Microsoft for scanning.</li><li>✓ When you submit an email, you will get information about any policies that may have allowed the incoming email into your tenant, as well as examination of any URLs and attachments in the mail.</li></ul>
<b>Roles Required</b>	<ul style="list-style-type: none"><li>✓ <b>Organization Management</b> or <b>Security Administrator</b> in the <b>Security &amp; Compliance Center</b></li><li>✓ <b>Organization Management</b> or <b>Hygiene Management</b> in <b>Exchange Online</b></li></ul>

## W-4, D-2

### Submit Emails through Submission Explorer

Please go to – <https://protection.office.com>

Please navigate to – ① **Threat management** > ② **Submission** > ③ **New Submission**

For **Email** – Choose **Object type**, **Submission format**, **Reason for submission** & press **submit**

For **URL/Attachment** –

Mention URL link/download the attachment, choose **Reason for submission** & press **submit**

5. What are the reasons for a user to be restricted from sending email? How to unblock users from restricted users?

#### Reasons for Restriction from Sending Email

- ✓ If a user exceeds one of the outbound sending limits (e.g. 30 messages/minute) as specified in the service limits or in outbound spam policies.
- ✓ The user is restricted from sending email, but they can still receive email.
- ✓ When they try to send email, the message is returned in a **non-delivery report (NDR)** with the error code **5.1.8 (Access Denied)** and the following text:

#### Unblock user from Restricted User

- ✓ In the Security & Compliance Center, go to **Threat management** > **Review** > **Restricted users**
- ✓ Find and select the user that you want to unblock. In the **Actions** column, click **Unblock**.
- ✓ Click **Next** when done.
- ✓ The next screen has recommendations to help prevent future compromise. Enabling multi-factor authentication (MFA) and changing the passwords are a good defense. Click **Unblock user** when done.
- ✓ It may take 30 minutes or more before restrictions are removed.

#### How to Resolve the Issue (5.1.8 – Access Denied)

- ✓ If the user is doing is willingly, admin may warn user and unblock.
- ✓ If the user account is hacked, then admin can **reset password**, **enable MFA**, **Do MHA**, try **Message trace**

## W-4, D-2

6. What is the purpose of Anti-Phishing & Anti-Spam Policies? How to set up these policies?

<b>Purpose of Anti-Phishing &amp; Anti-Spam Policies</b>	<ul style="list-style-type: none"><li>✓ In Microsoft 365 organizations with mailboxes in Exchange Online or standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, email messages are automatically protected against spam and malware by EOP.</li><li>✓ Spam is unsolicited and unwanted email. Malware is viruses and spyware.</li><li>✓ Viruses infect other programs and data, and they spread throughout your computer looking for programs to infect.</li><li>✓ Spyware is a specific type of malware that gathers your personal information (for example, sign-in information and personal data) and sends it back to the malware author.</li><li>✓ EOP has built-in inbound and outbound malware filtering to help protect your organization from malicious software, and built-in spam filtering to help protect your organization from both receiving and sending spam (for example, in case of compromised accounts).</li><li>✓ Admins don't need to set up or maintain the filtering technologies because they're enabled by default. However, you can customize the settings based on the needs of your organization.</li></ul>
<b>Anti-phishing</b>	<ul style="list-style-type: none"><li>✓ In the <b>Security &amp; Compliance Center</b>, choose <b>Threat management &gt; Policy &gt; ATP anti-phishing</b>.</li><li>✓ Click <b>Default policy</b>.</li><li>✓ In the <b>Impersonation</b> section, click <b>Edit</b>, and then specify the following settings:<ul style="list-style-type: none"><li>○ On the <b>Add users to protect</b> tab, turn protection on.</li><li>○ On the <b>Add domains to protect</b> tab, turn on <b>Automatically include the domains I own</b>. If you have custom domains, add those as well.</li><li>○ On the <b>Actions</b> tab, select <b>Quarantine the message</b> for both the <b>impersonated user</b> and <b>impersonated domain</b> options. In addition, turn on impersonation safety tips.</li><li>○ On the <b>Mailbox intelligence</b> tab, make sure mailbox intelligence is turned on. In addition, turn on mailbox intelligence-based impersonation protection. In the <b>If email is sent by an impersonated user</b> list, choose <b>Quarantine the message</b>.</li><li>○ On the <b>Add trusted senders and domains</b> tab, specify any trusted senders or domains that you want to add.</li><li>○ On the <b>Review your settings</b> tab, after you have reviewed your settings, click <b>Save</b>.</li></ul></li><li>✓ In the <b>Spoof</b> section, click <b>Edit</b>, and then specify the following settings:<ul style="list-style-type: none"><li>○ On the <b>Spoofing filter settings</b> tab, make sure anti-spoofing protection is turned on.</li></ul></li></ul>

## W-4, D-2

	<ul style="list-style-type: none"><li>○ On the <b>Actions</b> tab, choose <b>Quarantine the message</b>.</li><li>○ On the <b>Review your settings</b> tab, after you have reviewed your settings, click <b>Save</b>. (If you didn't make any changes, click <b>Cancel</b>.)</li></ul> <p>✓ Close the default policy settings page.</p>
<b>Anti-Spam Protection</b>	<p>Anti-spam protection is available in subscriptions that include EOP.</p> <ol style="list-style-type: none"><li>1. In the Security &amp; Compliance Center, choose <b>Threat management &gt; Policy &gt; Anti-spam</b>.</li><li>2. On the <b>Custom</b> tab, turn <b>Custom settings</b> on.</li><li>3. Expand <b>Default spam filter policy</b>, click <b>Edit policy</b>, and then specify the following settings:<ul style="list-style-type: none"><li>○ In the <b>Spam and bulk actions</b> section, set the threshold to a value of 5 or 6.</li><li>○ In the <b>Allow lists</b> section, review (and if necessary, edit) your allowed senders and domains.</li></ul></li><li>4. Click <b>Save</b>.</li></ol>

### 7. How to create an outbound spam policy?

<p>Please go to – <a href="https://protection.office.com">https://protection.office.com</a></p> <p>Please navigate to –</p> <p><b>Threat management &gt; Policy &gt; Anti-spam settings &gt; Create an outbound policy &gt; type a suitable name</b></p>
<p>Check <b>notification</b> if required.</p>
<p>Set <b>Recipient Limits</b> for hourly &amp; daily limit (0 to max 10000)</p>
<p>Set <b>Automatic Forwarding</b></p>
<p>Set <b>Applied to &gt; Add Condition &gt; press Save</b></p>

## W-4, D-3

### 1. Message trace using SCC.

<b>Initial Option Trace</b>	<ul style="list-style-type: none"><li>✓ <b>Default Queries</b> - Queries provided by Office 365</li><li>✓ <b>Custom Queries</b> - Queries created and saved by admins in your organization</li><li>✓ <b>Autosaved Queries</b> - Last 10 queries that were run but not saved manually</li></ul>
<ul style="list-style-type: none"><li>✓ Please navigate to – <b>SCC &gt; Mail flow &gt; Message trace &gt; +Start a trace</b></li><li>✓ Please fill up – Date range, Time range, Time zone (default 2 days), Message ID, Delivery Status, Recipient, Sender</li><li>✓ Choose report type<ul style="list-style-type: none"><li>○ <b>Summary:</b><ul style="list-style-type: none"><li>▪ If the time range is less than <b>10 days</b>,</li><li>▪ No additional filtering options</li><li>▪ Results are available almost immediately</li><li>▪ Report returns up to <b>20,000 results</b></li></ul></li><li>○ <b>Enhanced summary:</b><ul style="list-style-type: none"><li>▪ Downloadable CSV files.</li><li>▪ Require By these people, To these people, or Message ID.</li><li>▪ Report returns up to <b>50,000 results</b>.</li><li>▪ Include Direction, Original client IP address &amp; many more.</li></ul></li><li>○ <b>Extended summary:</b><ul style="list-style-type: none"><li>▪ Downloadable CSV files.</li><li>▪ Require By these people, To these people, or Message ID.</li><li>▪ The Extended report returns up to <b>1000 results</b>.</li><li>▪ Include message events &amp; routing details with report (comprehensive)</li></ul></li></ul></li></ul>	

## W-4, D-3

### 2. What is Content Search? How to retrieve data by doing Content Search?

<b>Content Search</b>	<ul style="list-style-type: none"><li>✓ For in-place items such as <b>email, documents, and instant messaging conversations</b> in your organization.</li><li>✓ Possible to retrieve deleted email and other items of user mailbox as a PST file.</li></ul>
<ul style="list-style-type: none"><li>✓ Go to <a href="https://protection.office.com">https://protection.office.com</a></li><li>✓ Click <b>Search &gt; Content search</b>.</li><li>✓ On the Search page, click the arrow next to Add icon <b>New search</b>.</li><li>✓ After you've set up your search query, click <b>Save &amp; run</b>.</li><li>✓ On the Save search page, type a name for the search, and an optional description that helps identify the search. The name of the search has to be unique in your organization.</li><li>✓ Click <b>Save</b> to start the search.</li><li>✓ After you save and run the search, any results returned by the search are displayed in the results pane. Depending on how you have the preview setting configured, the search results are display or you have to click Preview results to view them. See the next section for details.</li><li>✓ To access this content search again or access other content searches listed on the Content search page, select the search and then click Open.</li><li>✓ To clear the results or create another search, click Add icon <b>New search</b>.</li><li>✓ You can <b>Export results</b> and <b>Export report</b></li></ul>	

### 3. What is Audit log search? How to perform it?

<b>Audit Log</b>	<ul style="list-style-type: none"><li>✓ Same as EAC except EAC has 8 different options available</li><li>✓ <b>Track user and administrative activity</b> within the tenant.</li><li>✓ Examples include changes made to Exchange Online and SharePoint Online tenant configuration settings, and changes made by users to documents and other items.</li><li>✓ Effectively manage <b>user experience, mitigate risks, and fulfill compliance obligations</b>.</li></ul>
<b>Permission</b>	<ul style="list-style-type: none"><li>✓ EAC Organization Management or,</li><li>✓ EAC Compliance Management or,</li><li>✓ MS 365 Global Admin</li></ul>
<b>Steps of - Audit log search</b>	<ul style="list-style-type: none"><li>✓ Navigation – <b>SCC &gt; Search &gt; Audit log search</b></li><li>✓ Step 1: <b>Run</b> an audit log search</li><li>✓ Step 2: <b>View</b> the search results</li><li>✓ Step 3: <b>Filter</b> the search results</li><li>✓ Step 4: <b>Export</b> the search results to a file</li></ul>

## W-4, D-3

### 4. What is the limitation of Content Search & Audit log search?

<b>Limitation of - Content Search</b>	<ul style="list-style-type: none"><li>✓ The maximum number of mailboxes in a Content Search that can be deleted 50,000</li><li>✓ The maximum number of user mailboxes in a Content Search that can be previewed 1,000</li><li>✓ Minimum alpha characters keyword 3</li><li>✓ Maximum number of items per user mailbox that are displayed 100</li><li>✓ The maximum number of items found in all user mailboxes that are displayed 1,000</li></ul>
<b>Limitation of - Audit Log Search</b>	<ul style="list-style-type: none"><li>✓ Download a maximum of <b>50,000</b> entries to a CSV file from a single audit log search.</li><li>✓ <b>Audit records</b> are retained for <b>90 days</b>.</li><li>✓ Take up to <b>30 minutes</b> or up to <b>24 hours</b> after to show the reports.</li><li>✓ Maximum date range of <b>90 days</b></li></ul>

### 5. What is eDiscovery? Use eDiscovery to export data.

<b>eDiscovery</b>	<ul style="list-style-type: none"><li>✓ Electronic Discovery</li><li>✓ <b>Process/single place</b> of identifying and delivering electronic information that can be used as evidence in <b>legal cases</b>.</li><li>✓ Search mailboxes and sites in the same eDiscovery search by using the Content Search tool.</li><li>✓ Core eDiscovery cases to identify, <b>hold</b>, and export content found in mailboxes and sites.</li><li>✓ Advance eDiscovery for E5 subscription</li></ul>
<ul style="list-style-type: none"><li>✓ Please Navigate to – <b>SCC &gt; eDiscovery &gt; eDiscovery &gt; +Create a Case &gt; Type Case Name &gt; Open</b></li><li>✓ There you will find three options available to perform – <b>Holds, Searches, Exports</b></li><li>✓ Holds – <b>+Create &gt; fill up choose location, create query &gt; press Save</b></li><li>✓ Searches – <b>+New Search &gt; fill up search query, location</b> (all locations, location on hold, specific location) <b>&gt; press Save</b></li><li>✓ Exports –</li></ul>	



## W-4, D-4

### 1. What is ATP? What are Safe Links and Safe Attachments?

<b>ATP</b>	<ul style="list-style-type: none"><li>✓ Advanced Threat Protection</li><li>✓ <b>Security solutions</b> that defend against sophisticated malware or hacking-based attacks targeting sensitive data</li><li>✓ Check emails after the message delivery to the recipient</li></ul>
<b>Features (ATP Plan-1)</b>	<ul style="list-style-type: none"><li>✓ Safe Attachments</li><li>✓ Safe links</li><li>✓ ATP Anti-phishing protection</li><li>✓ Real-time detection (nearly)</li></ul>
<b>Features (ATP Plan-2)</b>	<ul style="list-style-type: none"><li>✓ ATP Plan-1</li><li>✓ Threat tracker</li><li>✓ Threat explorer</li><li>✓ Attack simulator</li></ul>
<b>License Required</b>	<ul style="list-style-type: none"><li>✓ ATP Plan-1 (Business Premium)</li><li>✓ ATP Plan-2 (E5, A5)</li></ul>
<b>Safe Attachments</b>	<ul style="list-style-type: none"><li>✓ Provides <b>zero-day protection</b> to safeguard your messaging system, by checking email attachments for malicious content.</li><li>✓ Routes all messages and attachments that do not have a virus/malware signature to a special environment, and then uses <b>machine learning</b> and analysis techniques to detect malicious intent.</li><li>✓ If no suspicious activity is found, the message is forwarded to the mailbox.</li><li>✓ Default is <b>off</b></li></ul>
<b>Safe Links</b>	<ul style="list-style-type: none"><li>✓ Provides <b>time-of-click verification</b> of URLs, for example, in emails messages and Office files.</li><li>✓ Protection is ongoing and applies across your messaging and Office environment.</li><li>✓ Links are scanned for each click: safe links remain accessible and malicious links are dynamically blocked.</li><li>✓ Default is <b>off</b></li></ul>

## W-4, D-4

2. Explain types of actions can be taken on safe attachments.

Actions	Effect
Off (Default)	✓ Attachment will not be scanned for malware
Monitor	✓ Continue delivering the messages after malware is detected, track scan results
Block	✓ Block the current & future emails and attachments with detected malware
Replace	✓ Block the attachments with detected malware, continue to deliver the message
Dynamic Delivery	✓ Delivers the message without attachment immediately and reattach once scan is complete

3. What is the warning if I want to save the Dynamic Delivery options for safe attachment?

- ✓ Dynamic email delivery is for O365 hosted mailbox only.
- ✓ If this action is chosen for a recipient with a non-hosted mailbox, then a replace action will be taken for that recipient.

4. What is DLP? How to set up DLP?

<b>Data Loss Prevention</b>	<ul style="list-style-type: none"><li>✓ <b>Compliance feature</b> designed to help the organization prevent the <b>unintentional</b> or <b>accidental exposure</b> of <b>sensitive information</b> to <b>unwanted parties</b>.</li><li>✓ <b>Protect</b> identical sensitive information such as credit card numbers, social security numbers, or health records.</li><li>✓ DLP has its roots in Exchange Server and Exchange Online, and is also applicable in SharePoint Online and OneDrive for Business.</li></ul>
<b>License Required</b>	✓ Exchange Online plan-2 (included with E3, E5)

## W-4, D-4

Set up DLP from EAC
<ul style="list-style-type: none"><li>✓ Please go to – <a href="https://outlook.office365.com">https://outlook.office365.com</a></li><li>✓ Please navigate to – <b>Compliance management</b> &gt; <b>data loss prevention</b> &gt; click “+”</li></ul> <p>Choose any options –</p> <ul style="list-style-type: none"><li>✓ <b>New DLP policy from template</b></li><li>✓ <b>New DLP policy from custom template</b></li><li>✓ <b>New custom DLP policy</b></li></ul>
<ul style="list-style-type: none"><li>✓ Please type a suitable friendly name</li><li>✓ Choose a template</li><li>✓ Choose other options</li></ul>
<ul style="list-style-type: none"><li>✓ Click <b>Enforce</b></li></ul>

Set up DLP from SCC
<ul style="list-style-type: none"><li>✓ Please go to – <a href="https://protection.office.com">https://protection.office.com</a></li><li>✓ Please Navigate to- <b>Data loss prevention</b> &gt; <b>Policy</b> &gt; <b>+Create a policy</b></li></ul>
<ul style="list-style-type: none"><li>✓ You can select template to create policy or choose custom.</li></ul>
<ul style="list-style-type: none"><li>✓ Please type a suitable friendly name</li></ul>
<ul style="list-style-type: none"><li>✓ Choose a location for specific.</li></ul>
<ul style="list-style-type: none"><li>✓ Select Exchange Online only.</li></ul>
<ul style="list-style-type: none"><li>✓ To change policy settings, click <b>Edit</b></li></ul>
<ul style="list-style-type: none"><li>✓ Choose <b>Sensible info types</b></li></ul>
<ul style="list-style-type: none"><li>✓ Click <b>+ Add</b></li></ul>
<ul style="list-style-type: none"><li>✓ Select suitable template from the list.</li></ul>
<ul style="list-style-type: none"><li>✓ Block the user who try to send sensitive information.</li></ul>
<ul style="list-style-type: none"><li>✓ Review the settings again to confirm</li></ul> <ul style="list-style-type: none"><li>✓ Policy settings -</li></ul> <p>If the contents ..... Then notify people ..... If there are at least ..... instances of the same type of sensitive info, block access.....</p>

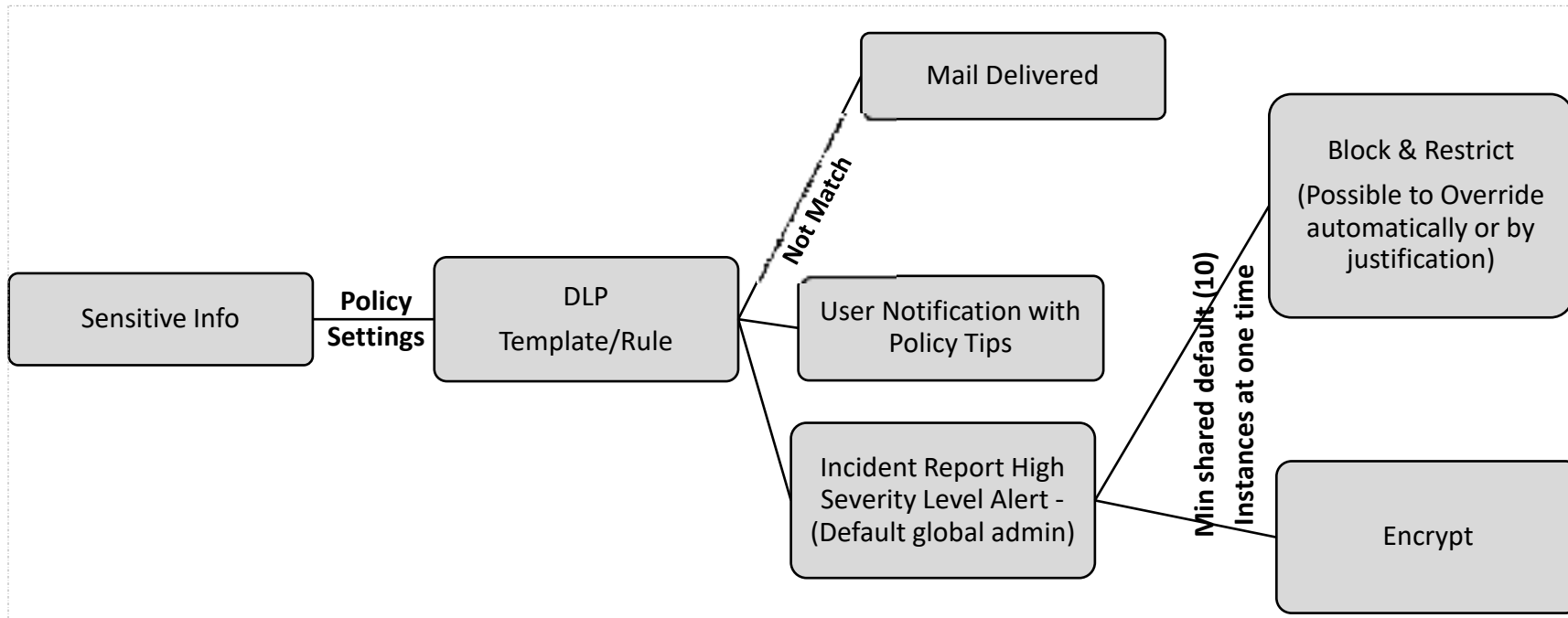
## **W-4, D-4**

### 5. What is ATP Attack Simulator?

- ✓ To run **nearly realistic attack scenarios** in your organization.
- ✓ Help to identify and find vulnerable users before a real attack impact
- ✓ Need to **enable MFA** before starting the simulator
- ✓ License – **ATP Plan-2**
- ✓ SCC permission - **Organization Management** or **Security Administrator**

## W-4, D-4

### 6. HOW DLP Works.



## W-4, D-5

1. How many types of mailbox migration methods are available?

<b>Cutover/Express</b>	<ul style="list-style-type: none"><li>✓ Migrate <b>all mailboxes at once</b> (cutover migration)</li><li>✓ <b>Exchange 2003-2013</b> only</li><li>✓ If there are fewer than <b>2000 mailboxes</b>.</li><li>✓ Recommended to migrate <b>150 users or less</b>.</li><li>✓ Migrate all <b>emails, contacts, calendars, tasks</b></li></ul>
<b>Staged</b>	<ul style="list-style-type: none"><li>✓ Migrate <b>all mailboxes</b> at an <b>interval of few days/weeks</b></li><li>✓ <b>Exchange 2003-2007</b> only</li><li>✓ If there are more than <b>2,000 mailboxes</b> but single batch max <b>2000 mailbox</b></li><li>✓ Migrate all <b>emails, contacts, calendars, tasks</b></li><li>✓ 30-days time to assign license after migration.</li></ul>
<b>Hybrid</b>	<ul style="list-style-type: none"><li>✓ To maintain both <b>on-premises</b> and <b>online mailboxes</b></li><li>✓ Gradually migrate users and email to Microsoft 365 or Office 365</li><li>✓ <b>Exchange 2010-2019</b></li><li>✓ <b>150-2,000 mailboxes</b></li><li>✓ Migrate all <b>emails, contacts, calendars, tasks</b></li></ul>
<b>IMAP</b>	<ul style="list-style-type: none"><li>✓ From third-party mails server such as gmail, yahoo etc</li><li>✓ Migrate only <b>emails</b>, not contacts &amp; calendars &amp; tasks</li><li>✓ Max <b>500,000 mailboxes</b></li><li>✓ Max <b>365 MB</b> per message</li><li>✓ Need to create mailbox in EAC before starting migration process</li></ul>
<b>G-Suite</b>	<ul style="list-style-type: none"><li>✓ Similar service like Exchange online from Google</li><li>✓ Migrate only <b>emails</b>, not contacts &amp; calendars</li><li>✓ Account owners must create an <b>app password</b> to access their account. This is because Google considers Outlook to be a less secure app and will not allow a connection to it with a password alone.</li></ul>

2. Explain the difference between migration types.

<b>Cutover/Express</b>	<b>Staged</b>	<b>Hybrid</b>
Exchange 2003-2013	Exchange 2003-2007	Exchange 2010-2019
Small organization	Medium organization	Large organization
Less than 2000 mailboxes (less than 150 mailboxes recommended)	More than 2000 mailboxes (a single batch 2000 maximum)	150-2000 mailboxes
All at once	Every after certain interval	Both Exchange Server & Online

## **W-4, D-5**

### 3. How to create an endpoint for migration in Exchange Online Admin Center?

- ✓ **Step 1: Create a migration endpoint**
  - Prior to performing on-boarding and off-boarding remote move migrations in an Exchange hybrid deployment, we recommend that you create Exchange remote migration endpoints. The migration endpoint contains the connection settings for an on-premises Exchange server that is running the MRS proxy service, which is required to perform remote move migrations to and from Exchange Online.
- ✓ **Step 2: Enable the MRSPProxy service**
  - If the MRSPProxy service isn't already enabled for your on-premises Exchange servers, follow these steps in the Exchange admin center (EAC):
- ✓ **Step 3: Use the EAC to move mailboxes**
  - You can use the remote move migration wizard on the Office 365 tab in the EAC on an Exchange server to either move existing user mailboxes in the on-premises organization to the Exchange Online organization or to move Exchange Online mailboxes to the on-premises organization. Choose one of the following procedures:
- ✓ **Step 4: Remove completed migration batches**
  - After your mailbox moves have completed, we recommend removing the completed migration batches to minimize the likelihood of errors if the same users are moved again.
- ✓ **Step 5: Re-enable offline access for Outlook on the web**
  - Offline access in Outlook on the web lets users access their mailbox when they're not connected to a network. If you migrate Exchange mailboxes to Exchange Online, users have to reset the offline access setting in their browser to use Outlook on the web offline.

## W-4, D-5

4. Explain the process to initiate IMAP/Cutover/Staged migration?

No	IMAP	Cutover	Staged
01	Add users and assign license	Prepare	Prepare
02	Prepare IMAP server and get information	Verify domain (TXT)	Verify domain (TXT)
03	Communicate changes to users IMAP		Use directory synchronization to user
04	Setup admin credentials or get or reset user email password from IMAP server		Create a list of mailboxes
05	Create list of mailboxes to migrate (CSV file)	Create Mail enabled Security Group	
06	Connect office 365 to email system	Connect Microsoft 365 to email system	Connect Microsoft 365 to email system
07	Migrate mailboxes	Migrate mailboxes	Migrate mailboxes
08	Routing email to O365 (MX)	Routing email to O365 (MX)	Routing email to O365 (MX)
09	Verify routing, then stop email synchronization	Delete the cutover migration batch	Delete the cutover migration batch
10		Assign licenses	Assign licenses
11	Welcome letter to users	Welcome letter to user	Welcome letter to user

5. Which items can or cannot be migrated using IMAP migration?

IMAP	<ul style="list-style-type: none"><li>✓ From third-party mails server such as gmail, yahoo etc</li><li>✓ Migrate only <b>emails</b>, not contacts &amp; calendars &amp; tasks</li><li>✓ Max <b>500,000 mailboxes</b></li><li>✓ Max <b>35 MB</b> per message</li><li>✓ Need to create mailbox in EAC before starting migration process</li></ul>
------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



## W-4, D-5

6. Name the port numbers that are required in hybrid deployment.

PORT	DESCRIPTION	ON-PREMISES ENDPOINT	
TCP 25 (SMTP)	SMTP mail flow between Microsoft 365 and on-premises Exchange	Exchange 2016, 2019	Mailbox/Edge
		Exchange 2013	CAS/Edge
		Exchange 2010	Hub/Edge
TCP 443 (HTTPS)	Autodiscover	Exchange 2016, 2019	Mailbox server: /autodiscover/autodiscover.svc/wssecurity
		Exchange 2010, 2013	CAS: /autodiscover/autodiscover.svc
TCP 443 (HTTPS)	Free/busy, MailTips, and message tracking (EWS)	Exchange 2010 - 2019	CAS: /ews/exchange.asmx/wssecurity
TCP 443 (HTTPS)	Multi-mailbox search (EWS)	Exchange 2010 - 2019	CAS: /ews/exchange.asmx/wssecurity /autodiscover/autodiscover.svc/wssecurity /autodiscover/autodiscover.svc
TCP 443 (HTTPS)	Mailbox migrations (EWS)	Exchange 2010 - 2019	CAS: /ews/mrsproxy.svc
TCP 443 (HTTPS)	OAuth (Autodiscover and EWS)	Exchange 2010 - 2019	CAS: /ews/exchange.asmx/wssecurity /autodiscover/autodiscover.svc/wssecurity /autodiscover/autodiscover.svc
TCP 443 (HTTPS)	AD FS (Windows Server)	Windows 2012 R2/2016	Server: /adfs/*
TCP 443 (HTTPS)	AAD Connect	Windows 2012 R2/2016	Server (AD FS): /adfs/*

7. What is HCW?

HCW	<ul style="list-style-type: none"> <li>✓ Hybrid Configuration Wizard</li> <li>✓ To deploy hybrid environment</li> <li>✓ To configure your local domain and Office 365 tenant, so that on-premises Exchange can merge with Exchange Online, resulting in the creation of a single, hybrid organization.</li> <li>✓ Need Credential of an On-premises Exchange user who is a member of the Domain Admin security group.</li> <li>✓ Credential of the Office 365 Global Administration Office 365 plan which supports hybrid deployment (Enterprise, Government, Academic or Midsize)</li> <li>✓ Can be downloaded only with Internet Explorer</li> </ul>
-----	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------