



- Expert Verified, Online, **Free**.

Custom View Settings

**Overview -**

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide. Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

**Existing Environment -****Active Directory Environment -**

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

**Network Infrastructure -**

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as DNS servers.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

**Requirements -****Planned Changes -**

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

**Technical Requirements -**

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.

Microsoft 365 Apps for enterprise applications must be installed from a network share only.

Disruptions to email access must be minimized.

**Application Requirements -**

Fabrikam identifies the following application requirements:

An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.

The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

**Security Requirements -**

Fabrikam identifies the following security requirements:

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.

After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.

The principle of least privilege must be used.

You are evaluating the required processes for Project1.

You need to recommend which DNS record must be created while adding a domain name for the project.

Which DNS record should you recommend?

- A. host (A)
- B. host information (HINFO)
- C. text (TXT)
- D. pointer (PTR)

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **mikl** 1 month, 1 week ago

C for me as well.

<https://learn.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide#add-a-domain>  
upvoted 1 times

 **Casticod** 2 months ago

**Selected Answer: C**

Its the first Step, C Correct

upvoted 2 times

 **osxvkwpfcfxobqjby** 2 months, 1 week ago

**Selected Answer: C**

Before you start you have to verify your custom domain with a TXT record.

<https://learn.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide>  
upvoted 3 times

**Overview -**

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

**Existing Environment -****Active Directory Environment -**

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

**Network Infrastructure -**

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as DNS servers.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

**Requirements -****Planned Changes -**

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

**Technical Requirements -**

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.

Microsoft 365 Apps for enterprise applications must be installed from a network share only.

Disruptions to email access must be minimized.

**Application Requirements -**

Fabrikam identifies the following application requirements:

An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.

The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

**Security Requirements -**

Fabrikam identifies the following security requirements:

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.

After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.

The principle of least privilege must be used.

You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.

Which authentication strategy should you implement for the pilot projects?

- A. pass-through authentication

- B. pass-through authentication and seamless SSO
- C. password hash synchronization and seamless SSO
- D. password hash synchronization

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉️  **osxvkwpfcfxobqjby** Highly Voted  2 months, 1 week ago

**Selected Answer: C**

"Users must be able to authenticate to cloud services if Active Directory becomes unavailable." That would be hash sync. Pass-through with fallback is also possible but more work to implement and maintain.

"After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically." that's the SSO.

upvoted 9 times

✉️  **PMR24875** 1 month, 1 week ago

Did the question change because is see "After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN." under security requirements which made me choose D

upvoted 1 times

✉️  **PMR24875** 1 month, 1 week ago

Never mind, didn't read well enough

upvoted 1 times

✉️  **letters1234** Most Recent  1 month, 3 weeks ago

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/choose-ad-authn>

upvoted 1 times

✉️  **Greatone1** 1 month, 3 weeks ago

**Selected Answer: C**

C is the correct answer

<https://www.examtopics.com/discussions/microsoft/view/11890-exam-ms-100-topic-15-question-3-discussion/>

upvoted 2 times

**Overview -**

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

**Existing Environment -****Active Directory Environment -**

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

**Network Infrastructure -**

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as DNS servers.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

**Requirements -****Planned Changes -**

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

**Technical Requirements -**

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.

Microsoft 365 Apps for enterprise applications must be installed from a network share only.

Disruptions to email access must be minimized.

**Application Requirements -**

Fabrikam identifies the following application requirements:

An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.

The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

**Security Requirements -**

Fabrikam identifies the following security requirements:

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.

After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.

The principle of least privilege must be used.

Which role should you assign to User1?

A. Hygiene Management

B. Security Reader

C. Security Administrator

D. Records Management

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **osxvkwpfcfxobqjby** Highly Voted  2 months, 1 week ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/purview/microsoft-365-compliance-center-permissions>

upvoted 5 times

 **imlearningstuffagain** Most Recent  1 week ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/answers/questions/1297022/view-the-reports-for-dlp-on-the-compliance-center>

upvoted 1 times

 **Nilz76** 2 weeks ago

**Selected Answer: B**

The Security Reader role in Microsoft 365 provides permissions to read security information and reports. The main task for User1 as per the scenario is to view DLP reports, and this role provides the necessary permissions for that task without granting extra, potentially unnecessary, permissions.

upvoted 3 times

**HOTSPOT -****Overview -**

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide. Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

**Existing Environment -****Active Directory Environment -**

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

**Network Infrastructure -**

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as DNS servers.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

**Requirements -****Planned Changes -**

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

**Technical Requirements -**

Fabrikam identifies the following technical requirements:

All users must be able to exchange email messages successfully during Project1 by using their current email address.

Users must be able to authenticate to cloud services if Active Directory becomes unavailable.

A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.

Microsoft 365 Apps for enterprise applications must be installed from a network share only.

Disruptions to email access must be minimized.

**Application Requirements -**

Fabrikam identifies the following application requirements:

An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.

The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

**Security Requirements -**

Fabrikam identifies the following security requirements:

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.

After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.

The principle of least privilege must be used.

You create the Microsoft 365 tenant.

You implement Azure AD Connect as shown in the following exhibit.

# Azure Active Directory admin center

» Home > Azure AD Connect

## Azure AD Connect

Azure Active Directory

Troubleshoot

Refresh

### SYNC STATUS



Sync Status

Enabled

Last Sync

Less than 1 hour ago

Password Hash Sync

Enabled

### USER SIGN-IN



Federation

Disabled

0 domains

Seamless single sign-on

Disabled

0 domains

Pass-through authentication

Disabled

0 agents

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

#### Answer Area

During Project1, sales department users can access [answer choice] applications by using SSO.

both on-premises and cloud-based  
only cloud-based  
only on-premises

If Active Directory becomes unavailable during Project1, sales department users can access the resources [answer choice].

both on-premises and in the cloud  
in the cloud only  
on-premises only

#### Answer Area

During Project1, sales department users can access [answer choice] applications by using SSO.

both on-premises and cloud-based  
only cloud-based  
only on-premises

#### Correct Answer:

If Active Directory becomes unavailable during Project1, sales department users can access the resources [answer choice].

both on-premises and in the cloud  
in the cloud only  
on-premises only

osxvkwpfcfxobqjby 2 months, 1 week ago

only on-prem: no sso configured in ADConnect

in the cloud only: AD is not available, assuming that the on-prem app use AD to authenticate users. Exchange online is still usable because of pass hash sync.

upvoted 9 times

 **CBZ57** Most Recent 1 week, 2 days ago

1. Hash Password ENabled so you can access to both
  2. cloud only
- upvoted 2 times

 **CheMetto** 1 day, 14 hours ago

it's asking applications, not mailbox. So during project 1, 100 users mailbox will be moved to M365, during project 2 all sales department will gain access to teams.. In my opinion is only on prem for the first 1 and cloud only for the second one.

upvoted 1 times

 **CheMetto** 1 day, 14 hours ago

mmh sorry, application using sso\*. Still on prem for the first 1, because no SSO enabled in AAD ( we don't see staging option, but i don't think they are using it ).

upvoted 1 times

 **gomezmax** 1 month, 3 weeks ago

Correct

upvoted 1 times

Your company has a Microsoft 365 subscription.

You need to identify all the users in the subscription who are licensed for Office 365 through a group membership. The solution must include the name of the group used to assign the license.

What should you use?

- A. Active users in the Microsoft 365 admin center
- B. Reports in Microsoft Purview compliance portal
- C. the Licenses blade in the Microsoft Entra admin center
- D. Reports in the Microsoft 365 admin center

**Correct Answer: D**

*Community vote distribution*

C (100%)

✉  **osxzkwpfcfxobqjby** Highly Voted 2 months, 1 week ago

**Selected Answer: C**

There is no license report in "Reports in the Microsoft 365 admin center".

<https://entra.microsoft.com> > Billing > Licenses > All Products > Open License > Licensed groups  
upvoted 11 times

✉  **larteyotoo** Most Recent 4 days, 20 hours ago

C is Correct

upvoted 1 times

✉  **Nilz76** 2 weeks ago

**Selected Answer: C**

Answer is C: The Licenses blade in the Microsoft Entra admin center. The Licenses blade is where you would manage group-based licensing. Here, you can see which groups have licenses assigned and the members of those groups.

upvoted 1 times

✉  **sherifhamed** 2 weeks, 6 days ago

**Selected Answer: C**

The best option to identify all the users in the subscription who are licensed for Office 365 through a group membership is  
C. the Licenses blade in the Microsoft Entra admin center.

upvoted 2 times

✉  **ATHOOS** 1 month, 2 weeks ago

**Selected Answer: C**

Correct Answer is C

upvoted 2 times

✉  **gomezmax** 1 month, 3 weeks ago

D is wrong Answer, the Answer should be Is C

upvoted 3 times

✉  **Greatone1** 1 month, 4 weeks ago

**Selected Answer: C**

C is correct

In the Azure AD Admin Center, select Azure Active Directory then select Licenses to open the Licenses blade. From there you need to click on the 'Managed your purchased licenses link'. Select a license you want to view,

upvoted 4 times

✉  **Dtriminio** 2 months, 1 week ago

**Selected Answer: C**

C is correct

upvoted 3 times

**HOTSPOT -**

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Type	Department
User1	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support.

How should you complete the membership rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

(user.userType ) and (user.department

<input type="checkbox"/> -eq "Guest" <input type="checkbox"/> -in "Guest" <input type="checkbox"/> -ne "Guest" <input type="checkbox"/> -notmatch "Member"	<input type="checkbox"/> -contains "Support" <input type="checkbox"/> -in "Support" <input type="checkbox"/> -match "Support" <input type="checkbox"/> -startsWith "Sup"
---	---

**Answer Area**

Correct Answer:

(user.userType ) and (user.department

<input checked="" type="checkbox"/> -eq "Guest" <input type="checkbox"/> -in "Guest" <input type="checkbox"/> -ne "Guest" <input type="checkbox"/> -notmatch "Member"	<input checked="" type="checkbox"/> -contains "Support" <input type="checkbox"/> -in "Support" <input type="checkbox"/> -match "Support" <input type="checkbox"/> -startsWith "Sup"
--	--

✉  **Jslei** 1 month ago

just tested this, both contains and match will work with department  
upvoted 2 times

✉  **imlearningstuffagain** 1 week ago

Microsoft recommends to limit the Match clause and use Contains (ref: <https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-rule-more-efficient>)  
upvoted 1 times

✉  **gomezmax** 1 month ago

Correct

upvoted 2 times

✉  **vinch** 1 month, 1 week ago

Good answer is -eq -match  
upvoted 1 times

✉  **nenge** 1 month, 2 weeks ago

This can be tricky if you're used to PowerShell syntax. In PS syntax, "-contains" would be incorrect as it checks for an item in a collection, not partial matches. In dynamic group syntax, it's the opposite. In dynamic group syntax, "-contains" matches partial strings, not items in collections.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#supported-expression-operators>  
upvoted 1 times

✉  **Perycles** 2 months, 1 week ago

Correct answers

(user.department -contains "Support") and (user.userType -eq "Guest")

Be carrefull : Case Sensitive

upvoted 4 times

**HOTSPOT -**

Your company uses a legacy on-premises LDAP directory that contains 100 users.

The company purchases a Microsoft 365 subscription.

You need to import the 100 users into Microsoft 365 by using the Microsoft 365 admin center.

Which type of file should you use and which properties are required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

File type to use:

- CSV
- JSON
- PST
- XML

Required properties for each user:

- Display Name and Department
- First Name and Last Name
- User Name and Department
- User Name and Display Name

**Answer Area**

File type to use:

- CSV
- JSON
- PST
- XML

Correct Answer:

Required properties for each user:

- Display Name and Department
- First Name and Last Name
- User Name and Department
- User Name and Display Name

 **Perycles** Highly Voted 2 months, 1 week ago

CSV file type

"displayName" and "User Name" are mandatory

ref: <https://learn.microsoft.com/fr-fr/training/modules/manage-accounts-licenses-microsoft-365/7-perform-bulk-user-maintenance>  
upvoted 8 times

 **gomezmax** Most Recent 1 month ago

Correct

upvoted 1 times

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Department
User1	Human resources
User2	Research
User3	Human resources
User4	Marketing

You need to configure group-based licensing to meet the following requirements:

To all users, deploy an Office 365 E3 license without the Power Automate license option.

To all users, deploy an Enterprise Mobility + Security E5 license.

To the users in the research department only, deploy a Power BI Pro license.

To the users in the marketing department only, deploy a Visio Plan 2 license.

What is the minimum number of deployment groups required?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **Perycles** Highly Voted 2 months, 1 week ago

3 groups needed :

- Group 1 : Allusers (deploy EMS+S E5 licence and O365 E3 licence with "PowerAutomate for Office 365" disabled).
- group 2 : "Research group" : deploy Power Bi Pro Licence (not included in O365 E3 but in O365 E5).
- Group 3 : "Marketing group" deploy Visio plan 2 Licence.

upvoted 11 times

 **letters1234** Most Recent 1 month, 3 weeks ago

**Selected Answer: C**

All users and the two deparments, three groups

upvoted 2 times

You have a Microsoft 365 subscription.

You view the Service health Overview as shown in the following exhibit.

## Service health

October 18, 2022 4:20 PM

Overview Issue history Reported issues

View the issues and health status of all services that are available with your current subscriptions. [Learn more about Service Health](#)

 Report an issue  Customize



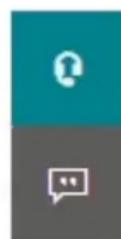
### Active issues

Issue title	Affected service	Issue type
> Microsoft service health (6)		
Issues in your environment that require action (0)		

### Microsoft service health

Shows the current health status of your Microsoft services, and updates when we fix issues.

Service	Status
Exchange Online	 3 advisories
Microsoft 365 suite	 2 advisories
Microsoft Teams	 1 advisory
OneDrive for Business	 1 advisory
SharePoint Online	 2 advisories



You need to ensure that a user named User1 can view the advisories to investigate service health issues.

Which role should you assign to User1?

- A. Message Center Reader
- B. Reports Reader
- C. Service Support Administrator
- D. Compliance Administrator

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **Nilz76** 2 weeks ago

**Selected Answer: C**

The role that would be relevant for viewing advisories to investigate service health issues is the Service Support Administrator role. This role is designed to enable individuals to investigate and troubleshoot service issues, making it a fitting choice for the task described.

Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:

- Open and manage service requests
- View and share message center posts
- Monitor service health

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide>

upvoted 1 times

 **rfree** 1 month, 2 weeks ago

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide>

People who are assigned the global admin or service support admin role can view service health.

upvoted 1 times

 **stai** 1 month, 3 weeks ago

Answer A is correct.

Message Center Reader

[Users in this role can monitor notifications and advisory health updates in Message center for their organization on configured services such as Exchange, Intune, and Microsoft Teams.]

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

upvoted 1 times

 **Casticod** 1 month, 3 weeks ago

Message center it's not the same of service health

upvoted 1 times

 **letters1234** 1 month, 3 weeks ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide#commonly-used-microsoft-365-admin-center-roles>

Service Support Admin - Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:

- Open and manage service requests
- View and share message center posts
- Monitor service health

upvoted 3 times

 **Casticod** 2 months ago

**Selected Answer: C**

In the link post by Venusasur, Search Service support administrator, and see the table

upvoted 2 times

 **Venusaur** 2 months, 1 week ago

Answer C is correct.

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide&redirectSourcePath=%252fen-us%252farticle%252fabout-office-365-admin-roles-da585eea-f576-4f55-a1e0-87090b6aaa9d>

upvoted 4 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:

Scope type: Directory -

Selected members: Group1 -

Assignment type: Active -

Assignment starts: Mar 15, 2023 -

Assignment ends: Aug 15, 2023 -

You add the following assignment for the Exchange Administrator role:

Scope type: Directory -

Selected members: Group2 -

Assignment type: Eligible -

Assignment starts: Jun 15, 2023 -

Assignment ends: Oct 15, 2023 -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
On July 15, 2023, Admin1 can reset the password of a user.	<input type="radio"/>	<input type="radio"/>
On June 20, 2023, Admin2 can manage Microsoft Exchange Online.	<input type="radio"/>	<input type="radio"/>
On May 1, 2023, Admin3 can reset the password of a user.	<input type="radio"/>	<input type="radio"/>

**Answer Area****Statements**

On July 15, 2023, Admin1 can reset the password of a user.

Yes

No

Correct Answer:

On June 20, 2023, Admin2 can manage Microsoft Exchange Online.

No

Yes

On May 1, 2023, Admin3 can reset the password of a user.

No

Yes

  Casticod 2 months ago

Yes, Yes, Yes ??

upvoted 10 times

  CheMetto 1 day, 14 hours ago

Yes no Yes. The second is no. It's eligible, Admin 2 has to activate the role then he can manage Exchange Online. for put a yes, the answer should be "Admin 2, after activate his role, can manage exchange online?" -> yes.

upvoted 1 times

✉ **Darekms0** 2 days, 1 hour ago

You need "organization management" role in other manage Exchange . YNY

upvoted 1 times

✉ **Nilz76** 2 weeks ago

Here are my thoughts and explainations:

Q: On July 15, 2023, admin 1 can reset the password of a user.

A: Yes. Admin 1 is a member of Group 1, which has been assigned the User Administrator role actively from March 15, 2023, to August 15, 2023. This role permits password reset actions among others.

Q: On June 20, 2023, admin 2 can manage Microsoft Exchange Online.

A: Yes, but with a condition. Admin 2 is a member of Group 2, which has been assigned the Exchange Administrator role as eligible from June 15, 2023, to October 15, 2023. However, since the assignment type is "Eligible," admin 2 needs to activate the role to perform the Exchange Administrator tasks. Once activated, admin 2 can manage Microsoft Exchange Online.

Q: On May 1, 2023, admin 3 can reset the password of a user.

A: Yes. Admin 3 is a member of both Group 1 and Group 2. Since Group 1 has the User Administrator role assigned actively from March 15, 2023, to August 15, 2023, admin 3 can reset the password of a user during this period.

Yes, Yes, Yes

upvoted 2 times

✉ **amurp35** 1 month ago

I want to say YYY is likely correct, considering that Admin 2 has eligible assignment and the whole reason to assign someone as eligible to a role is to be able to grant that permission in the first place. So there is nothing in the shown settings that prevents Admin 2 from doing so, though we don't know if they will need to be approved for it or not.

upvoted 1 times

✉ **mpetlk** 1 month ago

I guess it should be Yes, No, Yes as it says in MS

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/groups-assign-member-owner>

Eligible assignment requires member or owner to perform an activation to use the role. Activations may also require providing a multi-factor authentication (MFA), providing a business justification, or requesting approval from designated approvers.

Important

For groups used for elevating into Azure AD roles, Microsoft recommends that you require an approval process for eligible member assignments. Assignments that can be activated without approval can leave you vulnerable to a security risk from another administrator with permission to reset an eligible user's passwords.

Active assignments don't require the member to perform any activations to use the role. Members or owners assigned as active have the privileges assigned to the role at all times.

upvoted 1 times

✉ **vercracked\_007** 1 month, 1 week ago

YNY

Statement 2 doesn't say that admin to activates his role

upvoted 2 times

✉ **AMdf** 1 month, 2 weeks ago

Yes

?? - It depends

Yes

upvoted 2 times

✉ **Tedd\_TS** 2 months ago

Yes, Yes, Yes i think too

upvoted 2 times

✉ **Venusaur** 2 months, 1 week ago

[ ] On May 1, 2023, Admin3 can reset the password of a user.

This should be YES right?

Admin3 is member of Group1 + Group2

Group1 assignment start from Mar 15 2023 to Aug 15 2023.

May 1 2023 should be within the range.

upvoted 3 times

✉ **osxzkwpfcfxobqjby** 2 months, 1 week ago

- Y

Admin1 in Group1 has an active assignment for the User Administrator Role between mar 15 and aug 15.

- Y

This one is questionable. Admin2 in Group2 has an eligible assignment for the Exchange Administrator role from Jun 15 til Oct 15. It depends on the eligible assignment type. When MFA or justification is selected, the answer would be Y. But if approved is selected, it depends on approval of the request if admin2 can manage Exchange.

- N

Not in the right date range

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user#assign-a-role>  
upvoted 4 times

 **cb0900** 1 month, 4 weeks ago

Agree Admin2 is questionable. Does MS mark the answer where Admin2 manages to activate the Exchange Admin role (although this isn't mentioned in the question) then Y, or Admin2 doesn't take any action and as it's Eligible then answer is N.

upvoted 2 times

 **gbartumeu** 2 months ago

Admin3 is member of Group 1, and May 01, 2023 is in the date range (Mar 15, 2023 to Aug 15, 2023)

upvoted 8 times

You have a Microsoft 365 subscription.

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Global Administrator
User3	Service Support Administrator

You configure Tenant properties as shown in the following exhibit.

#### Technical contact

User1@contoso.com

#### Global privacy contact



#### Privacy statement URL

http://contoso.com/privacy

Which users will be contacted by Microsoft if the tenant experiences a data breach?

- A. User1 only
- B. User2 only
- C. User3 only
- D. User1 and User2 only
- E. User2 and User3 only

#### Correct Answer: B

##### Community vote distribution

B (60%) D (40%)

**gbartumeu** Highly Voted 1 month ago

##### Selected Answer: B

"Global privacy contact: Type the email address for the person to contact for inquiries about personal data privacy. This person is also who Microsoft contacts if there's a data breach related to Azure Active Directory services. If there's no person listed here, Microsoft contacts your Global Administrators."

Source: <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/properties-area>  
upvoted 12 times

**ae88d96** Highly Voted 1 month, 2 weeks ago

##### Selected Answer: D

Correct answer is D, see explanation below:

User1 is Security Administrator and Technical Contact hence he will receive a notification for being Technical Contact.  
User2 is Global Administrator so he will receive a notification as well.  
User3 is Service Support Administrator so he won't receive a notification.

Reference: <https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-azure-dynamics#customer-notification>

If warranted, one or more of the following roles may be notified via email of a security or privacy incident in conjunction with, or in lieu of, a service health notification:

Azure Subscription Administrators or Owners  
Azure Active Directory Global Tenant Administrators  
Azure Active Directory Tenant Technical Contacts

upvoted 7 times

**WORKTRAIN** 1 week, 3 days ago

Good point. Except for the Security Administrator. I don't agree, because the definition of the technical contact is this:  
<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/properties-area>

This is something different than the Security Administrator.

The technical contact is not in the answer. Therefore I choose answer B.

upvoted 1 times

✉️  **imlearningstuffagain** Most Recent 1 week ago

**Selected Answer: B**

Fully agree.

upvoted 1 times

✉️  **Nilz76** 2 weeks ago

**Selected Answer: D**

In the event of a data breach or any other significant security issue, Microsoft typically contacts the technical contact specified in the tenant properties, as well as the Global Administrator(s). In this scenario, User 1 is set as the technical contact, and User 2 is a Global Administrator.

D. User1 and User2 only

upvoted 1 times

✉️  **jt2214** 2 weeks, 2 days ago

**Selected Answer: B**

I'm going to go with B because the global privacy contact is blank.

"Global privacy contact. Type the email address for the person to contact for inquiries about personal data privacy. This person is also who Microsoft contacts if there's a data breach related to Microsoft Entra services. If there's no person listed here, Microsoft contacts your Global Administrators. For Microsoft 365 related privacy incident notifications,"

upvoted 2 times

✉️  **ZNZ** 2 weeks, 5 days ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/properties-area>

Technical contact. Type the email address for the person to contact for technical support within your organization.

Global privacy contact. Type the email address for the person to contact for inquiries about personal data privacy. This person is also who Microsoft contacts if there's a data breach related to Microsoft Entra services. If there's no person listed here, Microsoft contacts your Global Administrators. For Microsoft 365 related privacy incident notifications, see Microsoft 365 Message center FAQs

upvoted 1 times

✉️  **GenPatton** 3 weeks, 4 days ago

**Selected Answer: B**

"As noted previously, Microsoft 365 is committed to notifying customers within 72 hours of breach declaration. The customer's tenant administrator will be notified. Additionally, Microsoft 365 recommends that customers designate one or more individuals as Message Center Privacy readers" source: <https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365>

And "Only global administrators and Message center privacy readers can read data privacy messages." Source: <https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?preserve-view=true&view=o365-worldwide#commonly-used-microsoft-365-admin-center-roles>

And thus the answer is B.

upvoted 2 times

✉️  **gomezmax** 1 month ago

Correct B User 2

upvoted 1 times

✉️  **nielsh0172** 1 month, 2 weeks ago

**Selected Answer: D**

I agree with ae88d96

upvoted 1 times

✉️  **letters1234** 1 month, 3 weeks ago

**Selected Answer: D**

"If the TENANT experiences data breach" which would be the Azure Tenant. It's not the Microsoft 365 notification policy as that would be for 365 services.

<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-azure-dynamics#customer-notification>

If warranted, one or more of the following roles may be notified via email of a security or privacy incident in conjunction with, or in lieu of, a service health notification:

- Azure Subscription Administrators or Owners
- Azure Active Directory Global Tenant Administrators
- Azure Active Directory Tenant Technical Contacts

upvoted 2 times

✉️  **Greatone1** 1 month, 3 weeks ago

**Selected Answer: B**

It should be B

If warranted, one or more of the following roles may be notified via email of a security or privacy incident in conjunction with, or in lieu of, a service health notification:

Azure Subscription Administrators or Owners  
Azure Active Directory Global Tenant Administrators  
Azure Active Directory Tenant Technical Contacts

upvoted 1 times

 **Casticod** 2 months ago

**Selected Answer: D**

The question says which roles can do it, therefore the usual condition of least privileges does not apply, have to mention all the ones that can, therefore Global and Security administrator can contact (D)

upvoted 2 times

 **Casticod** 2 months ago

Please admin delete my post, Rethinking de Answer The correct it's B

upvoted 1 times

 **Dtriminio** 2 months, 1 week ago

**Selected Answer: B**

As noted previously, Microsoft 365 is committed to notifying customers within 72 hours of breach declaration. The customer's tenant administrator will be notified.

<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365>

upvoted 3 times

Your network contains an Active Directory forest named contoso.local.

You purchase a Microsoft 365 subscription.

You plan to move to Microsoft 365 and to implement a hybrid deployment solution for the next 12 months.

You need to prepare for the planned move to Microsoft 365.

What is the best action to perform before you implement directory synchronization? More than one answer choice may achieve the goal. Select the BEST answer.

- A. Purchase a third-party X.509 certificate.
- B. Create an external forest trust.
- C. Rename the Active Directory forest.
- D. Purchase a custom domain name.

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **Greatone1** Highly Voted 2 months ago

**Selected Answer: D**

Given answer is correct

upvoted 5 times

 **Nilz76** Most Recent 2 weeks ago

**Selected Answer: D**

D. Purchase a custom domain name

The best action to take before implementing directory synchronization for a hybrid deployment with Microsoft 365 would be to purchase a custom domain name. When you set up Microsoft 365, you're prompted to provide your domain name. This domain should match the domain you use within your on-premises Active Directory environment to ensure a seamless user experience and email delivery.

upvoted 1 times

 **CheMetto** 1 day, 14 hours ago

The problem is that the domain TLD is local. You can't purchase a domain named contoso.local, no one can sell it because is a special name used by iana... so as first step i guess you should rename your domain, then purchase a custom domain name

upvoted 1 times

You have a Microsoft 365 subscription.

You configure a new Azure AD enterprise application named App1. App1 requires that a user be assigned the Reports Reader role.

Which type of group should you use to assign the Reports Reader role and to access App1?

- A. a Microsoft 365 group that has assigned membership
- B. a Microsoft 365 group that has dynamic user membership
- C. a security group that has assigned membership
- D. a security group that has dynamic user membership

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **osxvkwpfcfxobqjby** Highly Voted  2 months, 1 week ago

**Selected Answer: C**

You can not assign Azure AD roles to dynamic groups. And you don't need a mailbox/sharepoint/etc, so it is not a 365 group.  
upvoted 8 times

 **Nilz76** Most Recent  2 weeks ago

**Selected Answer: C**

Answer is C. "a security group that has assigned membership"

Azure AD roles can't be assigned to dynamic groups, they can only be assigned to users or non-dynamic (assigned) groups. Dynamic groups in Azure AD are primarily used for automatic membership management based on user attributes, but they don't extend to managing role assignments.

For assigning Azure AD roles, we would typically use assigned groups or assign the roles directly to individual users.  
upvoted 2 times

 **sherifhamed** 2 weeks, 6 days ago

**Selected Answer: C**

The correct answer is C. a security group that has assigned membership. This type of group can be used to assign users and groups to an enterprise application and to a specific app role

Option A. a Microsoft 365 group that has assigned membership is not correct because Microsoft 365 groups are not supported for app role assignment

Option B. a Microsoft 365 group that has dynamic user membership is not correct because Microsoft 365 groups are not supported for app role assignment

Option D. a security group that has dynamic user membership is not correct because security groups with dynamic membership are not supported for app role assignment

upvoted 2 times

You have a new Microsoft 365 E5 tenant.

You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.

What should you do first?

- A. Enable auditing.
- B. Enable Microsoft 365 usage analytics.
- C. Create an Insider risk management policy.
- D. Create a communication compliance policy.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **Nilz76** 2 weeks ago

**Selected Answer: A**

A. Enable auditing

The first step you should take is to Enable auditing.

In order to monitor and get alerted on specific activities such as elevation of administrative privileges, auditing needs to be enabled in your Microsoft 365 environment. Auditing will record events such as changes in permissions and other administrative activities, which can then be monitored through alert policies to notify administrators when specific events occur.

upvoted 3 times

 **anonavia** 1 month, 4 weeks ago

**Selected Answer: A**

-A

When an elevation of Microsoft Exchange Online administrative privileges is detected in your Microsoft 365 E5 tenant, you should first enable auditing.

upvoted 3 times

 **osxzkwpfcfxobqjby** 2 months, 1 week ago

- A

But, question makes no sense. Audit is enabled by default. All other options are less obvious.

<https://learn.microsoft.com/en-us/purview/audit-solutions-overview#audit-standard>

upvoted 1 times

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices. You perform a proof of concept (PoC) deployment of Microsoft Defender for Endpoint for 10 test devices. During the onboarding process, you configure Microsoft Defender for Endpoint-related data to be stored in the United States. You plan to onboard all the devices to Microsoft Defender for Endpoint. You need to store the Microsoft Defender for Endpoint data in Europe. What should you do first?

- A. Delete the workspace.
- B. Create a workspace.
- C. Onboard a new device.
- D. Offboard the test devices.

**Correct Answer: B***Community vote distribution*

D (88%) 13%

✉️  **Nilz76**  2 weeks ago

**Selected Answer: D**

D. Offboard the test devices

Offboarding the test devices as a first step, followed by setting up/creating a new workspace in Europe. If the data storage location is tied to the workspace and cannot be changed once set, then it would make sense to offboard the test devices from the current workspace before creating a new workspace in the data storage location of Europe.

upvoted 6 times

✉️  **sherifhamed**  2 weeks, 4 days ago

**Selected Answer: D**

The correct answer is D. Offboard the test devices.

To store the Microsoft Defender for Endpoint data in Europe, you need to offboard the test devices from the current workspace that is configured to store data in the United States. This is because the data storage location cannot be changed once it is configured during the onboarding process.

According to the Microsoft documentation

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/data-storage-privacy?view=o365-worldwide>

upvoted 3 times

✉️  **pantcm** 1 month, 2 weeks ago

D is the correct answer

upvoted 1 times

✉️  **gomezmax** 1 month, 4 weeks ago

(D) Offboard the test devices. from here to the Moon

upvoted 1 times

✉️  **Greatone1** 2 months ago

D is the correct answer from MS 101

upvoted 3 times

✉️  **Dtriminio** 2 months, 1 week ago

**Selected Answer: D**

i will go with D

upvoted 1 times

✉️  **alecrobertburns** 2 months, 1 week ago

**Selected Answer: D**

Answer is D

To onboard them all in Europe you first have to offboard the 10 that are onboarded in the US

upvoted 2 times

✉️  **alecrobertburns** 2 months, 1 week ago

Answer is D

To onboard them all in Europe you first have to offboard the 10 that are onboarded in the US

upvoted 1 times

 **nublit** 2 months, 1 week ago

**Selected Answer: D**

Answer is D: First Offboard the test devices, delete the workspace, create a workspace in Europe, onboard new devices. Reference:  
<https://www.examtopics.com/discussions/microsoft/view/68005-exam-ms-101-topic-2-question-29-discussion/>  
upvoted 2 times

 **osxzkwpfcfxobqjby** 2 months, 1 week ago

**Selected Answer: B**

Create a new workspace. After that you can connect existing and new clients to the new workspace.

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/faq-data-collection-agents#how-can-i-use-my-existing-log-analytics-workspace>  
upvoted 2 times

You have a Microsoft 365 E5 subscription that contains a user named User1.  
User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.  
You need to remove User1 from the Restricted entities list.  
What should you use?

- A. the Exchange admin center
- B. the Microsoft Purview compliance portal
- C. the Microsoft 365 admin center
- D. the Microsoft 365 Defender portal
- E. the Microsoft Entra admin center

**Correct Answer: D***Community vote distribution*

D (100%)

 **sherifhamed** 2 weeks, 6 days ago

**Selected Answer: D**

In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & collaboration > Review > Restricted entities  
upvoted 2 times

 **SandyBridge** 4 weeks, 1 day ago

**Selected Answer: D**

D is the correct answer.

"In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use <https://security.microsoft.com/restrictedentities>"

ref: <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam?view=o365-worldwide>  
upvoted 2 times

 **Ruhansen** 1 month ago

D is correct

upvoted 1 times

 **Dtriminio** 2 months, 1 week ago

**Selected Answer: D**

Remove a user from the Restricted entities page in the Microsoft 365 Defender portal

In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use <https://security.microsoft.com/restrictedentities>.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam?view=o365-worldwide>  
upvoted 4 times

 **RAG** 2 months, 1 week ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam?view=o365-worldwide>  
upvoted 3 times

Your company has a Microsoft 365 E5 subscription.

Users in the research department work with sensitive data.

You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents. Users in other departments must not be restricted.

What should you do?

- A. Create a data loss prevention (DLP) policy that has a Content is shared condition.
- B. Modify the safe links policy Global settings.
- C. Create a data loss prevention (DLP) policy that has a Content contains condition.
- D. Create a new safe links policy.

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **Nilz76** 2 weeks ago

**Selected Answer: D**

D. Create a new safe links policy.

With this action, you can create a Safe Links policy specifically targeting the users in the research department, ensuring that only they are restricted from accessing potentially unsafe websites through hyperlinks, while other departments remain unaffected.

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-links-policies?view=o365-worldwide>  
upvoted 1 times

 **Ruhansen** 1 month ago

D - and assigned to different groups  
upvoted 1 times

 **Greatone1** 2 months ago

D is the correct answer

<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-links-policies#policies-that-apply-to-specific-email-recipients>  
upvoted 2 times

**HOTSPOT -**

You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender for Endpoint administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Device group	Device name	User access
1	ATP1	Device1	Group1
Last	Ungrouped devices (default)	Device2	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

- | Statements   | Yes                   | No                    |
|--|-----------------------|-----------------------|
| User1 can run an antivirus scan on Device2.              | <input type="radio"/> | <input type="radio"/> |
| User2 can collect an investigation package from Device2. | <input type="radio"/> | <input type="radio"/> |
| User3 can isolate Device1.                               | <input type="radio"/> | <input type="radio"/> |

**Answer Area**

Statements	Yes	No
User1 can run an antivirus scan on Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can isolate Device1.	<input checked="" type="radio"/>	<input type="radio"/>

Correct Answer:

Nilz76 2 weeks ago

Here are my thoughts. No, No, Yes

Q: User 1 can run an antivirus scan on device 2.

A: No. User 1 belongs to Group 1 and has the permission to "View data, alerts investigations" under role 1. Running an antivirus scan would

typically require additional permissions which are not listed here for User 1.

Q: User 2 can collect an investigation package from device 2.

A: No. User 2 belongs to Group 2 and has the permission to "View data" under role 2. Collecting an investigation package would likely require additional permissions which are not listed for User 2.

Q: User 3 can isolate device 2.

A: Yes. User 3 belongs to Group 3 and has the role of Microsoft Defender for Endpoint Administrator which includes permissions to "View data, alerts investigations, active remediations, manage security settings." These permissions encompass the ability to take actions such as isolating a device.

upvoted 4 times

✉️  **mhmyz** 1 month, 2 weeks ago

No, No, No

Box3: User3 can Remediation Action but, Group3 do not assinged ATP1.

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/user-roles-windows-defender-advanced-threat-protection>

upvoted 2 times

✉️  **hogehogehoge** 1 month, 3 weeks ago

Box3: No?

Because Defferent Group In User and Device.

upvoted 1 times

✉️  **rinzler1** 1 month, 2 weeks ago

User3 is in default Admin group, has access to everything related to Endpoints

upvoted 5 times

✉️  **Greatone1** 1 month, 3 weeks ago

Answer is correct

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/user-roles-windows-defender-advanced-threat-protection>

upvoted 4 times

**HOTSPOT -**

You have a Microsoft 365 E5 tenant.

You need to ensure that administrators are notified when a user receives an email message that contains malware. The solution must use the principle of least privilege.

Which type of policy should you create, and which Microsoft Purview solutions role is required to create the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Policy type:

Role:

  
  
  
**Answer Area**

Policy type:

Correct Answer:

Role:

 **osxvkwpfcfxobqjby** Highly Voted 2 months, 1 week ago

- Alert
- Security administrator (principle of least privilege)

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide>  
upvoted 12 times

 **letters1234** Highly Voted 1 month, 3 weeks ago

Security Administrator or Global Administrator are required to setup the alert notifications. Least privilege means SA instead of GA.  
<https://learn.microsoft.com/en-us/microsoft-365/security/defender/configure-email-notifications?view=o365-worldwide#create-rules-for-alert-notifications>  
upvoted 9 times

 **sergioandreslq** Most Recent 4 days, 9 hours ago

In the Alert policies, you can create an alert with to send a notification when: "Detected Malware in an email message", you set up an alert and add as information the category for this alert which is "threat management"  
<https://security.microsoft.com/alertpoliciesv2>

My selection for the role will be "security administrator"  
upvoted 1 times

✉ **Paul\_white** 1 week, 5 days ago

CORRECT!!!

<https://www.examtopics.com/discussions/microsoft/view/110911-exam-ms-101-topic-2-question-139-discussion/>

upvoted 1 times

✉ **MarkusSan** 1 week, 1 day ago

not correct, by link provided ;)

upvoted 1 times

✉ **Nilz76** 2 weeks ago

Policy type: Threat  
Role: Security Administrator

Explanation:

You would want to create a Threat Policy to ensure that administrators are notified when a user receives an email message containing malware. Specifically, you might want to configure a Threat Policy within the Microsoft 365 Security & Compliance Center or Microsoft 365 Defender.

The Security Administrator role is suited for this task as it has the necessary permissions to manage security configurations across the tenant, adhering to the principle of least privilege. This role can create and manage threat policies to ensure that alerts are generated and sent to administrators when malware is detected in email messages.

upvoted 1 times

✉ **MondherBB** 3 weeks, 4 days ago

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide&toc=%2Fmicrosoft-365%2Fcompliance%2Ftoc.json&bc=%2Fmicrosoft-365%2Fbreadcrumb%2Ftoc.json>

Communication Compliance Administrators Administrators of communication compliance that can create/edit policies and define global settings.

upvoted 1 times

✉ **vercracked\_007** 1 month ago

Alert and Security Admin

Organisation Management is not a Purview role indeed.

upvoted 2 times

✉ **Casticod** 1 month, 3 weeks ago

I think security administrator.

Organization management, not Purview role, its a Exchange Role. In the question need a Pureview role

upvoted 1 times

✉ **gomezmax** 1 month, 3 weeks ago

Correct, Alert and Organization Management.

upvoted 2 times

✉ **Greatone1** 1 month, 4 weeks ago

Should be Alert and Security Administrator

upvoted 3 times

You have a Microsoft 365 E5 subscription.

You need to compare the current Safe Links configuration to the Microsoft recommended configurations.

What should you use?

- A. Microsoft Purview
- B. Azure AD Identity Protection
- C. Microsoft Secure Score
- D. the configuration analyzer

**Correct Answer: C**

*Community vote distribution*

D (100%)

 certma2023 Highly Voted 2 months ago

**Selected Answer: D**

It should be answer D.

The goal of the configuration analyzer is to compare Exchange Online Protection policies (aka Threat Policies) currently configured with MS recommendations.

There are two tabs named "Standard recommendations" & "Strict recommendations" that give the gap between current configuration & MS recommendations.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/configuration-analyzer-for-security-policies?view=o365-worldwide#use-the-configuration-analyzer-in-the-microsoft-365-defender-portal>

upvoted 9 times

 Nilz76 Most Recent 2 weeks ago

**Selected Answer: D**

D. the Configuration Analyzer (my guess)

The Configuration Analyzer can help compare your current configurations against Microsoft's recommended configurations to ensure you are following best practices for security and compliance.

Although the Microsoft Secure Score can provide insights into your security posture and recommendations for improvement, the Configuration Analyzer is more aligned with comparing specific configurations against recommended settings.

upvoted 1 times

 ae88d96 1 month, 2 weeks ago

**Selected Answer: D**

Correct answer is D.

In the public documentation it is mentioned what's covered within the Configuration Analyzer.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/configuration-analyzer-for-security-policies?view=o365-worldwide#use-the-configuration-analyzer-in-the-microsoft-365-defender-portal>

Microsoft Defender for Office 365 policies: Includes organizations with Microsoft 365 E5 or Defender for Office 365 add-on subscriptions:

Anti-phishing policies in Microsoft Defender for Office 365, which include:

The same spoof settings that are available in the EOP anti-phishing policies.

Impersonation settings

Advanced phishing thresholds

Safe Links policies.

Safe Attachments policies.

upvoted 2 times

 gomezmax 1 month, 2 weeks ago

It should be D

upvoted 1 times

 Greatone1 1 month, 3 weeks ago

**Selected Answer: D**

Correct answer is D

upvoted 1 times

 **Takanami** 1 month, 4 weeks ago

Configuration Analyzer is correct, direct link:

<https://security.microsoft.com/configurationAnalyzer>

upvoted 1 times

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.



You need to enable user access to the partner company's portal.

Which Microsoft Defender for Endpoint setting should you modify?

- A. Alert notifications
- B. Alert suppression
- C. Custom detections
- D. Advanced hunting
- E. Indicators

**Correct Answer: E**

*Community vote distribution*

E (100%)

 **letters1234** 1 month, 3 weeks ago

**Selected Answer: E**

Answer lines up with image as well, Defender SmartScreen.

"To block malicious IPs/URLs (as determined by Microsoft), Defender for Endpoint can use:

- Windows Defender SmartScreen for Microsoft browsers
  - Network Protection for non-Microsoft browsers, or calls made outside of a browser"
- <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-ip-domain?view=o365-worldwide#overview>

upvoted 1 times

 **Dtriminio** 2 months, 1 week ago

**Selected Answer: E**

By creating indicators for IPs and URLs or domains, you can now allow or block IPs, URLs, or domains based on your own threat intelligence.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-ip-domain?view=o365-worldwide>

upvoted 3 times

 **RAG** 2 months, 1 week ago

**Selected Answer: E**

Same question as listed on <https://www.examtopics.com/discussions/microsoft/view/48796-exam-ms-101-topic-2-question-32-discussion/>

upvoted 3 times

**HOTSPOT -**

You have a Microsoft 365 E3 subscription.

You plan to launch Attack simulation training for all users.

Which social engineering technique and training experience will be available? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Social engineering technique:

- Credential harvest
- Link to malware
- Malware attachment

Training experience:

- Identity Theft
- Mass Market Phishing
- Web Phishing

**Answer Area**

Social engineering technique:

- Credential harvest
- Link to malware
- Malware attachment

Correct Answer:

Training experience:

- Identity Theft
- Mass Market Phishing
- Web Phishing

  **imlearningstuffagain** 1 week ago

"Note Attack simulation training offers a subset of capabilities to E3 customers as a trial. The trial offering contains the ability to use a Credential Harvest payload and the ability to select 'ISA Phishing' or 'Mass Market Phishing' training experiences. No other capabilities are part of the E3 trial offering"

ref: <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide>  
upvoted 2 times

  **Nilz76** 2 weeks ago

Social Engineering Technique: Credential Harvest  
Training experience: Web phishing

Credential Harvest: This social engineering technique is commonly simulated to train users on recognizing attempts to steal their credentials through phishing.

Web Phishing: This is a common training experience where users are educated on how to identify and avoid phishing attempts that lead them to malicious websites.

It's been mentioned in a public preview announcement that Attack simulation training has been opened to all E3 customers. See link below:  
<https://techcommunity.microsoft.com/t5/security-compliance-and-identity/attack-simulation-training-public-preview-now-open-to-all-e3/ba-p/1873169>

Full access to Attack simulation training, where you can run realistic attack scenarios and manage social engineering risk through phishing simulations, typically requires Microsoft Defender for Office 365 Plan 2 or a Microsoft 365 E5 subscription

upvoted 2 times

✉️ **faeem** 3 weeks, 1 day ago

Only the following are available as per the E3: Attack simulation training offers a subset of capabilities to E3 customers as a trial. The trial offering contains the ability to use a Credential Harvest payload and the ability to select 'ISA Phishing' or 'Mass Market Phishing' training experiences. No other capabilities are part of the E3 trial offering. When you use an E5, then all is open.

upvoted 1 times

✉️ **letters1234** 1 month, 3 weeks ago

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide#what-do-you-need-to-know-before-you-begin>

upvoted 1 times

✉️ **osxzkwpfcfxobqjby** 2 months, 1 week ago

- All are available

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide#simulations>

- All are available

<https://security.microsoft.com/attacksimulator?viewid=trainingcampaign>

upvoted 1 times

✉️ **RAG** 2 months, 1 week ago

Attack simulation training offers a subset of capabilities to E3 customers as a trial. The trial offering contains the ability to use a Credential Harvest payload and the ability to select 'ISA Phishing' or 'Mass Market Phishing' training experiences. No other capabilities are part of the E3 trial offering.

upvoted 5 times

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You need to ensure that users are prevented from opening or downloading malicious files from Microsoft Teams, OneDrive, or SharePoint Online.

What should you do?

- A. Create a new Anti-malware policy.
- B. Configure the Safe Links global settings.
- C. Create a new Anti-phishing policy.
- D. Configure the Safe Attachments global settings.

**Correct Answer: D**

*Community vote distribution*

D (83%)      B (17%)

 **Nilz76** 2 weeks ago

**Selected Answer: D**

D. Configure the Safe Attachments global settings.

Microsoft Defender for Office 365 includes a feature known as Safe Attachments, which checks to see if email attachments or web downloads are malicious. When configured, Safe Attachments can scan and take action on potentially malicious files not only in email attachments but also in documents in SharePoint, OneDrive, and Microsoft Teams.

upvoted 1 times

 **andrewtb** 1 month, 2 weeks ago

**Selected Answer: D**

Safe Attachments: Step 1: Use the Microsoft 365 Defender portal to turn on Safe Attachments for SharePoint, OneDrive, and Microsoft Teams (<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-configure?view=o365-worldwide#step-1-use-the-microsoft-365-defender-portal-to-turn-on-safe-attachments-for-sharepoint-onedrive-and-microsoft-teams>)

upvoted 1 times

 **mhmaiz** 1 month, 2 weeks ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-about?view=o365-worldwide>  
upvoted 1 times

 **Greatone1** 2 months ago

**Selected Answer: D**

D is the correct answer  
upvoted 2 times

 **moshkoshbgosh** 2 months, 1 week ago

**Selected Answer: D**

Safe attachments supports Teams, SharePoint, OneDrive - <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-about> .

The following text is taken directly from Safe Attachments Global Settings in the Defender portal... "

Global settings

Use this page to protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Microsoft Teams.  
Protect files in SharePoint, OneDrive, and Microsoft Teams

If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, Safe Attachments will prevent users from opening and downloading the file. Learn more

Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams

upvoted 3 times

 **Dtriminio** 2 months, 1 week ago

**Selected Answer: B**

In organizations with Microsoft Defender for Office 365, Safe Links scanning protects your organization from malicious links, including QR codes, that are used in phishing and other attacks. Specifically, Safe Links provides URL scanning and rewriting of inbound email messages during mail flow, and time-of-click verification of URLs and links in email messages, Teams, and supported Office 365 apps.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-about?view=o365-worldwide>  
upvoted 1 times

 **alecrobertburns** 2 months, 1 week ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/step-by-step-guides/utilize-microsoft-defender-for-office-365-in-sharepoint-online?view=o365-worldwide#stop-infected-file-downloads-from-sharepoint-online>  
upvoted 1 times

 **RAG** 2 months, 1 week ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-configure?view=o365-worldwide>  
upvoted 1 times

 **osxzkwpfcfxobqjby** 2 months, 1 week ago

**Selected Answer: B**

Safe attachments is only for mail so the answer is B

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure?view=o365-worldwide>  
upvoted 1 times

**HOTSPOT -**

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Device group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped devices (default)	<i>Not applicable</i>

You onboard a computer named computer1 to Microsoft Defender for Endpoint as shown in the following exhibit.

Settings > Endpoints > computer1



# computer1

## Device summary

### Risk level ⓘ

None

### Device details

#### Domain

adatum.com

#### OS

Windows 10 64-bit

Version 21H2

Build 19044.2130

Use the drop-down menus to select the answer choice that completes each statement.

NOTE: Each correct selection is worth one point.

### Answer Area

Computer1 will be a member of [answer choice].

Group3 only  
Group4 only  
Group3 and Group4 only  
Ungrouped devices

If you add the tag demo to Computer1, the computer will be a member of [answer choice].

Group1 only  
Group1 and Group2 only  
Group1, Group2, Group3, and Group4  
Ungrouped devices

**Answer Area**

Computer1 will be a member of [answer choice].

If you add the tag demo to Computer1, the computer will be a member of [answer choice].

The first dropdown menu shows:  
Group3 only  
Group4 only  
Group3 and Group4 only (highlighted)  
Ungrouped devices

The second dropdown menu shows:  
Group1 only  
Group1 and Group2 only  
Group1, Group2, Group3, and Group4 (highlighted)  
Ungrouped devices

Correct Answer:  
If you add the tag demo to Computer1, the computer will be a member of [answer choice].

**Nalle** Highly Voted 2 months, 1 week ago

Group 3 only  
Group 1 only

"If a device is also matched to other groups, it's added only to the highest ranked device group"  
upvoted 21 times

**RVerzijl** Most Recent 4 weeks ago

Group 3 only  
Group 1 only  
upvoted 3 times

**RVerzijl** 4 weeks ago

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide>

A device group with a rank of 1 is the highest ranked group. When a device is matched to more than one group, it's added only to the highest ranked group.  
upvoted 1 times

**jt2214** 1 month, 2 weeks ago

I didn't read the ranking at first. So it makes more sense, now.  
upvoted 1 times

**Greatone1** 1 month, 4 weeks ago

Group 3 and Group 1  
<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide>  
upvoted 2 times

**Casticod** 2 months ago

Group 3 only  
Group 1 Only  
<https://www.examtopics.com/discussions/microsoft/view/48754-exam-ms-101-topic-2-question-15-discussion/>  
upvoted 3 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.

The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.

You need to identify the following information:

The number of email messages quarantined by zero-hour auto purge (ZAP)

The number of times users clicked a malicious link in an email message

Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

To identify the number of emails quarantined by ZAP:

- Mailflow status report
- Spoof detections
- Threat protection status
- URL threat protection

To identify the number of times users clicked a malicious link  
in an email:

- Mailflow status report
- Spoof detections
- Threat protection status
- URL threat protection

**Answer Area**

To identify the number of emails quarantined by ZAP:

To identify the number of times users clicked a malicious link  
in an email:

**Correct Answer:**

Reports > Mailflow status report

## Mailflow status report

Type Direction  Mailflow

Filters: Date (UTC): 8/23/2021-9/21/2021 Mail direction: Inbound +1 [X](#)

Select a node in the chart to show or hide more information.

Legend:

- Rule block
- Malware block
- Phishing block
- Spam block
- Impersonation block
- Detonation block
- ZAP removed
- Delivered

Show trends [Export](#) [Refresh](#)

Date (UTC)	Total email	Edge filtered	Rule messages	Anti-malware engine, Safe Attachme...	DMARC, impersonation, spoof, phish...	Detonation detection	Anti-spam filtered	ZAP removed	Messages where no threats ...
9/21/2021	263,004	0	22,755	4,338	26,877	12	187,458	5	22,159
9/20/2021	1,007,087	0	69,528	20,599	117,619	60	733,155	41	66,085

**Greatone1** 1 month, 4 weeks ago

Mailflow Status Report

2) URL Protection

upvoted 4 times

✉ **osxvkwpfcfxobqjby** 2 months, 1 week ago

- Mailflow & URL

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide#how-to-see-if-zap-moved-your-message>

upvoted 4 times

Question #26

Topic 1

You have a Microsoft 365 tenant.

You plan to manage incidents in the tenant by using the Microsoft 365 Defender.

Which Microsoft service source will appear on the Incidents page of the Microsoft 365 Defender portal?

- A. Microsoft Sentinel
- B. Microsoft Defender for Cloud
- C. Azure Arc
- D. Microsoft Defender for Identity

**Correct Answer: D**

*Community vote distribution*

D (100%)

✉ **GenPatton** 3 weeks, 3 days ago

**Selected Answer: D**

Microsoft Sentinel is a SIEM system and will not forward alerts to M365 Defender. Events will rather be forwarded from M365 Defender TO Sentinel. Azure ARC and Defender for Cloud (not Defender for Cloud Apps) will send their alerts to Sentinel. That leaves MS Defender for Identity and that will indeed send alerts to M365 Defender interface.

upvoted 4 times

✉ **Shloeb** 3 weeks, 3 days ago

What kind of questions are these? How does this help in getting certified? Microsoft has lost their mind

upvoted 2 times

✉ **gomezmax** 1 month ago

C. Azure Arc

Right Answer

upvoted 1 times

✉ **Casticod** 1 month, 1 week ago

Real Question in exam

upvoted 2 times

✉ **cb0900** 1 month, 3 weeks ago

You can filter the alerts based on the Service Sources:

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue?view=o365-worldwide#service-sources>

upvoted 2 times

✉ **Greatone1** 1 month, 4 weeks ago

**Selected Answer: D**

D is correct

<https://www.examtopics.com/discussions/microsoft/view/56970-exam-ms-101-topic-2-question-70-discussion/>

upvoted 2 times

Your network contains an on-premises Active Directory domain named contoso.local. The domain contains five domain controllers.

Your company purchases Microsoft 365 and creates an Azure AD tenant named contoso.onmicrosoft.com.

You plan to install Azure AD Connect on a member server and implement pass-through authentication.

You need to prepare the environment for the planned implementation of pass-through authentication.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From a domain controller, install an Authentication Agent.
- B. From the Microsoft Entra admin center, configure an authentication method.
- C. From Active Directory Domains and Trusts, add a UPN suffix.
- D. Modify the email address attribute for each user account.
- E. From the Microsoft Entra admin center, add a custom domain name.
- F. Modify the User logon name for each user account.

**Correct Answer: ABE**

*Community vote distribution*

CEF (100%)

✉  **certma2023**  2 months ago

**Selected Answer: CEF**

I Agree. As the local ADDS name is "contoso.local", we need to make some few steps/prerequisites before being able to set up account synchronization:

- > Add a custom domain name on the Azure AD / MS Entra portal (ex. contoso.com)
- > Add a local UPN suffix at the ADDS Forest level (contoso.com)
- > Modify all user account UPN from username@contoso.local to username@contoso.com

Then comes the Azure AD Connect deployment & the PTA configuration.

upvoted 9 times

✉  **Milad666**  3 weeks ago

hey guys this is just annoying, so many questions the community and the answer from Examtopic differ, I agree for CEF but where did Examtopic make this answer ? and im fully from my Answer Suspecious...

upvoted 1 times

✉  **ggdevices** 4 weeks, 1 day ago

Looking at the article with the prerequisites the answer seems to be correct: <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-quick-start>

upvoted 1 times

✉  **Casticod** 1 month, 1 week ago

Real Question in exam

upvoted 3 times

✉  **mccheesey** 1 month, 3 weeks ago

CEF would be the logical answer in my mind... But in a roundabout way, I can see the justification behind ABE...

If they're just planning to not modify the UPNs at all from that .onmicrosoft.com domain, it makes sense to install the agent, enable an authentication method, and just modify the email address field without worrying about not having an actual domain attached to their UPNs. But of course, real world application vs. test questions are always different I suppose. :)

upvoted 1 times

✉  **amurp35** 1 month ago

You enable PTA when configuring AD Connect. In order to configure ADConnect, you must have the UPNs matching the domain in AzureAD.

upvoted 1 times

✉  **Casticod** 2 months ago

**Selected Answer: CEF**

CDF I don't Dude

upvoted 1 times

✉  **Casticod** 2 months ago

CEF, sorry

upvoted 1 times

 **osxvkwpfcfxobqby** 2 months, 1 week ago

**Selected Answer: CEF**

A. is required for HA, use it in real world, but it is not been asked for in this question.

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-quick-start>

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide#what-if-i-only-have-a-local-on-premises-domain>

upvoted 2 times

**HOTSPOT -**

You have a new Microsoft 365 E5 tenant.

Enable Security defaults is set to Yes.

A user signs in to the tenant for the first time.

Which multi-factor authentication (MFA) method can the user use, and how many days does the user have to register for MFA? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

MFA method:

- Call to phone
- Email message
- Security questions
- Text message to phone
- Notification to Microsoft Authenticator app

Number of days:

7
14
30
60

**Answer Area**

**Correct Answer:**

MFA method:

- Call to phone
- Email message
- Security questions
- Text message to phone
- Notification to Microsoft Authenticator app**

Number of days:

7
<b>14</b>
30
60

 **osxzkwpfcfxobqjby** Highly Voted  2 months, 1 week ago

- Notification to Microsoft Authenticator app
- 14 days

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/security-defaults#authentication-methods>  
upvoted 5 times

 **sherifhamed** Most Recent  2 weeks, 6 days ago

Correct.

the user can use the following multi-factor authentication (MFA) methods when signing in to the tenant for the first time:

- Microsoft Authenticator app
- SMS
- Voice call

The user has 14 days to register for MFA after the first sign-in  
upvoted 2 times

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Configuration
Group1	Global security group
User1	Enabled user account
User2	Disabled user account

You configure Azure AD Connect to sync contoso.com to Azure AD.

Which objects will sync to Azure AD?

- A. Group1 only
- B. User1 and User2 only
- C. Group1 and User1 only
- D. Group1, User1, and User2

**Correct Answer: D**

*Community vote distribution*

D (65%)      C (18%)      B (18%)

✉️  **Haso**  2 months ago

**Selected Answer: D**

It is D. Global security groups from your on-premises AD are synchronized to Azure AD, and they retain their membership and other attributes during the synchronization process. This means that if you have global security groups defined in your on-premises AD and these groups contain users or other groups, the membership information will be replicated to Azure AD.

Disabled user accounts are also synchronized: <https://learn.microsoft.com/en-us/answers/questions/233667/will-azure-ad-connect-sync-disabled-user-accounts>  
upvoted 9 times

✉️  **Ruhansen**  1 month ago

As stated here: <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user-and-contacts#disabled-accounts>

The answer is D

upvoted 1 times

✉️  **Casticod** 1 month, 1 week ago

Real Question in exam

upvoted 2 times

✉️  **Tisi** 1 month, 1 week ago

Azure AD Connect will sync both user accounts and security groups. However, by default, it does not sync disabled user accounts.

upvoted 1 times

✉️  **gomezmax** 1 month, 3 weeks ago

C. Group1 and User1 only User 2 is a disabled account

upvoted 1 times

✉️  **Mr4D97** 2 months ago

**Selected Answer: D**

Builtin security groups are listed here (<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#default-active-directory-security-groups>) and Global security group is not part of that list therefore it will be synchronised.

ANSWER IS D

upvoted 2 times

✉️  **Casticod** 2 months ago

**Selected Answer: B**

In this conversation not much is clarified, for me the answer is B

<https://www.examtopics.com/discussions/microsoft/view/48837-exam-ms-100-topic-3-question-77-discussion/>

upvoted 1 times

✉️  **moshkoshbgosh** 2 months, 1 week ago

**Selected Answer: B**

From <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user-and-contacts>

Azure AD Connect excludes built-in security groups from directory synchronization.

Disabled accounts are synchronized as well to Azure AD

upvoted 2 times

✉️  **moshkoshbgosh** 2 months ago

I'm starting to think this might be D... it's not specifically saying the global security group is a default global security group. Thoughts?

upvoted 3 times

✉️  **certma2023** 2 months ago

You're right. Group1 is definitively a custom group not a built in security group like "domain admins" or "enterprise admins". Therefore it should synchronize to Azure AD without any issue.

upvoted 2 times

✉️  **Mr4D97** 2 months ago

Yup, you're right. Built-in security groups are listed here (<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#default-active-directory-security-groups>) and Global security group is not part of that list therefore it will be synchronised.

ANSWER IS D

upvoted 1 times

✉️  **mrac** 2 months, 1 week ago

**Selected Answer: C**

C. Group1 and User1 only

Here's why:

Group1 is a global security group. By default, Azure AD Connect synchronizes security groups to Azure AD.

User1 is an enabled user. Enabled user accounts are synchronized to Azure AD by default.

User2 is a disabled user, and by default, disabled user accounts are not synchronized to Azure AD.

So, only Group1 and User1 will sync to Azure AD in this scenario.

upvoted 3 times

✉️  **certma2023** 2 months ago

nope, It's answer D. By default disabled users are synced to Azure AD. If you want to change that, you need to implement a custom inbound synchronization rule.

"Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms."

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user-and-contacts#disabled-accounts>

upvoted 2 times

You have a Microsoft 365 E5 subscription.

You need to create Conditional Access policies to meet the following requirements:

All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.

Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.

All users must be blocked from signing in from outside the United States and Canada.

Only users in the R&D department must be blocked from signing in from both Android and iOS devices.

Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.

What is the minimum number of Conditional Access policies you should create?

- A. 3
- B. 4
- C. 5
- D. 6
- E. 7
- F. 8

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **certma2023** Highly Voted 2 months ago

**Selected Answer: B**

I would go for B answer.

4 rules configured like that :

- > One rule that target all users & all location except a custom trusted location (Public IP Ranges of the company). This rule grant access with MFA + Compliant device.
- > One rule that target all users & all location except US & Canada. This rule block access.
- > One rule that target R&D Users only & Android+IOS Devices. This rule block access.
- > One rule that target all users except Finance users. The rule target only App1. This rule block access.

For me, it should meet the goals.

upvoted 6 times

 **Master\_Tx** Most Recent 1 month, 2 weeks ago

I personally dont recommend creating policies that combine functions unless there is a specific need, so I chose C. However B is what the question is asking for, as a MINIMUM.

upvoted 1 times

 **nsotis28** 1 month, 3 weeks ago

answer is correct

B

upvoted 1 times

**HOTSPOT -**

Your network contains an on-premises Active Directory domain.

You have a Microsoft 365 E5 subscription.

You plan to implement directory synchronization.

You need to identify potential synchronization issues for the domain. The solution must use the principle of least privilege.

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area****Tool:**

- AccessChk
- Azure AD Connect
- Active Directory Explorer
- IdFix**

**Required group membership:**

- Domain Admins
- Domain Users
- Server Operators
- Enterprise Admins**

**Answer Area****Tool:**

- AccessChk
- Azure AD Connect
- Active Directory Explorer
- IdFix**

**Required group membership:**

- Domain Admins
- Domain Users
- Server Operators
- Enterprise Admins**

**Correct Answer:**

 **osxvkwpfcfxobqjby**  2 months, 1 week ago

IdFix & Domain Users

You only need to identify problems, so no rights needed to fix them.

<https://microsoft.github.io/idfix/Step%201%20-%20Review%20the%20prerequisites/#permissions>  
upvoted 14 times

 **vercracked\_007**  1 month, 1 week ago

This must be domain admin and IDFix. A account needs read and write permissions to the domain.  
upvoted 3 times

 **rfree** 1 month, 2 weeks ago

Thinking IdFix and GAdministrator  
<https://lazyadmin.nl/it/idfix/>  
But to use the tool your will need of course to have read and write access to the Active Directory  
upvoted 1 times

 **Casticod** 2 months ago

IdFix

Domain Users

The application runs in the context of the authenticated user, which means that it will query the authenticated forest and must have rights to read the directory.

upvoted 4 times

**HOTSPOT -**

You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1	Enforced

Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs.

The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Location1	131.107.20.0/24	Yes
Location2	131.107.50.0/24	Yes

You create a conditional access policy that has the following configurations:

Users or workload identities assignments: All users

Cloud apps or actions assignment: App1

Conditions: Include all trusted locations

Grant access: Require multi-factor authentication

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
When User1 connects to App1 from a device that has an IP address of 131.107.50.10, User1 must use MFA.	<input type="radio"/>	<input type="radio"/>
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	<input type="radio"/>	<input type="radio"/>
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.	<input type="radio"/>	<input checked="" type="radio"/>

**Answer Area**

Correct Answer:

Statements	Yes	No
When User1 connects to App1 from a device that has an IP address of 131.107.50.10, User1 must use MFA.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Haso** 2 months ago

Y: User is in trusted location from CA policy  
Y: User is in trusted location from CA policy

N: Trusted IPs in the MFA settings contains a list of IPs that MFA can be skipped from.  
<https://c7solutions.com/2022/07/what-is-multifactor-authentication-trusted-ips>

upvoted 11 times

**osxvkwpfcfxobqjby** 2 months, 1 week ago

Y: User is in trusted location from CA policy  
Y: User is in trusted location from CA policy  
Y: User is in trusted location set by MFA config

MFA per user setting is an old (but still existing) one.  
AAD > All Users > Per-User MFA icon > Gray Service setting tab

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates#view-the-status-for-a-user>  
upvoted 3 times

✉️  **sergioandreslq** 3 days, 10 hours ago

Y: User is in trusted location from CA policy  
Y: User is in trusted location from CA policy  
Y: User is in trusted location set by per-user MFA config MFA is an old (but still existing) one.  
I tested this scenario, I put my up address as trusted IP in Per-user MFA and request MFA in Conditional access policy, after testing I am getting the request for the MFA, meaning that the bypass in per-user MFA is not being applied.  
upvoted 2 times

✉️  **certma2023** 2 months ago

No it should be YYN.

The trusted IPs configured inside the legacy per-user MFA settings are IPs where MFA is bypassed. Therefore if the user connect from the "Trusted IPs" IP range he won't be prompt for MFA.

upvoted 5 times

Question #33

Topic 1

You have a Microsoft 365 subscription.

You register two applications named App1 and App2 to Azure AD.

You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?

- A. From the Microsoft Entra admin center, create a conditional access policy.
- B. From the Microsoft 365 admin center, configure the Modern authentication settings.
- C. From the Enterprise applications blade of the Microsoft Entra admin center, configure the Users settings.
- D. From Multi-Factor Authentication, configure the service settings.

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉️  **sherifhamed** 2 weeks, 5 days ago

**Selected Answer: A**

The correct answer is A. From the Microsoft Entra admin center, create a conditional access policy.

A conditional access policy is a way to enable and enforce MFA for specific applications or users in Microsoft Entra.

upvoted 2 times

✉️  **GLL** 1 month, 3 weeks ago

**Selected Answer: A**

Conditional Access is found in the Microsoft Entra admin center under Protection > Conditional Access.

upvoted 1 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription.

You need to implement identity protection. The solution must meet the following requirements:

Identify when a user's credentials are compromised and shared on the dark web.

Provide users that have compromised credentials with the ability to self-remediate.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

To identify when users have compromised credentials, configure:

- A registration policy
- A sign-in risk policy
- A user risk policy**
- A multifactor authentication registration policy

To enable self-remediation, select:

- Generate a temporary password
- Require multi-factor authentication
- Require password change**

**Answer Area**

To identify when users have compromised credentials, configure:

- A registration policy
- A sign-in risk policy
- A user risk policy**
- A multifactor authentication registration policy

**Correct Answer:**

To enable self-remediation, select:

- Generate a temporary password
- Require multi-factor authentication**
- Require password change**

 **RAG** 2 months, 1 week ago

Looks correct - <https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa>

upvoted 4 times

 **certma2023** 2 months ago

The second one is obviously correct. Require password change is the MS recommendation for a compromised account (user with a high risk or high sign-in risk).

For the first one the question is unclear. To identify a user with compromised credentials we would go to the "Risky Users" blade. But if the question is about configuring a rule that apply an action on account with credentials shared on the dark Web (or the regular Web like GitHub repos), we would create either a conditional access policy (new way with only an Azure AD P1 license) or either a risk user policy inside the Azure AD Identity Protection blade (legacy way that require an Azure AD P2 license).

Therefore the second one should be correct too, assuming that the question about configuring a rule that apply a specific action to compromised account (MS also say "leaked credentials" is some documentations).

upvoted 2 times

 **amurp35** 1 month ago

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk-user?source=recommendations>

"admins with P2 can create CA policies incorporating Identity Protection risk policies"

also references p2 required to utilize user risk in CA policies:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa>

upvoted 1 times

 **Nandokun01** 1 month, 3 weeks ago

Correct (as expected :) ) but since I dont see the CA policy option as an answer they must be looking for the old risk policy option to set these up. I didnt realize the P1 vs P2 difference until you mentioned it so thanks!

upvoted 1 times

**HOTSPOT -**

Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription.

The domain contains the users shown in the following table.

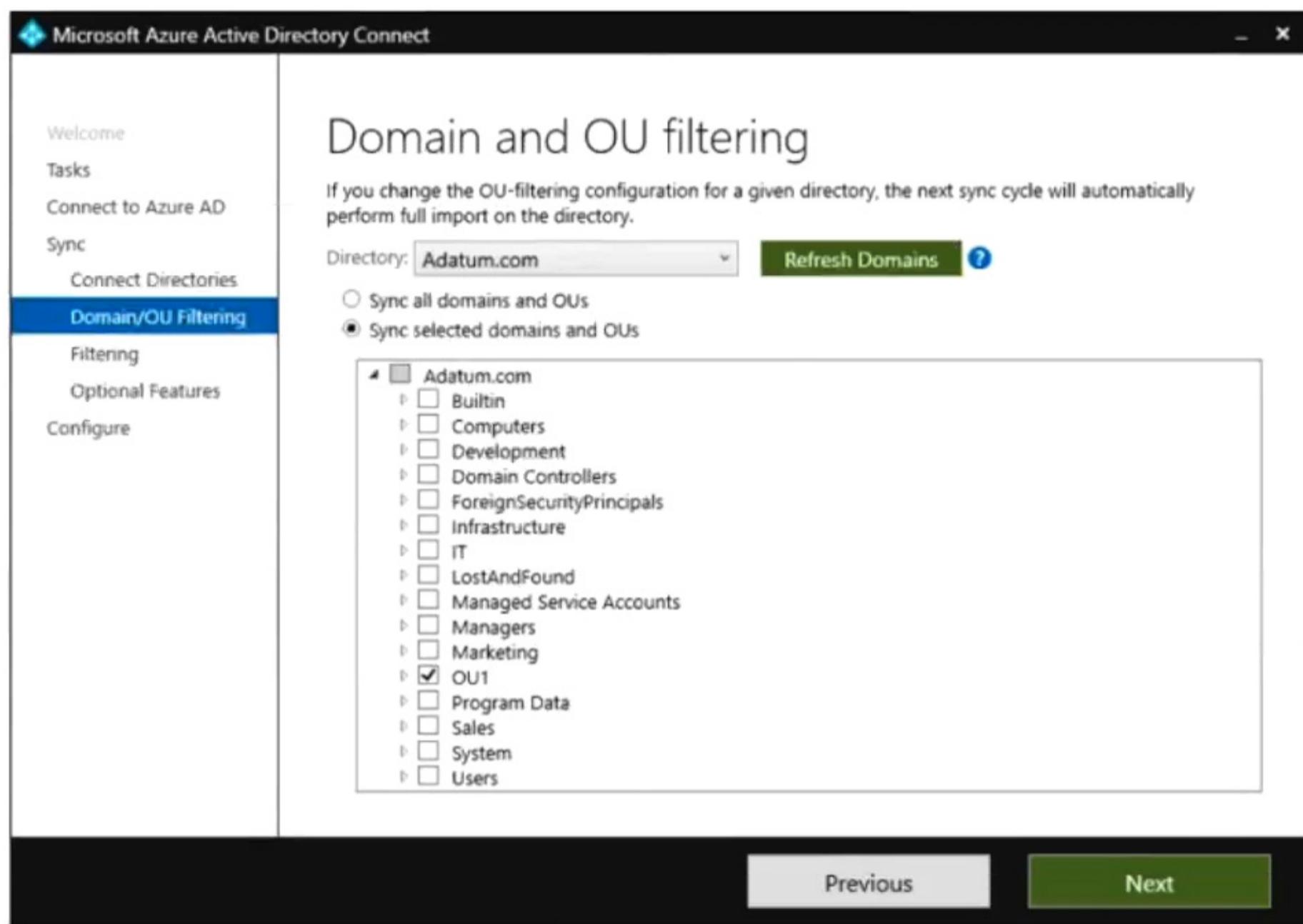
Name	Member of	In organizational unit (OU)
User1	Group1	OU1
User2	Group2	OU1

The domain contains the groups shown in the following table.

Name	Member of	In OU
Group1	None	Sales
Group2	Group1	OU1

You are deploying Azure AD Connect.

You configure Domain and OU filtering as shown in the following exhibit.



You configure Filter users and devices as shown in the following exhibit.

Microsoft Azure Active Directory Connect

Welcome  
Tasks  
Connect to Azure AD  
Sync  
Connect Directories  
Domain/OU Filtering  
**Filtering**  
Optional Features  
Configure

## Filter users and devices

For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.

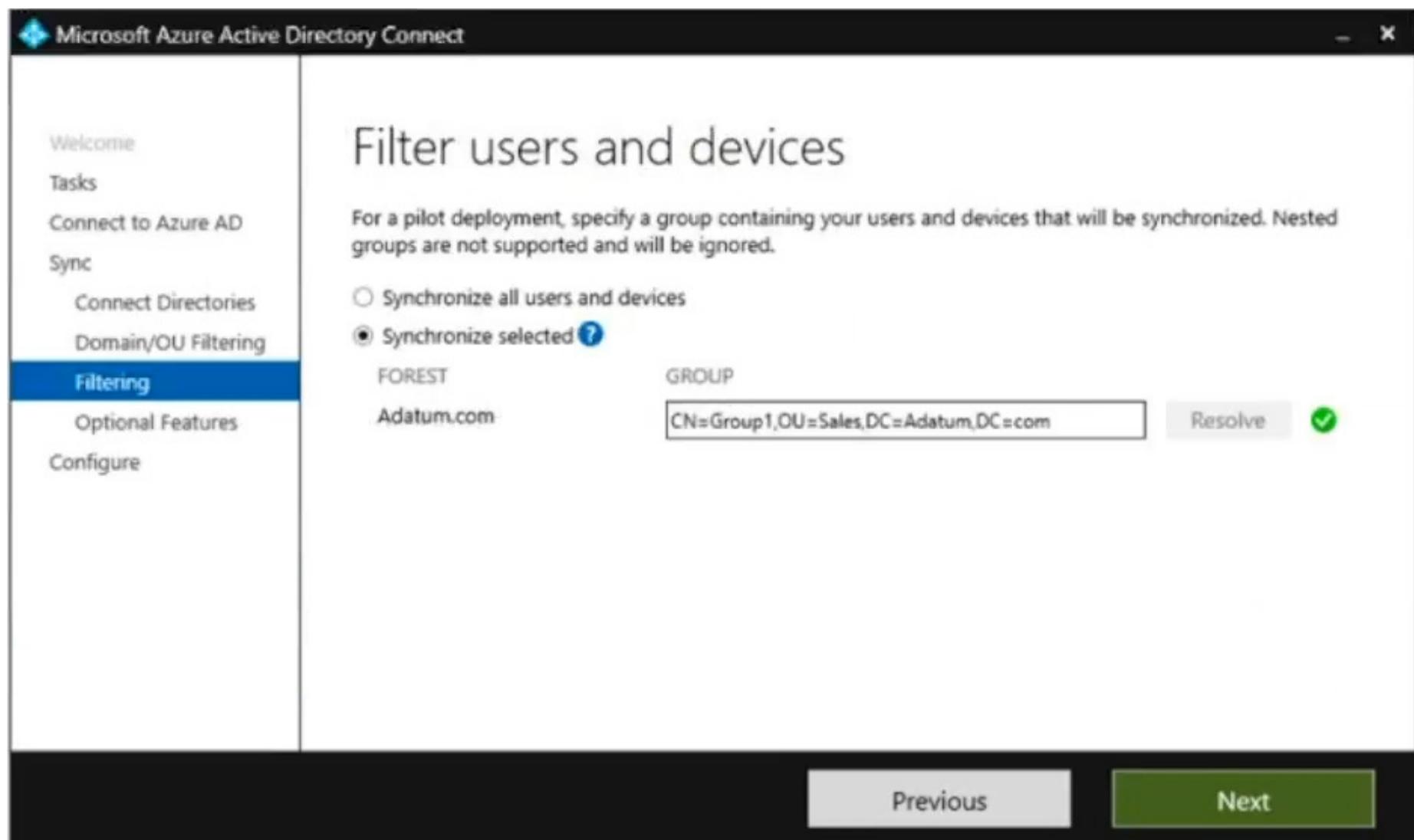
Synchronize all users and devices  
 Synchronize selected [?](#)

FOREST  
Adatum.com

GROUP  
CN=Group1,OU=Sales,DC=Adatum,DC=com

Resolve

Previous Next



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

### Answer Area

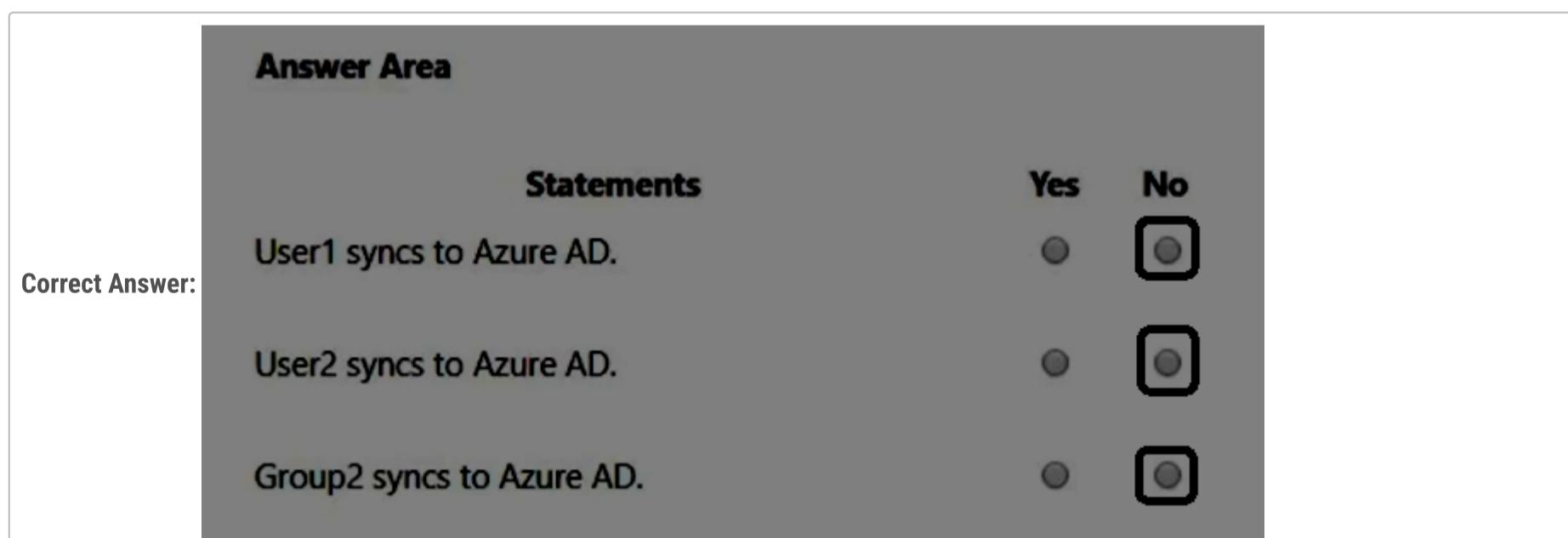
Statements	Yes	No
User1 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>
User2 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>
Group2 syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>

**Answer Area**

**Statements**

**Correct Answer:**

Statements	Yes	No
User1 syncs to Azure AD.	<input type="radio"/>	<input checked="" type="checkbox"/>
User2 syncs to Azure AD.	<input type="radio"/>	<input checked="" type="checkbox"/>
Group2 syncs to Azure AD.	<input type="radio"/>	<input checked="" type="checkbox"/>



**Casticod** Highly Voted 2 months ago

It should be No, No, No since group is Sales OU which does not synchronize

When using OU-based filtering in conjunction with group-based filtering, the OU(s) where the group and its members are located must be included. (<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#group-based-filtering>)  
<https://www.examtopics.com/discussions/microsoft/view/82530-exam-ms-100-topic-3-question-89-discussion/>

upvoted 13 times

**mhmyz** Highly Voted 1 month, 1 week ago

N,N,N

Group1 is not in OU1.So any groups and users does not sync.

Group-based filtering

When using OU-based filtering in conjunction with group-based filtering, the OU(s) where the group and its members are located must be included.

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-sync-configure-filtering>

upvoted 5 times

✉️ **MondherBB** Most Recent 3 weeks, 2 days ago

I think the answer should be

User1 Yes - The user is in OU1 and in Group1 (reply to both conditions)

User2 No – the syn service will check in sales OU

Group 2 No – Nested group

upvoted 1 times

✉️ **vercracked\_007** 1 month ago

YNY

It doesn't matter Group1 is in the Sales OU. It's just used for the filter.

OU1 syncs

Based on filter User 1 will sync

User2 to will Not sync

Group 2 wil be synced because its a group in OU1 and nog a user or device. So filter does not affect the group.

upvoted 5 times

✉️ **EEMS700** 3 weeks, 6 days ago

YNY is correct.

Only users, devices and groups in OU1 will sync, based on the filter (groupmembership) of group1

This was my fault in the past.

the membership of a group who is a member of a filtergrup has no affect to the members inside the group.

all devices, groups and users must be a member of the filtergroup itself.

user1 is in ou1 and member of group1 -> sync

user2 is in ou1 but no member of group1 -> no sync

group1 is in sales and no member of group1 -> no sync

group2 is in ou1 and member of group1 -> sync

upvoted 2 times

✉️ **letters1234** 1 month, 2 weeks ago

User 1 is member of Group 1 and in OU1, user/device filter applies for the user so allows sync

User 2 is member of group 2 and in OU1, user/device filter doesnt inlcude user so doesnt sync

Group 2 is in OU1, meaning it will sync, filter is for devices/users not groups.

Y,N,Y

The nesting comment is saying for the targeted group, if there are members of the group that are security groups, they will be ignored. The filter is for Users/Devices.

upvoted 1 times

✉️ **Nandokun01** 1 month, 3 weeks ago

OU filters define the connector scope and are an include/exclude conditional statement. Group-based filtering is an object-level condition which evaluates during each connector's sync cycle. If the OU is not in scope the object will never import via its connector so it will not be evaluated during the sync cycles. Casticod is correct

upvoted 2 times

✉️ **Greatone1** 1 month, 4 weeks ago

No sure answer from previous exam question

<https://www.examtopics.com/discussions/microsoft/view/82530-exam-ms-100-topic-3-question-89-discussion/>

upvoted 1 times

✉️ **Venusaur** 2 months ago

Filtering already show that OU=SALES will be synced only.

so all answers NO

upvoted 4 times

✉️ **Mr4D97** 2 months ago

User 1 =Y

User 2 = N (Part of nested group 2 which is not in filter)

Group 2 = N (nested group not included)

upvoted 4 times

✉️ **osxzkwpfcfxobqjby** 2 months, 1 week ago

User1: OU1+Group1 = Y

User2: Group2 not in filter = N

Group2: nested groups are not supported but group1 is in OU1 = Y

upvoted 3 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) method registered
User1	Group1	Microsoft Authenticator app (push notification)
User2	Group2	Microsoft Authenticator app (push notification)
User3	Group1	None

You configure the Microsoft Authenticator authentication method policy to enable passwordless authentication as shown in the following exhibit.

The screenshot shows the 'Enable and Target' section of a policy configuration. The 'Enable' toggle is turned on. Under 'Target', the 'Select groups' option is selected, and 'Group1' is listed. In the 'Authentication mode' dropdown, 'Any' is chosen.

Both User1 and User2 report that they are NOT prompted for passwordless sign-in in the Microsoft Authenticator app.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 will be prompted for passwordless authentication once User1 sets up phone sign-in in the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>
User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>
User3 can use passwordless authentication without further action.	<input type="radio"/>	<input type="radio"/>

**Correct Answer:**

Answer Area	
Statements	
User1 will be prompted for passwordless authentication once User1 sets up phone sign-in in the Microsoft Authenticator app.	<input checked="" type="radio"/> Yes <input type="radio"/> No
User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.	<input type="radio"/> Yes <input checked="" type="radio"/> No
User3 can use passwordless authentication without further action.	<input type="radio"/> Yes <input checked="" type="radio"/> No

**gomezmax** 1 month, 3 weeks ago

Yes Correct YNN

upvoted 1 times

**certma2023** 2 months ago

Answer is correct. YNN.

User1 need to enable the phone sign-in option inside the Microsoft Authenticator app on his/her phone to be able to use passwordless (<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-phone#enable-phone-sign-in>)

User2 is registered for MFA with the Authenticator App but is not targeted by the passwordless configuration (as he/she is not member of group1).

User3 has not registered yet for MFA.

upvoted 3 times

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview policies to meet the following requirements:

Identify documents that are stored in Microsoft Teams and SharePoint that contain Personally Identifiable Information (PII).

Report on shared documents that contain PII.

What should you create?

- A. a data loss prevention (DLP) policy
- B. a retention policy
- C. an alert policy
- D. a Microsoft Defender for Cloud Apps policy

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **cb0900** 2 days, 19 hours ago

**Selected Answer: A**

Also in ms-101 Qs:

<https://www.examtopics.com/discussions/microsoft/view/65993-exam-ms-101-topic-2-question-78-discussion/>  
upvoted 1 times

 **KT\_Paradise75** 1 month, 1 week ago

The only answer here is A

upvoted 3 times

You have a Microsoft 365 E5 subscription that contains the resources shown in the following table.

Name	Type
Group1	Microsoft 365 group
Group2	Distribution group
Site1	Microsoft SharePoint site

You create a sensitivity label named Label1.

To which resource can you apply Label1?

- A. Group1 only
- B. Group2 only
- C. Site1 only
- D. Group1 and Group2 only
- E. Group1, Group2, and Site1

**Correct Answer: E**

*Community vote distribution*

E (100%)

 **Martham** 6 days, 19 hours ago

Given Answer is correct

upvoted 1 times

 **Dtriminio** 2 months, 1 week ago

**Selected Answer: E**

<https://learn.microsoft.com/en-us/purview/sensitivity-labels-teams-groups-sites>

upvoted 3 times

 **RAG** 2 months, 1 week ago

**Selected Answer: E**

This is the correct see <https://learn.microsoft.com/en-gb/purview/sensitivity-labels>

upvoted 4 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription.

You need to meet the following requirements:

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.

Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

**Correct Answer:**

The image shows the same list of Microsoft Purview compliance solutions as the previous screenshot, but with a different visual state. The 'Information protection' option is highlighted with a thick black border around its entire row, indicating it is the selected answer. The other options remain unselected.

 **AMDF**  1 month, 2 weeks ago

Correct:

<https://www.examtopics.com/discussions/microsoft/view/94672-exam-ms-101-topic-3-question-153-discussion/>

upvoted 5 times

 **Dtriminio**  2 months, 1 week ago

Enable co-authoring for files with sensitivity labels

1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect. Then select Turn on co-authoring for files with sensitivity labels, and Apply

upvoted 3 times

You have a Microsoft 365 E5 subscription.

You plan to create a data loss prevention (DLP) policy that will be applied to all available locations.

Which conditions can you use in the DLP rules of the policy?

- A. sensitive info types
- B. content search queries
- C. keywords
- D. sensitivity labels

**Correct Answer: C**

*Community vote distribution*

A (80%)      D (20%)

✉️  **sherifhamed** 2 weeks, 5 days ago

**Selected Answer: A**

The correct answer is A. sensitive info types.

Sensitive info types are predefined patterns that can help you identify and protect sensitive data, such as credit card numbers, social security numbers, bank account numbers, and so on<sup>1</sup>. You can use sensitive info types as conditions in your DLP rules to detect and protect data that matches these patterns. For example, you can create a DLP rule that blocks the external sharing of documents that contain credit card numbers<sup>2</sup>.

B, C, and D are incorrect because they are not valid conditions for DLP rules in Office

upvoted 2 times

✉️  **sergioandreslq** 3 days, 9 hours ago

I tested with the creation of DLP for all locations, only Sensitive Info Types was available for all the workloads.

Correct answer is A

upvoted 1 times

✉️  **AMDF** 1 month, 1 week ago

**Selected Answer: A**

Vote for A

upvoted 1 times

✉️  **SheryID** 1 month, 2 weeks ago

**Selected Answer: A**

Tested in Lab Environment, in create a new DLP policy, where locations are set to all, under customize advanced DLP rules > create rule > conditions > add a condition > content contains > add > then only option is "sensitive info types"

upvoted 3 times

✉️  **gomezmax** 1 month, 3 weeks ago

Should be A

upvoted 1 times

✉️  **Greatone1** 1 month, 4 weeks ago

**Selected Answer: A**

A should be the correct answer

<https://www.examtopics.com/discussions/microsoft/view/94556-exam-ms-101-topic-3-question-154-discussion/>

upvoted 1 times

✉️  **moshkoshbgosh** 2 months, 1 week ago

**Selected Answer: A**

Sorry mods - can you delete the previous response I posted, the answer should be A, not D.

The reason I'm suggesting A is that this needs to apply to all locations, but sensitivity labels can't be applied to Teams Chat and Channel Messages. I know this is being fussy about the wording, but it would be a way to reduce the choice to one valid option. <https://learn.microsoft.com/en-us/purview/dlp-policy-reference#location-support-for-how-content-can-be-defined>

upvoted 3 times

✉️  **certma2023** 2 months ago

I would go for answer A too. When you select all locations inside the policy configuration (Exchange, Sharepoint, OneDrive, MS Defender for Cloud, Endpoint...), the only options you have on the custom rule is "sensitive info types".

upvoted 1 times

 **moshkoshbgosh** 2 months, 1 week ago

**Selected Answer: D**

The reason I'm suggesting D is that this needs to apply to all locations, but sensitivity labels can't be applied to Teams Chat and Channel Messages. I know this is being fussy about the wording, but it would be a way to reduce the choice to one valid option. <https://learn.microsoft.com/en-us/purview/dlp-policy-reference#location-support-for-how-content-can-be-defined>

upvoted 1 times

 **moshkoshbgosh** 2 months, 1 week ago

please delete, it should have said A as per the link.

upvoted 1 times

 **Dtriminio** 2 months, 1 week ago

**Selected Answer: D**

A+D are correct

upvoted 2 times

 **osxzvkwpfcfxobqjby** 2 months, 1 week ago

**Selected Answer: A**

Cannot select right answers: A+D

<https://learn.microsoft.com/en-us/purview/dlp-policy-reference#content-contains>

upvoted 2 times

You have a Microsoft 365 E5 tenant.

Users store data in the following locations:

Microsoft Teams -

Microsoft OneDrive -

Microsoft Exchange Online -

Microsoft SharePoint -

You need to retain Microsoft 365 data for two years.

What is the minimum number of retention policies that you should create?

- A. 1
- B. 2
- C. 3
- D. 4

**Correct Answer: C**

*Community vote distribution*

C (65%)      B (35%)

✉  **moshkoshbgosh** Highly Voted 2 months, 1 week ago

**Selected Answer: C**

There's a trap with this one, you need two policies for Teams

1. Teams channel/chats
2. Teams private channel messages
3. OneDrive, SharePoint, Exchange

upvoted 12 times

✉  **jay209328032038** Most Recent 6 days, 1 hour ago

**Selected Answer: C**

Definitely 3 - Just tested on a live tenant, this is because you cannot choose Teams channels and chats with private chats, and you cannot choose Teams with OD/SPO/Exchange

upvoted 1 times

✉  **smiff** 3 weeks, 6 days ago

**Selected Answer: B**

2 policies, checked directly from compliance admin center on Sep 23, 23.

upvoted 1 times

✉  **mhmyz** 1 month ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/purview/create-retention-policies?tabs=teams-retention>

"Teams private channel messages: Messages from private channel chats and private channel meetings. If you select this option, you can't select the other Teams locations in the same retention policy."

upvoted 1 times

✉  **Nandokun01** 1 month, 3 weeks ago

Aside from adaptive policies you cannot create a policy with Teams channel messages and Teams private channel messages(<https://go.microsoft.com/fwlink/?linkid=2220113>). Thats 2 for teams and 1 for Exchange mailboxes, SharePoint, OneDrive = C:3

upvoted 2 times

✉  **Greatone1** 1 month, 4 weeks ago

**Selected Answer: C**

3 is the correct answer from previous test

upvoted 1 times

✉  **nublit** 2 months ago

**Selected Answer: B**

In my opinion the correct answer is B.

1 Retention policy for Exchange, OneDrive and SharePoint

1 Retention policy for Teams channels and chat.

upvoted 2 times

 **mrac** 2 months, 1 week ago

**Selected Answer: B**

To retain Microsoft 365 data for two years across all the mentioned locations (Microsoft Teams, OneDrive, Exchange Online, and SharePoint), you should create:

B. 2

One Retention Policy for Teams, OneDrive, and SharePoint:

Create a single retention policy that covers Microsoft Teams, OneDrive, and SharePoint. This policy will ensure that data stored in these locations is retained for the specified duration (two years).

Another Retention Policy for Exchange Online:

Create a separate retention policy for Microsoft Exchange Online. This policy will ensure that emails and related data stored in Exchange Online mailboxes are also retained for the same duration (two years).

So, the correct answer is B. 2 retention policies.

upvoted 2 times

 **osxzkwpfcfxobqjby** 2 months, 1 week ago

**Selected Answer: B**

Just checked.

Policy 1

- Microsoft OneDrive
- Microsoft SharePoint
- Microsoft Exchange Online

Policy 1

- Microsoft Teams

<https://learn.microsoft.com/en-us/purview/create-retention-policies?tabs=other-retention>

<https://compliance.microsoft.com/informationgovernance?viewid=retention>

upvoted 3 times

**HOTSPOT -**

You have a Microsoft 365 tenant.

You plan to create a retention policy as shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

**Answer Area**

Microsoft SharePoint files that are affected by the policy will be [answer choice].

recoverable for up to seven years  
deleted seven years after they were created  
retained for only seven years from when they were created

Once the policy is created, [answer choice].

some data may be deleted immediately  
data will be retained for a minimum of seven years  
users will be prevented from permanently deleting email messages for seven years

**Correct Answer:**

**Answer Area**

Microsoft SharePoint files that are affected by the policy will be [answer choice].

recoverable for up to seven years  
deleted seven years after they were created  
retained for only seven years from when they were created

Once the policy is created, [answer choice].

some data may be deleted immediately  
data will be retained for a minimum of seven years  
users will be prevented from permanently deleting email messages for seven years

**Mr4D97** Highly Voted 2 months ago

Deleted 7 years after they were created = Correct

Data will be retained for a min of 7 years = incorrect, data will be stored for a MAX of 7 years

Should be: "Some data will be deleted immediately" (as it says data that is currently older than 7 years will be deleted once this policy is enabled)  
upvoted 18 times

**gomezmax** Most Recent 1 month, 3 weeks ago

First one is correct Deleted 7 years after they were created = Correct

but 2nd It's not correct should be some data may be deleted immediately

upvoted 4 times

You have a Microsoft 365 subscription.

You need to configure a compliance solution that meets the following requirements:

Defines sensitive data based on existing data samples

Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages

Which two components should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a trainable classifier
- B. a sensitive info type
- C. an insider risk policy
- D. an adaptive policy scope
- E. a data loss prevention (DLP) policy

**Correct Answer: AE**

*Community vote distribution*

AE (69%) BE (31%)

 **Hard1k** Highly Voted 1 month, 2 weeks ago

**Selected Answer: AE**

The correct answers are A and E.

A. A trainable classifier is used to define sensitive data based on existing data samples.

E. A data loss prevention (DLP) policy is used to automatically prevent data that matches the samples from being shared externally in Microsoft SharePoint or email messages.

The other options are not necessary for this solution.

B. A sensitive info type is a pre-defined category of sensitive data. This can be used to help you create a DLP policy, but it is not required.

C. An insider risk policy is used to detect and prevent malicious activity by internal users. This is not relevant to the requirement to prevent sensitive data from being shared externally.

D. An adaptive policy scope is used to define the scope of a DLP policy. This can be used to fine-tune the policy to apply to specific users, groups, or locations. However, it is not required for this solution.

upvoted 7 times

 **sherifhamed** Most Recent 2 weeks, 5 days ago

**Selected Answer: AE**

The correct answer is A and E. You should configure a trainable classifier and a data loss prevention (DLP) policy.

upvoted 1 times

 **Casticod** 1 month, 1 week ago

**Selected Answer: AE**

Watch this: Defines sensitive data based on existing data samples

For this mi decisión its A+E.

A Microsoft Purview trainable classifier is a tool you can train to recognize various types of content by giving it samples to look at. Once trained, you can use it to identify items for application of Office sensitivity labels, Communications compliance policies, and retention label policies.  
<https://learn.microsoft.com/en-us/purview/classifier-get-started-with>

upvoted 1 times

 **RJTW070** 1 month, 1 week ago

**Selected Answer: BE**

From MS 101 exam <https://www.examtopics.com/discussions/microsoft/view/103044-exam-ms-101-topic-3-question-161-discussion/>

See this

upvoted 1 times

 **Nandokun01** 1 month, 3 weeks ago

"Define from available sample data" means it's looking for a trainable classifier as the SIT definition in the DLP policy. Answer is AE(<https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide>)

upvoted 3 times

 **gomezmax** 1 month, 3 weeks ago

Agree Should be, BE

upvoted 1 times

 **Greatone1** 1 month, 4 weeks ago

**Selected Answer: BE**

From MS 101 exam <https://www.examtopics.com/discussions/microsoft/view/103044-exam-ms-101-topic-3-question-161-discussion/>  
upvoted 3 times

 **Nandokun01** 1 month, 3 weeks ago

Previous test question most voted answer is insider risk policy which is wrong. "define from available sample data" means its looking for a trainable classifier as the SIT definition in the DLP policy. Answer is AE(<https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide>)

upvoted 5 times

**HOTSPOT -**

You have a Microsoft 365 subscription that contains a Microsoft SharePoint site named Site1. Site1 has the files shown in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	2
File4.bmp	3
File5.doc	5

For Site1, users are assigned the roles shown in the following table.

Name	Role
User1	Owner
User2	Visitor

You create a data loss prevention (DLP) policy named Policy1 that contains a rule as shown in the following exhibit.

## Edit rule

### Conditions

We'll apply this policy to content that matches these conditions.

#### Content contains

Default

Any of these

#### Sensitive info types

IP Address

High confidence



Instance count

2

to Any



Add

Create group

+ Add condition

### Exceptions

We won't apply this rule to content that matches any of these exceptions.

+ Add exception

### Actions

Use actions to protect content when the conditions are met.

#### Restrict access or encrypt the content in Microsoft 365 locations

##### Restrict access or encrypt the content in Microsoft 365 locations

Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.

By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.

Block everyone.

Block only people outside your organization.

Block only people who were given access to the content through the "Anyone with the link" option.

How many files will be visible to User1 and User2 after Policy1 is applied to Site1? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

## Answer Area

User1:

1
2
3
4
5

User2:

1
2
3
4
5

## Answer Area

User1:

1
2
3
4
5

Correct Answer:

User2:

1
2
3
4
5

 **mhmyz** 1 month ago

File types supported for scanning

The following file types are supported for scanning, for schema extraction, and classification where applicable:

Structured file formats supported by extension include scanning, schema extraction, and asset and column level classification: AVRO, ORC, PARQUET, CSV, JSON, PSV, SSV, TSV, TXT, XML, GZIP

Document file formats supported by extension include scanning and asset level classification: DOC, DOCM, DOCX, DOT, ODP, ODS, ODT, PDF, POT, PPS, PPSX, PPT, PPTM, PPTX, XLC, XLS, XLSB, XLSM, XLSX, XLT

<https://learn.microsoft.com/en-us/purview/microsoft-purview-connector-overview>

upvoted 4 times

 **hogehogehoge** 1 month, 3 weeks ago

I think bmpfile is not target in this rule. So User2 can open file4.

upvoted 3 times

 **osxvkwpfcfxobqjby** 2 months, 1 week ago

Instances found in doc is 2 or more.

User1: can open all files because he is the owner: 5

User2: can open files with less than 2 IPs: 1

<https://support.microsoft.com/en-us/office/overview-of-data-loss-prevention-in-sharepoint-server-2016-and-2019-80f907bb-b944-448d-b83d-8fec4abcc24c>

upvoted 2 times

 **sergioandreslq** 3 days, 9 hours ago

- Block everyone. Only the content owner, last modifier, and site admin will continue to have access

<https://learn.microsoft.com/en-us/purview/dlp-policy-reference#actions>

User1 Owner: can open all files because he is the owner: 5  
User2: can open files with less than 2 ips and the format is not supported by data classification  
User 2 can see: file1.docx, file4.bmp,  
however,  
the file2.txt-file5.xlsx and file5.doc are supported for data classification and the content has more than 2 ips.  
upvoted 2 times

 **Nandokun01** 1 month, 3 weeks ago

file type is .bmp = out of scope (unless OCR is enabled). Answer is 5/2  
upvoted 6 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

#### PROVISION FROM ACTIVE DIRECTORY



##### Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

##### Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

#### USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.

You need to ensure that User2 can access the resources in Azure AD.

Solution: From the Microsoft Entra admin center, you assign User2 the Security Reader role. You instruct User2 to sign in as user2@contoso.com.

Does this meet the goal?

A. Yes

B. No

#### Correct Answer: B

Community vote distribution

B (100%)

**mhmyz** 1 month ago

B.No

Correct solution is to make custom domain named fabricam.com.

upvoted 1 times

**Greatone1** 1 month, 4 weeks ago

**Selected Answer: B**

Should be no

upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

#### PROVISION FROM ACTIVE DIRECTORY



##### Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

##### Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

#### USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.

You need to ensure that User2 can access the resources in Azure AD.

Solution: From the on-premises Active Directory domain, you set the UPN suffix for User2 to @contoso.com. You instruct User2 to sign in as user2@contoso.com.

Does this meet the goal?

A. Yes

B. No

#### Correct Answer: A

Community vote distribution

A (100%)

Greatone1 1 month, 4 weeks ago

**Selected Answer: A**

Correct answer is A

upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

#### PROVISION FROM ACTIVE DIRECTORY



##### Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

##### Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

#### USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.

You need to ensure that User2 can access the resources in Azure AD.

Solution: From the Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com.

Does this meet the goal?

A. Yes

B. No

#### Correct Answer: A

##### Community vote distribution

B (50%)

A (50%)

**jbuexamtopics** 2 days, 1 hour ago

**Selected Answer: B**

Very tricky, I'll go for B because it didn't mention that fabrikam.com was verified.

upvoted 1 times

**sherifhamed** 2 weeks, 4 days ago

**Selected Answer: A**

The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

review:

<https://www.examtopics.com/discussions/microsoft/view/50100-exam-ms-100-topic-2-question-56-discussion/>

upvoted 2 times

**Casticod** 1 month, 1 week ago

**Selected Answer: B**

From the first reading, I think that the local active directory has the UPN added, since the user logs in locally with Fabrikam.com. I can add the domain Fabrikam.com to Entra admin center. What happens is that the question does not make it clear if the domain configuration is completed. If this step is not taken, when you synchronize and check, it will assign the domain onmicrosoft.com and not Fabrikam.com, the answer is NO

upvoted 3 times

 **letters1234** 1 month, 2 weeks ago

**Selected Answer: B**

Wouldnt this be no, due to there being no federation between the two domains, yes someone could sign in, however there is no notes around the domain being verified or any other setup that would also be required to allow federated sign in. The previous question, where they basically create a user called User2 in the existing domain and ask them to sign in is the most likely if there is a single correct answer. This question feels like only part of the story.

upvoted 2 times

 **Greatone1** 1 month, 2 weeks ago

Looking at previous test no one has a real answer.

<https://www.examtopics.com/discussions/microsoft/view/50100-exam-ms-100-topic-2-question-56-discussion/>

upvoted 1 times

 **Greatone1** 1 month, 3 weeks ago

**Selected Answer: A**

the answer is A.

upvoted 4 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain.

You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD.

Solution: You run idfix.exe and export the 10 user accounts.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **RJTW070** 1 month, 1 week ago

**Selected Answer: B**

No, running idfix.exe and exporting the 10 user accounts does not meet the goal of ensuring that the 10 user accounts are synchronized to Azure AD. IdFix is a tool used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory1. It provides you the ability to query, identify, and remediate the majority of object synchronization errors in your Window's Server AD forests in preparation for deployment to Microsoft 3652. However, simply exporting the 10 user accounts using IdFix will not ensure that they are synchronized to Azure AD. You need to review the errors reported by IdFix and take appropriate actions to fix them before synchronizing the accounts to Azure AD

upvoted 2 times

 **RJTW070** 1 month, 1 week ago

**Selected Answer: B**

No, modifying the Azure AD credentials from Azure AD Connect does not meet the goal of ensuring that the 10 user accounts are synchronized to Azure AD. If you have discovered that 10 user accounts in an organizational unit (OU) are not synchronized to Azure AD, while all the other user accounts synchronized successfully, and you have reviewed Azure AD Connect Health and discovered that all the user account synchronizations completed successfully, then you should troubleshoot an object that is not syncing with Azure Active Directory1. You can start by understanding the synchronization process and then follow the troubleshooting steps mentioned in the article

upvoted 1 times

 **Takanami** 1 month, 3 weeks ago

To give more context to why Answer is B:

You need to check if that OU containing those 10 users who are not synchronized is part of the OU Filtering option in Azure AD Connect. Check the box for that OU and save, the sync will start immediately after saving changes in Azure AD Connect.

upvoted 1 times

 **Greatone1** 1 month, 4 weeks ago

**Selected Answer: B**

Correct answer should be no

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain.

You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD.

Solution: From Azure AD Connect, you modify the Azure AD credentials.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **RJTW070** 1 month, 1 week ago

**Selected Answer: B**

No, modifying the Azure AD credentials from Azure AD Connect does not meet the goal of ensuring that the 10 user accounts are synchronized to Azure AD. If you have discovered that 10 user accounts in an organizational unit (OU) are not synchronized to Azure AD, while all the other user accounts synchronized successfully, and you have reviewed Azure AD Connect Health and discovered that all the user account synchronizations completed successfully, then you should troubleshoot an object that is not syncing with Azure Active Directory1.

upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain.

You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD.

Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

*Community vote distribution*

A (71%)      B (29%)

✉️  **sherifhamed** 2 weeks, 4 days ago

**Selected Answer: B**

Suggested Answer: B 

The question states that "all the user account synchronizations completed successfully". Therefore, the synchronization rule is configured correctly. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering>

-----

Review:

<https://www.examtopics.com/discussions/microsoft/view/10379-exam-ms-100-topic-3-question-16-discussion/>

upvoted 1 times

✉️  **santi32** 3 weeks, 3 days ago

**Selected Answer: B**

No, this solution doesn't necessarily meet the goal.

If the 10 user accounts in an OU are not being synchronized to Azure AD, it's more likely an issue with the scope of the synchronization (i.e., which OUs are selected for synchronization) rather than a need for a new outbound synchronization rule.

To resolve the issue, you'd typically:

Open the Azure AD Connect tool on the server where it's installed.

Check the configuration to see which OUs are selected for synchronization.

Ensure the OU containing the 10 user accounts is selected for synchronization.

Creating a new outbound synchronization rule without addressing the potential OU filtering issue would not guarantee synchronization of those 10 user accounts.

upvoted 1 times

✉️  **RJTW070** 1 month, 1 week ago

**Selected Answer: A**

Yes, creating a new outbound synchronization rule from the Synchronization Rules Editor could potentially solve the issue<sup>1</sup>. However, you need to be careful while creating the rule and ensure that it correctly targets the 10 user accounts in the specific Organizational Unit (OU) that are not being synchronized<sup>2</sup>. Also, any changes to synchronization rules should be done by an advanced user as incorrect changes may result in deletion of objects from your target directory

upvoted 1 times

✉️  **letters1234** 1 month, 2 weeks ago

**Selected Answer: A**

Other two answers for this group are definitely no, this one is yes as the OU may be excluded or not part of what was setup to sync.

upvoted 1 times

✉️  **Greatone1** 1 month, 3 weeks ago

**Selected Answer: A**

Correct answer should be yes  
upvoted 2 times

 **osxvkwpfcfxobqjby** 2 months, 1 week ago

**Selected Answer: A**

The other administrator has forgotten/meshedup a rule so you have to create an extra one.

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-create-custom-sync-rule>

upvoted 1 times

**HOTSPOT -**

You have a Microsoft 365 subscription.

You need to review metrics for the following:

The daily active users in Microsoft Teams

Recent Microsoft service issues -

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Teams daily active users:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

Recent Microsoft service issues:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

**Answer Area**

Teams daily active users:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

Correct Answer:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

 **gomezmax** 1 month, 3 weeks ago

Correct

upvoted 2 times

 **Casticod** 2 months ago

The answer is correct if we take the values offered, but we must be attentive to whether in the exam they add the statistics section of the team administration portal, since (in a period of 7 days) but you can see the activity of one of them by hovering over the selected day or exporting the report to CSV

upvoted 3 times

## DRAG DROP -

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2.

You need to ensure that each group can perform the tasks shown in the following table.

Group	Task
Group1	<ul style="list-style-type: none"> <li>Manage service requests.</li> <li>Purchase new services.</li> <li>Manage subscriptions.</li> <li>Monitor service health.</li> </ul>
Group2	<ul style="list-style-type: none"> <li>Assign licenses.</li> <li>Add users and groups.</li> <li>Create and manage user views.</li> <li>Update password expiration policies.</li> </ul>

The solution must use the principle of least privilege.

Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Roles**

Billing Administrator

Global Administrator

Helpdesk Administrator

License Administrator

Service Support Administrator

User Administrator

**Answer Area**Group1:  RoleGroup2:  Role**Answer Area**

Correct Answer:

Group1: Billing Administrator

Group2: User Administrator

amurp35 1 month ago

correct <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference?view=o365-worldwide#billing-administrator>  
 upvoted 1 times

Casticod 2 months ago

Correct: <https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide#commonly-used-microsoft-365-admin-center-roles>  
 upvoted 1 times

You have a Microsoft 365 subscription.

You need to add additional onmicrosoft.com domains to the subscription. The additional domains must be assignable as email addresses for users.

What is the maximum number of onmicrosoft.com domains the subscription can contain?

- A. 1
- B. 2
- C. 5
- D. 10

**Correct Answer: C**

*Community vote distribution*

C (63%) A (38%)

✉  **nsotis28** Highly Voted 1 month, 3 weeks ago

i created 5 "onMicrosoft" domains and added all of them as additional email address. Also i received a test email on all of them so i'll select 5  
Correct answer C

upvoted 5 times

✉  **sherifhamed** Most Recent 2 weeks, 5 days ago

**Selected Answer: C**

The correct answer is C. 5.

According to the first web search result1, you can add additional onmicrosoft.com domains to your Microsoft 365 subscription, but you are limited to a total of five onmicrosoft.com domains in your Microsoft 365 environment. Once they are added, they cannot be removed. You can use these domains as email addresses for your users, as well as for other services such as SharePoint and Teams.

upvoted 1 times

✉  **Tjorno** 3 weeks ago

**Selected Answer: C**

Only 5 onmicrosoft domains are possible

upvoted 1 times

✉  **martin\_salan07** 3 weeks ago

**Selected Answer: C**

[https://learn.microsoft.com/pt-BR/microsoft-365/admin/setup/add-or-replace-your-onmicrosoftcom-domain?view=o365-worldwide&WT.mc\\_id=365AdminCSH\\_inproduct](https://learn.microsoft.com/pt-BR/microsoft-365/admin/setup/add-or-replace-your-onmicrosoftcom-domain?view=o365-worldwide&WT.mc_id=365AdminCSH_inproduct)

upvoted 1 times

✉  **santi32** 3 weeks, 3 days ago

**Selected Answer: A**

Every Microsoft 365 tenant comes with one default onmicrosoft.com domain. However, you cannot add additional onmicrosoft.com domains to the subscription. The primary purpose of the onmicrosoft.com domain is to allow the tenant to be functional (for email, for example) even if there's no custom domain associated.

So, the answer is:

- A. 1

upvoted 1 times

✉  **Casticod** 1 month, 4 weeks ago

**Selected Answer: C**

5 domains <https://learn.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq?view=o365-worldwide#why-do-i-have-an--onmicrosoft-com--domain>

upvoted 2 times

✉  **Casticod** 2 months ago

I also don't understand the question, because it says to assign email addresses, that means that aliases count. I only hope that the question does not touch me, but if it does, I would put 5

upvoted 2 times

✉  **moshkoshbgosh** 2 months ago

**Selected Answer: A**

The wording here could be misleading... while 5 is the maximum number of onmicrosoft.com domains that can be added, the question states "The additional domains must be assignable as email addresses for users" which means we can only have one active... so depending on how you interpret the question it could go either way...

upvoted 2 times

HOTSPOT -

You have an Azure AD tenant that contains the administrative units shown in the following table.

Name	Members
AU1	User1, User2
AU2	User3

You have the following users:

- A user named User1 that is assigned the Password Administrator for AU1 and AU2.
- A user named User2 that is assigned the User Administrator for AU1.
- A user named User3 that is assigned the User Administrator for the tenant.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
User1 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>
User2 can update the display name of User1.	<input type="radio"/>	<input type="radio"/>
User1 can reset the password of User2.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
User1 can reset the password of User3.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can update the display name of User1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can reset the password of User2.	<input type="radio"/>	<input checked="" type="radio"/>

Correct Answer:

 **gbartumeu** 1 month ago

I think is Y,Y,Y.

"If an administrator forgets their own password, ...":

"Ask another administrator to reset it for you. In this case, the other administrator must be either a Global admin, a User Management admin, or a Password admin. However, if the administrator who forgot their password is a Global admin, another Global administrator must reset it for them."

<https://learn.microsoft.com/es-es/training/modules/manage-secure-access-microsoft-365/2-manage-user-passwords>  
upvoted 4 times

 **Be41223** 1 month ago

The answer is N,Y,N.

User1 can't reset password of User3, not only are they in different administrative units, password administrators can only reset the passwords of non-admins and other password administrators.

User2 can update the display name of User1, User2 is a User administrator and is in the same Administrative unit as User1 allowing them control to do so.

User1 can't reset the password of User2, as User2 is a different admin. <https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide#commonly-used-microsoft-365-admin-center-roles>

upvoted 7 times

✉️👤 **JensV** 1 month ago

<https://learn.microsoft.com/en-us/azure/active-directory/roles/privileged-roles-permissions?tabs=admin-center#who-can-reset-passwords>

upvoted 2 times

✉️👤 **nsotis28** 1 month, 3 weeks ago

provided answer is correct

upvoted 1 times

✉️👤 **Greatone1** 1 month, 4 weeks ago

I think this one is correct as an Admin cannot reset another Admins password

upvoted 4 times

Your network contains an Active Directory domain named adatum.com that is synced to Azure AD.

The domain contains 100 user accounts.

The city attribute for all the users is set to the city where the user resides.

You need to modify the value of the city attribute to the three-letter airport code of each city.

What should you do?

- A. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.
- B. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets.
- C. From Windows PowerShell on a domain controller, run the Get-MgUser and Update-MgUser cmdlets.
- D. From Azure Cloud Shell, run the Get-MgUser and Update-MgUser cmdlets.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **sherifhamed** 2 weeks, 5 days ago

**Selected Answer: A**

The correct answer is A. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.

The Get-ADUser and Set-ADUser cmdlets are used to retrieve and modify user accounts in Active Directory. You can use these cmdlets to bulk update the city attribute for all the users in the domain by using a CSV file that contains the mapping of the city names to the airport codes. For example, you can create a CSV file like this:

upvoted 1 times

 **mhmyz** 4 weeks ago

**Selected Answer: A**

Get-ADUser

<https://learn.microsoft.com/en-us/powershell/module/activedirectory/get-aduser?view=windowsserver2022-ps>

Set-ADUser

<https://learn.microsoft.com/en-us/powershell/module/activedirectory/set-aduser?view=windowsserver2022-ps>

upvoted 1 times

 **Greatone1** 1 month, 4 weeks ago

**Selected Answer: A**

The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active Directory (Azure AD). Therefore, the city attribute must be changed in the on-premise Active Directory.

upvoted 2 times

**HOTSPOT -**

Your company has a Microsoft 365 E5 subscription.

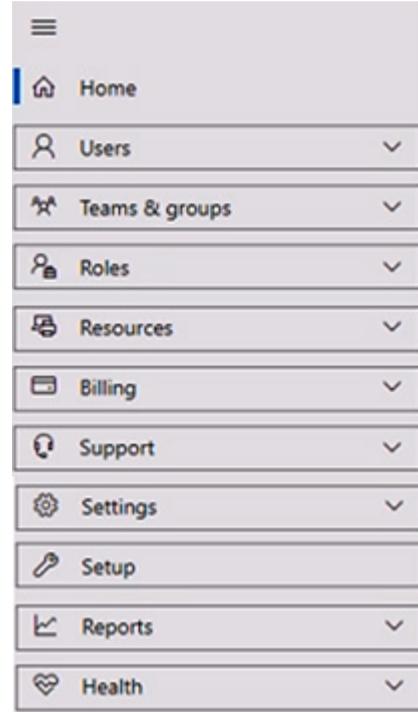
You need to perform the following tasks:

View the Adoption Score of the company.

Create a new service request to Microsoft.

Which two options should you use in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



**Correct Answer:**

A screenshot of the Microsoft 365 Admin Center navigation menu. The menu items listed vertically are: Home, Users, Teams & groups, Roles, Resources, Billing, Support, Settings, Setup, Reports, and Health. The 'Support' and 'Reports' items are highlighted with a thick black rectangular border around their respective rows.

**gomezmax** 1 month, 3 weeks ago

IT is Reports then Adoption Score  
upvoted 2 times

**Casticod** 2 months ago

Correct.  
Support to open case a MS  
Report to access to the adoption Score  
upvoted 2 times

You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Type
Group1	Security
Group2	Mail-enabled security
Group3	Microsoft 365
Group4	Distribution

You add another user named User5 to the User Administrator role.

You need to identify which two management tasks User5 can perform.

Which two tasks should you identify? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Delete User2 and User4 only.
- B. Reset the password of User4 only.
- C. Reset the password of any user in Azure AD.
- D. Delete User1, User2, and User4 only.
- E. Reset the password of User2 and User4 only.
- F. Delete any user in Azure AD.

**Correct Answer:** AE

*Community vote distribution*

AE (100%)

 **Mustardonk** Highly Voted  2 months ago

Wrong picture?  
upvoted 5 times

 **sherifhamed** Most Recent  2 weeks, 4 days ago

The Question with the right picture here:

<https://www.examtopics.com/discussions/microsoft/view/98896-exam-ms-100-topic-3-question-21-discussion/>  
upvoted 4 times

 **Martham** 5 days, 21 hours ago

Thanks alot  
upvoted 1 times

 **sherifhamed** 2 weeks, 5 days ago

!!!!!!! Wrong picture !!!!!!  
upvoted 1 times

 **Tisi** 4 weeks, 1 day ago

Wrong picture  
upvoted 3 times

 **Master\_Tx** 1 month, 1 week ago

This doesnt match what's on the exam. There is a second image that should go with this.  
upvoted 2 times

 **Casticod** 2 months ago

Selected Answer: AE

A and E are correct.  
upvoted 1 times

 **f7d3be6** 2 months ago

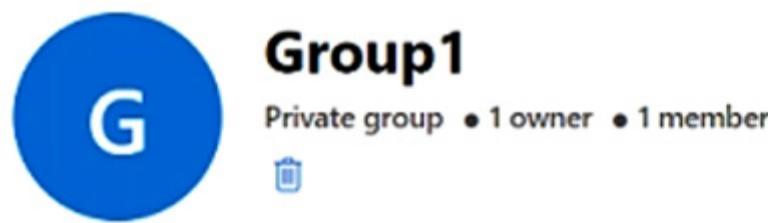
<https://www.examtopics.com/discussions/microsoft/view/98896-exam-ms-100-topic-3-question-21-discussion/>  
upvoted 2 times

 **Vaati** 2 months ago

Seems Wrong picture indeed  
upvoted 3 times

**HOTSPOT -**

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.



General Members **Settings** Microsoft Teams

**General settings**

- Allow external senders to email this group  Private  
 Send copies of group conversations and events to group members  Public

- Hide from my organization's global address list

**Privacy**

- Private  
 Public

An external user named User1 has an email address of user1@outlook.com.

You need to add User1 to Group1.

What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Action:

- Add User1 to the subscription as an active user.  
For Group1, change the Privacy setting to Public.  
For Group1, select Allow external senders to email this group.  
Invite User1 to collaborate with your organization as a guest.

Portal:

- The Microsoft Entra admin center  
The Exchange admin center  
The Microsoft 365 admin center  
The Microsoft Purview compliance portal

**Answer Area**

Action:

- Add User1 to the subscription as an active user.  
For Group1, change the Privacy setting to Public.  
For Group1, select Allow external senders to email this group.  
**Invite User1 to collaborate with your organization as a guest.**

Correct Answer:

Portal:

- The Microsoft Entra admin center**  
The Exchange admin center  
The Microsoft 365 admin center  
The Microsoft Purview compliance portal

**Casticod** 1 month, 2 weeks ago

I just tested in my test tenant that from the Microsoft 365 portal you can create a guest user and add it to an existing group. Therefore in the second section there are 2 possible answers. Microsoft 365 admin center and Entra admin center... OMG I have always done it for Entra and I didn't know this

upvoted 2 times

**GLL** 1 month ago

I have tried to invite an external user to my test tenant as a guest in Microsoft 365 admin center. and it will automatically turn to Entra admin center.

upvoted 1 times

✉️ **Master\_Tx** 1 month, 1 week ago

You're correct. There are two possible answers in section 2, as you can use both admin portals to do this.

upvoted 1 times

✉️ **hogehogehoge** 1 month, 3 weeks ago

I think portal is The Microsoft 365 administrator. Because I test my lab. It is impossible to change group type in Entra portal.

upvoted 1 times

✉️ **hogehogehoge** 1 month, 3 weeks ago

Sorry. This answer is correct. Because Group type is not necessary to change.

upvoted 1 times

✉️ **Greatone1** 1 month, 4 weeks ago

Given answer is correct

<https://www.examtopics.com/discussions/microsoft/view/94423-exam-ms-100-topic-3-question-94-discussion/>

upvoted 2 times

Question #59

Topic 1

You have a Microsoft 365 subscription that contains a user named User1.

User1 requires admin access to perform the following tasks:

Manage Microsoft Exchange Online settings.

Create Microsoft 365 groups.

You need to ensure that User1 only has admin access for eight hours and requires approval before the role assignment takes place.

What should you use?

- A. Azure AD Identity Protection
- B. Microsoft Entra Verified ID
- C. Conditional Access
- D. Azure AD Privileged Identity Management (PIM)

**Correct Answer: D**

*Community vote distribution*

D (100%)

✉️ **RJTW070** 1 month, 1 week ago

**Selected Answer: D**

Pim should be right

upvoted 2 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type
Group1	Security
Group2	Mail-enabled security
Group3	Microsoft 365
Group4	Distribution

All the groups are deleted.

Which groups can be restored, and what is the retention period? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Groups that can be restored:

- Group3 only
- Group1 and Group2 only
- Group2 and Group4 only
- Group1, Group2, and Group3 only
- Group1, Group2, Group3, and Group4

Retention period:

- 24 hours
- 7 days
- 14 days
- 30 days
- 90 days

**Answer Area**

Groups that can be restored:

- Group3 only**
- Group1 and Group2 only
- Group2 and Group4 only
- Group1, Group2, and Group3 only
- Group1, Group2, Group3, and Group4

Correct Answer:

Retention period:

- 24 hours
- 7 days
- 14 days
- 30 days**
- 90 days

 **imlearningstuffagain** 6 days, 22 hours ago

Correct: [https://learn.microsoft.com/en-US/microsoft-365/admin/create-groups/restore-deleted-group?view=o365-worldwide&WT.mc\\_id=365AdminCSH\\_inproduct&tabs=outlook](https://learn.microsoft.com/en-US/microsoft-365/admin/create-groups/restore-deleted-group?view=o365-worldwide&WT.mc_id=365AdminCSH_inproduct&tabs=outlook)

upvoted 1 times

 **sherifhamed** 2 weeks, 5 days ago

Correct.

According to the web search results, you can restore only Microsoft 365 groups that have been deleted within the last 30 days, unless they have been permanently purged.

upvoted 1 times

 **amurp35** 1 month ago

Correct. The reason for the ability to restore something that is deleted in the M 365 world is to recover data. There is no data associated with any of those groups and therefore no restore function as you can just recreate them yourself with no harm. The 365 group however, has a mailbox and other data associated with it and therefore must be covered by retention, compliance, discovery, etc. and be recoverable.

upvoted 1 times

 **Greatone1** 1 month, 2 weeks ago

Letters already provided the answer only m 365 groups can be restored not security or distribution groups. This functionality is restricted exclusively to Microsoft 365 groups in Azure AD. It isn't available for security groups and distribution groups. Please note that the 30-day group restoration period isn't customizable.

upvoted 2 times

✉️ **letters1234** 1 month, 2 weeks ago

When you delete a Microsoft 365 group in Azure Active Directory (Azure AD), part of Microsoft Entra, the deleted group is retained but not visible for 30 days from the deletion date. This behavior is so that the group and its contents can be restored if needed. This functionality is restricted exclusively to Microsoft 365 groups in Azure AD. It isn't available for security groups and distribution groups.

Mail-enabled security group is still a security group

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-restore-deleted>

upvoted 2 times

✉️ **Greatone1** 1 month, 3 weeks ago

Should be group 3 and 30 days

upvoted 2 times

✉️ **DiligentSam** 1 month, 3 weeks ago

From ChatGPT, Mail-enabled security, Microsoft 365 and Distribution can be restored.

but i can't find this answer

Q2 30 days

upvoted 1 times

✉️ **amurp35** 1 month ago

ChatGPT and other tools will quite often give you the wrong answers because it "sounds right" to their algorithms.

upvoted 2 times

✉️ **Greatone1** 1 month, 4 weeks ago

Deleted users and deleted Office 365 groups are available for restore for 30 days. You cannot restore a deleted security group.

upvoted 2 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription.

From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

**Activation**

Setting	State
Activation maximum duration (hours)	8 hour(s)
On activation, require	Azure MFA
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	No
Approvers	None

**Assignment**

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	15 day(s)
Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	Yes

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

**Answer Area**

A user that is assigned the Global Administrator role as active [answer choice].

▼

will lose the role after eight hours  
can reactivate the role every eight hours  
can reactivate the role every 15 days  
will lose the role after 15 days

You can make the Global Administrator role available to activation requests [answer choice].

▼

for up to eight hours  
for up to three months  
for up to 15 days  
until the requests are revoked manually

**Answer Area**

A user that is assigned the Global Administrator role as active [answer choice].

▼

will lose the role after eight hours  
can reactivate the role every eight hours  
can reactivate the role every 15 days  
will lose the role after 15 days

**Correct Answer:**

You can make the Global Administrator role available to activation requests [answer choice].

▼

for up to eight hours  
for up to three months  
for up to 15 days  
until the requests are revoked manually

1) 15 days. The user is Assigned the role in active state. The active assignment expires after 15 days, as shown in the config details. 2) the role can be made available to activation requests for 3 months. This is because the role assignment can be an Eligible assignment and an Eligible assignment is configured to expire after 3 months. Eligible assignments require themselves to be activated just in time by the assignee within the 3 month period.

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user>  
upvoted 11 times

✉️ **Shloeb** 3 weeks, 2 days ago

Correct. Others are misunderstanding this. 8 hours is meant for the activation request not the actual assignment.  
upvoted 2 times

✉️ **amurp35** 1 month ago

meant to reference this 2nd link as well that completely clarifies the point: <https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings?source=recommendations>  
upvoted 2 times

✉️ **santi32** Most Recent 3 weeks, 3 days ago

A user that is assigned the Global Administrator role as active [will lose the role after 15 days].  
You can make the Global Administrator role available to activation requests [for up to eight hours].  
upvoted 2 times

✉️ **spectre786** 1 month, 3 weeks ago

First one : will lose the role after 8 hours AND can reactivate every 8 hours  
Right ?  
upvoted 2 times

✉️ **Casticod** 1 month, 3 weeks ago

First Option Correct 8 Hours  
The second options are 15 Days... <https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-renew-extend>  
upvoted 3 times

✉️ **nsotis28** 1 month, 3 weeks ago

first is correct - will lose the role after 8 hours  
second is questionable -- why not 15 days ?  
upvoted 3 times

✉️ **cb0900** 1 month, 2 weeks ago

Re: the second question, agree it would be 15 days in this case.  
The first question states "A user that is assigned the Global Administrator role as active" and the active assignment is set to expire after 15 days.  
upvoted 2 times

**HOTSPOT -**

You have a Microsoft 365 subscription.

A user named user1@contoso.com was recently provisioned.

You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must NOT be enabled.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

```
-Scopes User.ReadWrite.All, Organization.Read.All

Connect-AzureAD
Connect-MgGraph
Connect-MSOLService

$E3 = Get-AzureADUser | Where SkuPartNumber -eq 'EnterprisePack'
Get-MgSubscribedSku
Get-MSOLAccountSKU

$disabledPlans = $E3.ServicePlans | Where ServicePlanName -in
("MICROSOFTBOOKINGS") | select -ExcludeProperty ServicePlanID

$licenseOptions= @(
    @{
        SkuId = $E3.SkuId
        DisabledPlans = $disabledPlans
    }
)
-UserId User1@contoso.com -AddLicenses $licenseOptions -RemoveLicenses @()

Set-AzureADUser
Set-MgUserLicense
Set-MSOLUser
```

**Answer Area**

```
-Scopes User.ReadWrite.All, Organization.Read.All

Connect-AzureAD
Connect-MgGraph
Connect-MSOLService

$E3 = Get-AzureADUser | Where SkuPartNumber -eq 'EnterprisePack'
Get-MgSubscribedSku
Get-MSOLAccountSKU

$disabledPlans = $E3.ServicePlans | Where ServicePlanName -in
("MICROSOFTBOOKINGS") | select -ExcludeProperty ServicePlanID

$licenseOptions= @(
    @{
        SkuId = $E3.SkuId
        DisabledPlans = $disabledPlans
    }
)
-UserId User1@contoso.com -AddLicenses $licenseOptions -RemoveLicenses @()

Set-AzureADUser
Set-MgUserLicense
Set-MSOLUser
```

**Correct Answer:**

  **Ruhansen** 1 month ago

Correct - All Graph commands

upvoted 1 times

  **929826d** 1 month, 4 weeks ago

Correct

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365-powershell?view=o365-worldwide>

upvoted 2 times

You have a Microsoft E5 subscription.

You need to ensure that administrators who need to manage Microsoft Exchange Online are assigned the Exchange Administrator role for five hours at a time.

What should you implement?

- A. Azure AD Privileged Identity Management (PIM)
- B. a conditional access policy
- C. a communication compliance policy
- D. Azure AD Identity Protection
- E. groups that have dynamic membership

**Correct Answer: A**

 **Paul\_white** 2 weeks, 2 days ago

GIVEN ANSWERS IS CIRRECT!!!

upvoted 1 times

You have a Microsoft 365 subscription.

You suspect that several Microsoft Office 365 applications or services were recently updated.

You need to identify which applications or services were recently updated.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. From the Microsoft 365 admin center, review the Service health blade.
- B. From the Microsoft 365 admin center, review the Message center blade.
- C. From the Microsoft 365 admin center, review the Products blade.
- D. From the Microsoft 365 Admin mobile app, review the messages.

**Correct Answer: BD**

*Community vote distribution*

BD (50%)

AB (50%)

 **sherifhamed** 2 weeks, 4 days ago

**Selected Answer: BD**

B & D is correct

Take a look here:

<https://www.examtopics.com/discussions/microsoft/view/26962-exam-ms-100-topic-2-question-19-discussion/>  
upvoted 4 times

 **saya\_222** 3 weeks, 1 day ago

A&B is correct.

<https://www.examtopics.com/exams/microsoft/ms-100/view/7/>  
upvoted 1 times

 **sherifhamed** 2 weeks, 4 days ago

A&B are B&D Here

- B. From the Microsoft 365 admin center, review the Message center blade.
- D. From the Office 365 Admin mobile app, review the messages.

upvoted 1 times

 **saya\_222** 3 weeks, 1 day ago

Topic2 #19

upvoted 1 times

 **Hard1k** 1 month, 2 weeks ago

**Selected Answer: AB**

A. From the Microsoft 365 admin center, review the Service health blade. The Service health blade in the Microsoft 365 admin center provides information about the status of Microsoft 365 services. If a service has been recently updated, it will be listed on the Service health blade.

B. From the Microsoft 365 admin center, review the Message center blade. The Message center blade in the Microsoft 365 admin center provides information about important messages from Microsoft. If there have been any recent updates to Microsoft Office 365 applications or services, a message will be posted in the Message center.

The other options are not correct. Option C, reviewing the Products blade in the Microsoft 365 admin center, will not show you which applications or services have been recently updated. Option D, reviewing the messages in the Microsoft 365 Admin mobile app, will only show you messages that have been sent to you personally.

upvoted 4 times

 **Shloeb** 3 weeks, 1 day ago

No. The given answer is correct. In the Microsoft 365 Admin App, Message Center plays the same role. It gives you any information about updates etc. It is not used for personal messages.

upvoted 1 times

You have a Microsoft 365 subscription that contains the domains shown in the following exhibit.

## Domains

+ Add domain    Buy domain    Refresh

Domain name ↑	Status	Choose columns
Sub1.contoso221018.onmicrosoft.com (D...)	⚠ Possible service issues	
contoso.com	ℹ Incomplete setup	
contoso221018.onmicrosoft.com	✓ Healthy	
Sub2.contoso221018.onmicrosoft.com	ℹ Incomplete setup	

Which domain name suffixes can you use when you create users?

- A. only Sub1.contoso221018.onmicrosoft.com
- B. only contoso221018.onmicrosoft.com and Sub2.contoso221018.onmicrosoft.com
- C. only contoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com
- D. all the domains in the subscription

**Correct Answer: B**

amurp35 Highly Voted 1 month ago

I believe the correct answer is not listed as an option. The correct answer would be sub1.contoso221018.onmicrosoft.com and contoso221018.onmicrosoft.com.

upvoted 6 times

DiligentSam Highly Voted 1 month, 3 weeks ago

my answer  
Sub1.contoso221018.onmicrosoft.com - Possible service issues  
contoso221018.onmicrosoft.com - healthy

upvoted 5 times

gomezmax Most Recent 1 week ago

B is correct

upvoted 1 times

sherifhamed 2 weeks, 3 days ago

check this:  
<https://www.examtopics.com/discussions/microsoft/view/49388-exam-ms-100-topic-3-question-75-discussion/>

upvoted 1 times

nsotis28 1 month, 3 weeks ago

Domains with status "incomplete setup" can not be used

upvoted 4 times

Casticod 1 month, 4 weeks ago

anything it's correct think that only contoso221018.onmicrosoft.com and Sub1.contoso221018.onmicrosoft.com until the domain is finished configuring the domain, accounts cannot be assigned to users, in a healthy state or with possible malfunctions if it can be

upvoted 1 times

Casticod 1 month, 4 weeks ago

In the exam Ms-100 exist a similar question, and the comments content excellent explaineds  
<https://www.examtopics.com/discussions/microsoft/view/49388-exam-ms-100-topic-3-question-75-discussion/>  
upvoted 4 times

 **letters1234** 1 month, 2 weeks ago

Not the same graphic in that question, in ours the Sub2 is incomplete. Where in the other page, its showing as active/healthy. For ours, either graphics wrong or answer set is wrong.  
upvoted 1 times

 **Casticod** 1 month, 1 week ago

I'm Say... "and the comments content excellent explaineds" but I'm not say, that is the same Scenario.  
upvoted 2 times

 **Vaati** 2 months ago

Why B?

upvoted 2 times

You have a Microsoft 365 subscription.  
You plan to implement Microsoft Purview Privileged Access Management.  
Which Microsoft Office 365 workloads support privileged access?

- A. Microsoft Exchange Online only
- B. Microsoft Teams only
- C. Microsoft Exchange Online and SharePoint Online only
- D. Microsoft Teams and SharePoint Online only
- E. Microsoft Teams, Exchange Online, and SharePoint Online

**Correct Answer: A***Community vote distribution*

A (67%) E (33%)

✉  certma2023  2 months ago

**Selected Answer: A**

Answer A.

PAM only works with Exchange Online at that time. Based on my test you see only Exchange roles inside the O365 Admin Portal (Settings -> Org Settings -> Security & Privacy -> Privileged Access)

The documentation also says:

"When will privileged access support Office 365 workloads beyond Exchange?

Privileged access management will be available in other Office 365 workloads soon. Visit the Microsoft 365 Roadmap for more details."

<https://learn.microsoft.com/en-us/purview/privileged-access-management>

upvoted 6 times

✉  sherifhamed  2 weeks, 5 days ago

**Selected Answer: E**

E. Microsoft Teams, Exchange Online, and SharePoint Online

Privileged Access Management (PAM) can be implemented for Microsoft Teams, Exchange Online, and SharePoint Online, among other workloads. It's not limited to just one or two of these services but can be extended to cover these services and more, depending on your organization's requirements.

upvoted 2 times

✉  amurp35 4 weeks, 1 day ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/purview/privileged-access-management>

upvoted 4 times

✉  sherifhamed 2 weeks, 5 days ago

According to the reference that you provided, Microsoft Purview Privileged Access Management supports Microsoft Teams, Exchange Online, and SharePoint Online.

The correct answer is E. Microsoft Teams, Exchange Online, and SharePoint Online.

upvoted 1 times

✉  jbuexamtopics 2 weeks, 4 days ago

on what part of the document they mentioned it? Upon checking this is what's written on FAQ

When will privileged access support Office 365 workloads beyond Exchange?

Privileged access management will be available in other Office 365 workloads soon. Visit the Microsoft 365 Roadmap for more details.

upvoted 1 times

✉  jbuexamtopics 2 weeks, 4 days ago

Sorry this is for Access Support. But still, can you show us where it's mentioned on the link?

upvoted 1 times

✉  PhoenixMan 1 month ago

A is the correct answer,

<https://learn.microsoft.com/en-us/purview/privileged-access-management-solution-overview>

or <https://www.examtopics.com/discussions/microsoft/view/96751-exam-ms-100-topic-4-question-79-discussion/>

upvoted 2 times

 **RJTW070** 1 month, 1 week ago

**Selected Answer: E**

I agree E

upvoted 1 times

 **DiligentSam** 1 month, 3 weeks ago

From ChatGPT, answer is E

The documentation also says:

"When will privileged access support Office 365 workloads beyond Exchange?

Privileged access management will be available in other Office 365 workloads soon. Visit the Microsoft 365 Roadmap for more details."

upvoted 1 times

 **SandyBridge** 4 weeks, 1 day ago

If you are going to use ChatGPT, do us all a favor and do not spread misinformation.

upvoted 2 times

 **amurp35** 4 weeks, 1 day ago

Exactly: <https://learn.microsoft.com/en-us/purview/privileged-access-management> meaning PAM is not supported outside of Exchange Online

upvoted 1 times

 **Greatone1** 1 month, 4 weeks ago

**Selected Answer: A**

A is the correct answer

Source: <https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management?view=o365-worldwide>

upvoted 4 times

 **mrac** 2 months ago

**Selected Answer: E**

Microsoft Purview Privileged Access Management (PAM) helps you manage, control, and monitor access within Microsoft 365. It's designed to manage privileged access for various Microsoft Office 365 workloads, including Microsoft Teams, Exchange Online, and SharePoint Online.

So, the correct answer is E. Microsoft Teams, Exchange Online, and SharePoint Online.

upvoted 4 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Service Support Administrator
User3	Cloud Application Administrator
User4	None

You plan to provide User4 with early access to Microsoft 365 feature and service updates.

You need to identify which Microsoft 365 setting must be configured, and which user can modify the setting. The solution must use the principle of least privilege.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Microsoft 365 setting:

Office installation options  
 Privileged access  
 Release preferences

User:

User1 only  
 User2 only  
 User3 only  
 User1 and User2 only  
 User1 and User3 only

**Answer Area**

Microsoft 365 setting:

Office installation options  
Privileged access  
 Release preferences

**Correct Answer:**

User:

User1 only  
 User2 only  
User3 only  
 User1 and User2 only  
 User1 and User3 only

 certma2023 Highly Voted 2 months ago

Answer is wrong.

To have new features & updates on all users or some/targeted users you need to configure "release preference" for the entire organization/tenant. Only the Global Admins can change this.

<https://learn.microsoft.com/en-us/microsoft-365/admin/manage/release-options-in-office-365?view=o365-worldwide#set-up-the-release-option-in-the-admin-center>

upvoted 18 times

 nsotis28 Highly Voted 1 month, 3 weeks ago

release preferences

user1

upvoted 9 times

 Casticod 1 month, 3 weeks ago

Me too

<https://learn.microsoft.com/en-us/microsoft-365/admin/manage/release-options-in-office-365?view=o365-worldwide>

upvoted 5 times

✉  **imlearningstuffagain** Most Recent 6 days, 21 hours ago

The suggested answer is wrong: <https://learn.microsoft.com/en-us/microsoft-365/admin/manage/release-options-in-office-365?view=o365-worldwide>

Partial quote: "You can change how your organization receives Microsoft 365 updates by following these steps. You have to be a global admin in Microsoft 365 to opt in."

upvoted 2 times

Question #68

Topic 1

HOTSPOT -

You have a Microsoft 365 subscription.

You are planning a threat management solution for your organization.

You need to minimize the likelihood that users will be affected by the following threats:

Opening files in Microsoft SharePoint that contain malicious content

Impersonation and spoofing attacks in email messages

Which policies should you create in Microsoft 365 Defender? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

Opening files in SharePoint that contain malicious content:

- Anti-spam
- Anti-Phishing
- Safe Attachments
- Safe Links

Impersonation and spoofing attacks in email messages:

- Anti-spam
- Anti-Phishing
- Safe Attachments
- Safe Links

#### Answer Area

Opening files in SharePoint that contain malicious content:

- Anti-spam
- Anti-Phishing
- Safe Attachments
- Safe Links

Correct Answer:

Impersonation and spoofing attacks in email messages:

- Anti-spam
- Anti-Phishing
- Safe Attachments
- Safe Links

✉  **gomezmax** 1 month, 1 week ago

Correct

upvoted 2 times

✉  **Greatone1** 1 month, 4 weeks ago

Yes correct

safe attachments

anti-phishing

upvoted 2 times

**HOTSPOT -**

You have a Microsoft 365 E5 tenant.

You have the alerts shown in the following exhibit.

[Home](#) > [Alerts](#) > [View alerts](#)

## View alerts

<input type="checkbox"/>	Severity	Alert name	Status	Tags	Category	Activity count	Last occurrence...
<input type="checkbox"/>	● Medium	Alert1	Active	-	Threat management	2	3 minutes ago
<input type="checkbox"/>	● High	Alert5	Resolved	-	Permissions	1	8 minutes ago

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

### Answer Area

For Alert1, you can change Status to [answer choice].

- Investigating only
- Investigating or Resolved only
- Investigating or Dismissed only
- Investigating, Resolved, or Dismissed

For Alert5, you can [answer choice].

- not change Status
- change Status to Dismissed only
- change Status to Dismissed or Active only
- change Status to Dismissed or Investigating only
- change Status to Dismissed, Investigating, or Active

### Answer Area

For Alert1, you can change Status to [answer choice].

- Investigating only
- Investigating or Resolved only
- Investigating or Dismissed only
- Investigating, Resolved, or Dismissed

### Correct Answer:

For Alert5, you can [answer choice].

- not change Status
- change Status to Dismissed only
- change Status to Dismissed or Active only
- change Status to Dismissed or Investigating only
- change Status to Dismissed, Investigating, or Active

**faeem** 2 weeks, 6 days ago

Hi, just tested now. Went to an incident and changed the status to resolved. Then went back into the incident and was able to change it back to in progress.

upvoted 1 times

**saya\_222** 3 weeks, 1 day ago

1 : Investigating, Resolved, or Dismissed  
2 : change Status to Dismissed, Investigating, or Active

<https://www.examtopics.com/exams/microsoft/ms-101/>

→Topic3 #140

upvoted 3 times

**Romke\_en\_Tomke** 2 weeks ago

You can post direct url: <https://www.examtopics.com/discussions/microsoft/view/94571-exam-ms-101-topic-3-question-140-discussion/>  
upvoted 1 times

**amurp35** 4 weeks, 1 day ago

The three status options are actually: 'New, In-Progress, or Resolved' and these options are not shown.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwide>

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-sec-ops-manage-incidents-and-alerts?view=o365-worldwide>  
upvoted 2 times

 **AMDF** 1 month, 1 week ago

Alert1 correct  
Alert5 should be "not change status"

For resolved issue there is no option to change status

upvoted 1 times

Question #70

Topic 1

You have a Microsoft 365 E3 subscription that uses Microsoft Defender for Endpoint Plan 1.

Which two Defender for Endpoint features are available to the subscription? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. advanced hunting
- B. security reports
- C. digital certificate assessment
- D. device discovery
- E. attack surface reduction (ASR)

**Correct Answer: BE**

*Community vote distribution*

BE (100%)

 **Hard1k** 1 month, 2 weeks ago

**Selected Answer: BE**

Correct answers  
upvoted 4 times

 **letters1234** 1 month, 2 weeks ago

Can only see ASR and reports on the features for Defender P1  
<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1?view=o365-worldwide>  
upvoted 3 times

 **Greatone1** 1 month, 4 weeks ago

**Selected Answer: BE**

Answer is correct  
<https://www.examtopics.com/discussions/microsoft/view/94078-exam-ms-101-topic-2-question-123-discussion/>  
upvoted 3 times

You are reviewing alerts in the Microsoft 365 Defender portal.

How long are the alerts retained in the portal?

- A. 30 days
- B. 60 days
- C. 3 months
- D. 6 months
- E. 12 months

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **Casticod** 1 month, 2 weeks ago

**Selected Answer: C**

Correct <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data-retention?view=o365-worldwide>  
upvoted 3 times

You have a Microsoft 365 E5 subscription.

From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users.

What is the longest time range that can be included in the report?

- A. 1 day
- B. 7 days
- C. 30 days
- D. 90 days

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **cb0900** 1 month, 2 weeks ago

**Selected Answer: C**

Agree. Detailed data for 30 days.  
<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-email-security?view=o365-worldwide#compromised-users-report>  
upvoted 1 times

 **Casticod** 1 month, 2 weeks ago

**Selected Answer: C**

Correct <https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-users?view=o365-worldwide#timeline>  
upvoted 1 times

**HOTSPOT -**

You have a Microsoft 365 subscription.

You deploy the anti-phishing policy shown in the following exhibit.

**Phishing threshold and protections****Phishing threshold**

- 1 - Standard

**User impersonation protection**

- On for 0 user(s)

**Domain impersonation protection**

- Off for owned domains
- Off - 0 domain(s) specified

**Trusted impersonated senders and domains**

- Off

**Mailbox intelligence**

- On

**Mailbox intelligence for impersonations**

- Off (Mailbox intelligence must be turned on to access this)

**Spoof intelligence**

- Off

**Edit protection settings**

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

**Answer Area**

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

Add trusted senders and domains
Enable domains to protect
Enable users to protect
Phishing email threshold

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

Add trusted senders and domains
Enable intelligence for impersonation protection
Enable spoof intelligence

**Answer Area**

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

Add trusted senders and domains
Enable domains to protect
<b>Enable users to protect</b>
Phishing email threshold

**Correct Answer:**

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

<b>Add trusted senders and domains</b>
Enable intelligence for impersonation protection
Enable spoof intelligence

 **faeem** 3 weeks, 1 day ago

If the sender already communicated, you cannot set impersonation: User impersonation protection does not work if the sender and recipient have previously communicated via email. If the sender and recipient have never communicated via email, the message can be identified as an impersonation attempt. <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about?view=o365-worldwide>

upvoted 1 times

 **amurp35** 4 weeks, 1 day ago

Looks correct to me. You want to add the CEO as a protected user for impersonation protection. You also want to add the other CEO as a trusted sender so as to ensure good email delivery to that person from your senders.

proof: see 5. here:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-mdo-configure?view=o365-worldwide>

"enable users to protect"

upvoted 3 times

 **Casticod** 1 month, 2 weeks ago

The second option, For me, should be Impersonation protection. <https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/email-protection-basics-in-microsoft-365-spoof-and-impersonation/ba-p/3562938>

upvoted 1 times

 **letters1234** 1 month, 2 weeks ago

Would probably go for Phishing threshold as looking at the policy in security.microsoft.com / policies & rules / threat policies:

Phishing threshold & protection

-Phishing threshold

1 - Standard

-User impersonation protection

Off - 0 sender(s) specified

-Domain impersonation protection

Off for owned domains

Off - 0 domain(s) specified

Would most likely want to set Domain Impersonation Protection to On for owned domains and configure that.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about?view=o365-worldwide#domain-impersonation-protection>

upvoted 2 times

**HOTSPOT -**

You use Microsoft Defender for Endpoint.

You have the Microsoft Defender for Endpoint device groups shown in the following table.

Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped devices (default)	Last	Not applicable

You plan to onboard computers to Microsoft Defender for Endpoint as shown in the following table.

Name	Operating system
Computer1-London	Windows 10
Server1-London	Windows Server 2016

To which device group will each computer be added? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Computer1-London:

Group1  
Group2  
Group3  
Ungrouped devices

Server1-London:

Group1  
Group2  
Group3  
Ungrouped devices

**Answer Area**

Computer1-London:

**Group1**  
Group2  
Group3  
Ungrouped devices

Correct Answer:

Server1-London:

**Group1**  
**Group2**  
Group3  
Ungrouped devices

 **jt2214** 2 weeks, 3 days ago

I I wish they were all this easy.

upvoted 1 times

 **amurp35** 4 weeks, 1 day ago

Yes, answer is correct due to rankings.

upvoted 1 times

 **Greatone1** 1 month, 4 weeks ago

Answer is correct. Devices can only be added to one group. They get added to the highest rank lowest number if they match multiple groups.

upvoted 2 times

**DRAG DROP -**

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You need to configure policies to meet the following requirements:

Customize the common attachments filter.

Enable impersonation protection for sender domains.

Which type of policy should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Policy Types	Answer Area
Anti-malware	Customize the common attachments filter: <input type="text"/>
Anti-phishing	Enable impersonation protection for sender domains: <input type="text"/>
Anti-spam	
Safe Attachments	

Policy Types	Answer Area
Correct Answer: Anti-spam	Customize the common attachments filter: <input checked="" type="text"/> Anti-malware
Safe Attachments	Enable impersonation protection for sender domains: <input checked="" type="text"/> Anti-phishing

 **amurp35** 4 weeks, 1 day ago

Correct

upvoted 1 times

 **f7d3be6** 2 months ago

Correct Antimalware ,anti-phishing <https://answers.microsoft.com/en-us/msoffice/forum/all/impersonation-protection/97b82164-5331-4ee6-97e0-423f17c55399>

upvoted 4 times

You have an Azure AD tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Security Operator
User3	Security Reader
User4	Compliance Administrator

You plan to implement Microsoft Defender for Endpoint.

You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint.

You need to identify which user can view security incidents from the Microsoft 365 Defender portal.

Which user should you identify?

- A. User1
- B. User2
- C. User3
- D. User4

**Correct Answer: A**

*Community vote distribution*

A (76%) C (24%)

✉️  **AMDF** Highly Voted 1 month, 1 week ago

**Selected Answer: A**

A is correct

Answer is correct "A". Security Administrator will not lose access after RBAC is enabled. Security Reader will so definitely not C.

Initially, only those with Azure AD Global Administrator or Security Administrator rights will be able to create and assign roles in Microsoft Defender Security Center, therefore, having the right groups ready in Azure AD is important.

Turning on role-based access control will cause users with read-only permissions (for example, users assigned to Azure AD Security reader role) to lose access until they are assigned to a role.

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide>

upvoted 7 times

✉️  **amurp35** Most Recent 4 weeks, 1 day ago

**Selected Answer: A**

"Turning on role-based access control will cause users with read-only permissions (for example, users assigned to Azure AD Security reader role) to lose access until they are assigned to a role."

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide>

upvoted 2 times

✉️  **Jillis** 1 month ago

**Selected Answer: A**

AMDF is correct

upvoted 2 times

✉️  **letters1234** 1 month, 2 weeks ago

**Selected Answer: C**

Security reader Security readers can perform the following tasks:

- View a list of onboarded devices
- View security policies
- View alerts and detected threats
- View security information and reports

Security readers can't add or edit security policies, nor can they onboard devices.

upvoted 2 times

✉️  **mccheesey** 1 month, 3 weeks ago

**Selected Answer: C**

This should be C I think...

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide>

"Security Reader - Members have read-only access to many security features of Identity Protection Center, Privileged Identity Management, Monitor Microsoft 365 Service Health, and the Defender and compliance portals."

I see nothing in this statement or anywhere around the Security Reader role in this article indicating they wouldn't be able to view incidents within that portal.

upvoted 1 times

 **Greatone1** 1 month, 3 weeks ago

<https://www.examtopics.com/discussions/microsoft/view/49358-exam-ms-101-topic-2-question-27-discussion/>

upvoted 3 times

 **Greatone1** 1 month, 4 weeks ago

**Selected Answer: A**

A is correct

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide>

upvoted 2 times

 **Casticod** 1 month, 4 weeks ago

**Selected Answer: C**

Only view security incident... Security reader.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-roles-permissions?view=o365-worldwide&tabs=M365Admin>

upvoted 1 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription.

All company-owned Windows 11 devices are onboarded to Microsoft Defender for Endpoint.

You need to configure Defender for Endpoint to meet the following requirements:

Block a vulnerable app until the app is updated.

Block an application executable based on a file hash.

The solution must minimize administrative effort.

What should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Block a vulnerable app until the app is updated:

- An allow or block file
- A file indicator
- A remediation request
- An update ring

Block an application executable based on a file hash:

- An allow or block file
- A file indicator
- A remediation request
- An update ring

**Answer Area**

Block a vulnerable app until the app is updated:

- An allow or block file
- A file indicator
- A remediation request**
- An update ring

Correct Answer:

Block an application executable based on a file hash:

- An allow or block file
- A file indicator**
- A remediation request
- An update ring

 spectre786 1 month, 1 week ago

First : Remediation Request

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/tvm-block-vuln-apps?view=o365-worldwide>

Second : File Indicator

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide>

upvoted 4 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.

Name	Operating system	Tag
Device1	Windows 10	Inventory1
Computer1	Windows 10	Inventory2
Device3	Android	Inventory3

Defender for Endpoint has the device groups shown in the following table.

Rank	Name	Matching rule
1	Group1	Tag Contains Inventory And OS in Android
2	Group2	Name Starts with Device And Tag Contains Inventory
Last	Ungrouped devices (default)	Not applicable

You create an incident email notification rule configured as shown in the following table.

Setting	Value
Name	Rule1
Alert severity	Low
Device group scope	Group1, Group2
Recipient email address	User1@contoso.com

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	<input type="radio"/>	<input type="radio"/>
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	<input type="radio"/>	<input type="radio"/>
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	<input type="radio"/>	<input type="radio"/>

**Answer Area****Statements**

Correct Answer:  
If a high-severity incident is triggered for Device1, an incident email notification will be sent.

 Yes No

If a low-severity incident is triggered for Computer1, an incident notification email will be sent.

 Yes No

If a low-severity incident is triggered for Device3, an incident notification email will be sent.

 Yes No

 amurp35 4 weeks, 1 day ago

Correct

upvoted 1 times

 nsotis28 1 month, 3 weeks ago

correct answer

upvoted 1 times

 Greatone1 1 month, 4 weeks ago

No - High severity Alert.

No - Doesn't have 'Device' in name

Yes - Has OS name Andriod and Tag contains 'Inventory'

upvoted 1 times

You have a Microsoft 365 tenant that contains two users named User1 and User2.

You create the alert policy shown in the following exhibit.

### Policy1

**Name your alert**

Description: Add a description Severity: Medium

Category: Information governance

**Create alert settings**

Conditions: Activity is FileChangeActivity Aggregation: Aggregated

Scope: All users Threshold: 5

Window: 1 hour

**Set your recipients**

Recipients: User1@sk220912.outlook.onmicrosoft.com Daily notification limit: 25

User2 runs a script that modifies a file in a Microsoft SharePoint library once every four minutes and runs for a period of two hours.

How many alerts will User1 receive?

- A. 2
- B. 5
- C. 10
- D. 25
- E. 30

#### Correct Answer: D

##### Community vote distribution

A (83%) D (17%)

**Jillis** Highly Voted 1 month ago

**Selected Answer: A**

I would say: A

"When multiple events that match the conditions of an alert policy occur with a short period of time, they are added to an existing alert by a process called alert aggregation. When an event triggers an alert, the alert is generated and displayed on the Alerts page and a notification is sent. If the same event occurs within the aggregation interval, then Microsoft 365 adds details about the new event to the existing alert instead of triggering a new alert. The goal of alert aggregation is to help reduce alert "fatigue" and let you focus and take action on fewer alerts for the same event."

<https://learn.microsoft.com/en-us/purview/alert-policies?view=o365-worldwide#alert-aggregation>

upvoted 5 times

**Jahanzeb88** 3 weeks, 3 days ago

so the aggregated threshold is 5, so shouldnt the answer be 5 as well?

upvoted 1 times

**gomezmax** Most Recent 5 days, 22 hours ago

I'm Sorry for My Wrong Answer, but it is A

upvoted 1 times

✉  **Greatone1** 2 weeks ago

2 is correct answer

<https://www.examtopics.com/discussions/microsoft/view/94370-exam-ms-101-topic-3-question-150-discussion/>

upvoted 2 times

✉  **santi32** 3 weeks, 3 days ago

**Selected Answer: D**

With the alert aggregation process:

The first 5 modifications will trigger the first alert. The next 10 modifications within that same hour will be aggregated to the existing alert, so no new alerts will be generated within the first hour.

In the second hour, the script again modifies the file 15 times. This means another alert will be generated after the first 5 modifications. The remaining 10 will again be aggregated to the same alert due to the 1-hour window.

Given this aggregation behavior, User1 will receive:

1 alert (from the first hour) + 1 alert (from the second hour) = 2 alerts in total.

So, you are correct. The answer is:

A. 2

upvoted 1 times

✉  **spectre786** 1 month, 1 week ago

Anyone got the right answer please ?

upvoted 1 times

✉  **nsotis28** 1 month, 3 weeks ago

picture is wrong

In any case key here is "aggregation"

<https://learn.microsoft.com/en-us/purview/alert-policies?view=o365-worldwide>

upvoted 1 times

✉  **spectre786** 1 month, 1 week ago

So right answer is A. 2 ?

upvoted 1 times

✉  **gomezmax** 1 month, 3 weeks ago

D Good 25

upvoted 2 times

Your company has 10,000 users who access all applications from an on-premises data center.

You plan to create a Microsoft 365 subscription and to migrate data to the cloud.

You plan to implement directory synchronization.

User accounts and group accounts must sync to Azure AD successfully.

You discover that several user accounts fail to sync to Azure AD.

You need to resolve the issue as quickly as possible.

What should you do?

- A. From Active Directory Administrative Center, search for all the users, and then modify the properties of the user accounts.
- B. Run idfix.exe, and then click Edit.
- C. From Windows PowerShell, run the start-AdSyncSyncCycle -PolicyType Delta command.
- D. Run idfix.exe, and then click Complete.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **Greatone1** 1 month, 4 weeks ago

**Selected Answer: B**

IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.

Reference:

<https://docs.microsoft.com/en-us/office365/enterprise/prepare-directory-attributes-for-synch-with-idfix>

upvoted 1 times

 **Casticod** 1 month, 4 weeks ago

**Selected Answer: B**

Correct It is necessary to modify the maximum threshold of modifications in each synchronization.

upvoted 1 times

**HOTSPOT -**

Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:

Contoso.com -

East.contoso.com -

The forest contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	East.contoso.com
User3	Fabrikam.com

The forest syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

**PROVISION FROM ACTIVE DIRECTORY****Azure AD Connect cloud provisioning**

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

**Azure AD Connect sync**

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Disabled

**USER SIGN-IN**

Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 can authenticate to Azure AD by using a username of user1@contoso.com.	<input type="radio"/>	<input type="radio"/>
User2 can authenticate to Azure AD by using a username of user2@contoso.com.	<input type="radio"/>	<input type="radio"/>
User3 can authenticate to Azure AD by using a username of user3@contoso.com.	<input type="radio"/>	<input type="radio"/>

**Answer Area**

Statements	Yes	No
User1 can authenticate to Azure AD by using a username of user1@contoso.com.	<input checked="" type="checkbox"/>	<input type="radio"/>
User2 can authenticate to Azure AD by using a username of user2@contoso.com.	<input type="radio"/>	<input checked="" type="checkbox"/>
User3 can authenticate to Azure AD by using a username of user3@contoso.com.	<input type="radio"/>	<input checked="" type="checkbox"/>

**Correct Answer:**

 **Greatone1**  1 month, 4 weeks ago

Box 1: Yes -

The UPN of user1 is user1@contoso.com so he can authenticate to Azure AD by using the username user1@contoso.com.

Box 2: No -

The UPN of user2 is user2@east.contoso.com so he cannot authenticate to Azure AD by using the username user2@contoso.com.

Box 3: No -

The UPN of user3 is user3@fabrikam.com so he cannot authenticate to Azure AD by using the username user3@contoso.com.

upvoted 5 times

 **rfree**  3 weeks, 2 days ago

Image shows Password Hash Sync is Disabled. Doesn't this mean NO passwords are synced, hence no one can log into Azure?

upvoted 1 times

 **BlindSentry** 3 weeks ago

Pass-through is enabled so the AD server authenticates the password

upvoted 1 times

**HOTSPOT -**

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2022	Domain controller
Server2	Windows Server 2016	Member server
Server3	Server Core installation of Windows Server 2022	Member server

You purchase a Microsoft 365 E5 subscription.

You need to implement Azure AD Connect cloud sync.

What should you install first and on which server? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Install:

The Azure AD Application Proxy connector

Azure AD Connect

The Azure AD Connect provisioning agent

Active Directory Federation Services (AD FS)

Server:

Server1 only

Server2 only

Server3 only

Server1 or Server2 only

Server1 or Server3 only

Server1, Server2, or Server3

**Answer Area**

Correct Answer:

Install:

The Azure AD Application Proxy connector

Azure AD Connect

**The Azure AD Connect provisioning agent**

Active Directory Federation Services (AD FS)

Server:

Server1 only

Server2 only

Server3 only

**Server1 or Server2 only**

Server1 or Server3 only

Server1, Server2, or Server3

 **letters1234** 1 month, 2 weeks ago

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/cloud-sync/how-to-prerequisites?tabs=public-cloud#in-your-on-premises-environment>

2016+ domain member server, server core not supported.

upvoted 2 times

 **certma2023** 2 months ago

Answer is correct.

You need to install a small agent on an On-Premises server. This server must run Windows Server 2016 ou later. Agent installation on DC is not supported. Agent installation on Windows Server Core is not supported.

upvoted 2 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Member of	Device
User1	Group1	Device1
User2	Group1	Device2, Device3

The devices are configured as shown in the following table.

Name	Platform	Azure AD join type
Device1	Windows 11	None
Device2	Windows 10	Joined
Device3	Android	Registered

You have a Conditional Access policy named CAPolicy1 that has the following settings:

Assignments -

Users or workload identities: Group1

Cloud apps or actions: Office 365 SharePoint Online

Conditions -

Filter for devices: Exclude filtered devices from the policy

Rule syntax: device.displayName -startsWith "Device"

Access controls -

Grant -

Grant: Block access -

Session: 0 controls selected -

Enable policy: On -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
User1 can access Site1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device2.	<input type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device3.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
Correct Answer: User1 can access Site1 from Device1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Site1 from Device2.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device3.	<input checked="" type="radio"/>	<input type="radio"/>

amurp35 Highly Voted 4 weeks ago

read the policy like this: "exclude from the block if the device starts with "device"". The first device is not registered. It is not, therefore, excluded from the block as it is not analyzed. It is blocked. The next two devices, however, are excluded from the block. N/Y/Y

upvoted 6 times

Paul\_white 1 week, 5 days ago

MY BROTHER YOU ARE TOO GOOD!!!! EXCELLENT RESPONSE

upvoted 1 times

ghjbhj 3 weeks, 4 days ago

Correct, <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-condition-filters-for-devices#policy-behavior-with-filter-for-devices>

Unregistered device + positive operators = filter not applied

If the filter does not apply, the device is not excepted from the block policy and is therefore blocked. N/Y/Y

upvoted 1 times

hogehogehoge Most Recent 1 month, 3 weeks ago

This answer is correct. Device1 is not registered in Azure AD. In this case, Device filter is not enabled. So Device1 is blocked.

upvoted 1 times

spectre786 1 month, 1 week ago

I think the policy is there to Block Access not to allow. So whoever is targeted by this policy, should be blocked. So the answer should be Y/N/N, right?

upvoted 6 times

PhoenixMan 1 month ago

Yes I think the same, the policy blocks access and the answer should be Y/N/N

upvoted 2 times

You have a Microsoft 365 E5 subscription.

Conditional Access is configured to block high-risk sign-ins for all users.

All users are in France and are registered for multi-factor authentication (MFA).

Users in the media department will travel to various countries during the next month.

You need to ensure that if the media department users are blocked from signing in while traveling, the users can remediate the issue without administrator intervention.

What should you configure?

- A. an exclusion group
- B. the MFA registration policy
- C. named locations
- D. self-service password reset (SSPR)

**Correct Answer: D**

*Community vote distribution*

D (91%) 9%

✉️  **letters1234**  1 month, 2 weeks ago

**Selected Answer: D**

A & B - Are excluding users from MFA, which is not a secure method of managing users and the risk to their accounts.  
C - Named locations requires IP ranges, how do you know each Wi-Fi/network range the reps will visit? Wouldn't trust ChatGPT as far as I could throw it.  
D - You can allow users to self-remediate their sign-in risks and user risks by setting up risk-based policies. If users pass the required access control, such as Azure AD Multifactor Authentication or secure password change, then their risks are automatically remediated.  
<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock#self-remediation-with-risk-based-policy>

upvoted 8 times

✉️  **Shloeb** 2 weeks, 1 day ago

Named locations makes sense as now there is an option to choose the location based on country. You do not need to specify the IP ranges anymore. Have a look:  
<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#countriesregions>

upvoted 1 times

✉️  **amurp35** 4 weeks ago

You are thinking of user-risk, which gets remediated through SSPR.

upvoted 1 times

✉️  **santi32**  3 weeks, 3 days ago

**Selected Answer: D**

D. self-service password reset (SSPR)

SSPR allows users to reset their passwords on their own without needing administrative intervention. In conjunction with Azure AD Identity Protection, when users have a risky sign-in, they can be prompted to perform a password reset as a remediation action. This combination ensures that even if a sign-in is considered high-risk, the user can validate their identity and reset their password to regain access.

upvoted 2 times

✉️  **amurp35** 4 weeks ago

**Selected Answer: B**

This would be classified as a sign-in risk rather than a user-risk. Therefore, MFA self-remediates the risk. The question states that folks in France are registered for MFA, not the media department. The MFA registration policy needs checked, because MFA is what self-remediates the sign-in risk:  
<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies#sign-in-risk-based-conditional-access-policy>

Therefore, the correct answer is actually B. Stop trusting ChatGPT and other non-primary sources.

upvoted 1 times

✉️  **ghjbhj** 3 weeks, 4 days ago

I agree that sign-in risk is remediated by MFA, but re-reading the question shows that all users are in France, and all have MFA. If all users are already registered for MFA, what can be changed in the MFA policy to allow self-remediate?

B is most likely the answer but can't find the justification

upvoted 1 times

 **gomezmax** 1 month, 2 weeks ago

The Answer Is C  
upvoted 1 times

 **DiligentSam** 1 month, 3 weeks ago

C.named locations. This answer from ChatGPT  
By configuring named locations in Conditional Access, you can define trusted locations where users can sign in without being subject to the same level of risk assessment as other locations. This will allow the media department users to sign in from their travel locations without being blocked, as long as they are still using MFA. Additionally, if they are blocked, they can remediate the issue themselves by verifying their identity through MFA. This can be done without administrator intervention, using self-service password reset (SSPR) or other MFA verification methods.

upvoted 1 times

 **amurp35** 4 weeks ago

Why do people supply 'answers' from ChatGPT? It makes things up, literally.  
upvoted 1 times

 **amurp35** 4 weeks ago

Also, you actually quoted the correct answer even though you chose the wrong one. See your comment "Additionally, if they are blocked, they can remediate the issue themselves by verifying their identity through MFA". Think, why would you add whole countries as named locations?  
That defeats the purpose of MFA.  
upvoted 1 times

 **Ranger\_DanMT** 1 month, 3 weeks ago

nevermind answer is correct <https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock#:~:text=If%20a%20user%20has%20registered,a%20self%2Dservice%20password%20reset>.  
upvoted 2 times

 **Ranger\_DanMT** 1 month, 3 weeks ago

Pretty sure the answer to this would be B?  
upvoted 1 times

You have a Microsoft 365 E5 subscription that contains the following user:

Name: User1 -

UPN: user1@contoso.com -

Email address: user1@marketmg.contoso.com

MFA enrollment status: Disabled -

When User1 attempts to sign in to Outlook on the web by using the user1@marketing.contoso.com email address, the user cannot sign in.

You need to ensure that User1 can sign in to Outlook on the web by using user1@marketing.contoso.com.

What should you do?

- A. Assign an MFA registration policy to User1.
- B. Reset the password of User1.
- C. Add an alternate email address for User1.
- D. Modify the UPN of User1.

**Correct Answer: D**

*Community vote distribution*

D (60%) C (40%)

✉️  **jt2214** 3 days, 11 hours ago

**Selected Answer: D**

I agree with Milad  
upvoted 1 times

✉️  **MZeeshanTayyab** 1 week, 2 days ago

**Selected Answer: D**

D is right  
upvoted 2 times

✉️  **Paul\_white** 2 weeks, 1 day ago

ANSWER IS D  
upvoted 3 times

✉️  **darcone23** 2 weeks, 2 days ago

**Selected Answer: C**

User1 is using the the "user1@marketing.contoso.com" when signing into OWA which is not their correct email - "user1@marketmg.contoso.com". "user1@marketing.contoso.com" should be added as an alternate email address to the user and then it can be used for login: "You can choose which email address to send mail from, and you can sign in to your Outlook.com account with any of your aliases—they all use the same password."

<https://support.microsoft.com/en-us/office/add-or-remove-an-email-alias-in-outlook-com-459b1989-356d-40fa-a689-8f285b13f1f2>  
upvoted 2 times

✉️  **Milad666** 1 week, 3 days ago

Bro ! at least test it to your test environment then comment it in below! you can NOT login with Email Address. you Could ONLY Login with your UPN! So answer is D.

This behavior applies not only to Office365, but also to Active Directory Local Exchange and all LDAP-based authentications that exist!  
upvoted 2 times

✉️  **spectre786** 1 month, 1 week ago

I think it's D. Modify the UPN  
upvoted 2 times

**HOTSPOT -**

Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2
Group2	Security Group - Global	OU2

The groups have the members shown in the following table.

Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.

You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)

The screenshot shows the 'Domain and OU filtering' configuration page in the Microsoft Azure Active Directory Connect interface. The left sidebar lists various tabs: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, Connect Directories, Azure AD sign-in, Domain/OU Filtering (which is selected and highlighted in blue), Identifying users, Filtering, Optional Features, and Configure. The main content area has a title 'Domain and OU filtering'. It includes a 'Directory:' dropdown set to 'fabrikam.com', a 'Refresh Ou/Domain' button, and a help (?) icon. Below these are two radio buttons: 'Sync all domains and OUs' (unchecked) and 'Sync selected domains and OUs' (checked). A tree view shows the domain structure under 'fabrikam.com': Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, Infrastructure, LostAndFound, Managed Service Accounts, OU1, OU2 (with a checked checkbox), Program Data, System, and Users. At the bottom are 'Previous' and 'Next' navigation buttons.

You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering tab.)

 Microsoft Azure Active Directory Connect

Welcome  
Express Settings  
Required Components  
User Sign-In  
Connect to Azure AD  
Sync  
Connect Directories  
Azure AD sign-in  
Domain/OU Filtering  
Identifying users  
**Filtering**  
Optional Features  
Configure

## Filter users and devices

For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.

Synchronize all users and devices  
 Synchronize selected [?](#)

FOREST	GROUP
fabrikam.com	<input type="text" value="CN=Group2,OU=OU2,DC=fabrikam,DC=com"/> <a href="#">Resolve</a> 

[Previous](#) [Next](#)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

#### Answer Area

Statements	Yes	No
User2 will synchronize to Azure AD.	<input type="radio"/>	<input type="radio"/>
Group2 will synchronize to Azure AD.	<input type="radio"/>	<input type="radio"/>
User3 will synchronize to Azure AD.	<input type="radio"/>	<input type="radio"/>

#### Answer Area

Statements	Yes	No
User2 will synchronize to Azure AD.	<input type="radio"/>	<input checked="" type="radio"/>
Group2 will synchronize to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User3 will synchronize to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>

  amurp35 4 weeks ago

Answers are correct. The filtered group's members are only synced if they also reside in an OU that is also chosen to be synced by the directory options prior.

upvoted 2 times

  nsotis28 1 month, 3 weeks ago

Answers are correct

upvoted 1 times

 **Greatone1** 1 month, 3 weeks ago

Answers are correct

User 2 is not synced because it's not in an OU that is synced.

User 3 is synced because it is in both a synced OU and Group.

upvoted 3 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription.

From Azure AD Identity Protection on August 1, you configure a Multifactor authentication registration policy that has the following settings:

Assignments: All users -

Controls: Require Azure AD multifactor authentication registration

Enforce Policy: On -

On August 3, you create two users named User1 and User2.

Users authenticate by using Azure Multi-Factor Authentication (MFA) for the first time on the dates shown in the following table.

User	Date
User1	August 5
User2	August 7

By which dates will User1 and User2 be forced to complete their Azure MFA registration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User1:

- August 6
- August 17
- August 19
- September 3
- September 5

User2:

- August 8
- August 17
- August 19
- August 21
- September 7

**Answer Area**

User1:

- August 6
- August 17
- August 19**
- September 3
- September 5

Correct Answer:

User2:

- August 8
- August 17
- August 19**
- August 21**
- September 7

  flim322 1 month, 2 weeks ago

Answers are corrected.

"Azure AD Identity Protection will prompt your users to register the next time they sign in interactively and they'll have 14 days to complete registration."

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy>

upvoted 3 times

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 subscription.

You need to sync the domain with the subscription. The solution must meet the following requirements:

On-premises Active Directory password complexity policies must be enforced.

Users must be able to use self-service password reset (SSPR) in Azure AD.

What should you use?

- A. password hash synchronization
- B. Azure AD Identity Protection
- C. Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
- D. pass-through authentication

**Correct Answer: D**

*Community vote distribution*

D (100%)

✉️  **letters1234** 1 month, 2 weeks ago

**Selected Answer: D**

Password hash sync just does comparison of password hash. Passthrough respects the DC and doesn't approve the ticket itself.  
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback>

upvoted 1 times

✉️  **Casticod** 1 month, 3 weeks ago

**Selected Answer: D**

Azure Active Directory (Azure AD) self-service password reset (SSPR) lets users reset their passwords in the cloud, but most companies also have an on-premises Active Directory Domain Services (AD DS) environment for users. Password writeback allows password changes in the cloud to be written back to an on-premises directory in real time <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback>

upvoted 1 times

✉️  **Casticod** 1 month, 3 weeks ago

Password writeback is supported in environments that use the following hybrid identity models:

Password hash synchronization  
Pass-through authentication  
Active Directory Federation Services  
D or A??

upvoted 3 times

✉️  **Ranger\_DanMT** 1 month, 3 weeks ago

answer is correct, SSPR works for both Pass-thru and hash sync. The key here is that on-prem password policies need enforced.  
<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta>

upvoted 3 times

✉️  **Greatone1** 1 month, 3 weeks ago

**Selected Answer: D**

Correct answer should be D

Source : <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#:~:text=is%20using%20federated%2C-,pass,-%2Dthrough%20authentication%2C%20or>  
upvoted 1 times

✉️  **hogehogehoge** 1 month, 3 weeks ago

I think A is correct. Because Users must use SSPR in AzureAD.

upvoted 1 times

You have a Microsoft 365 E5 subscription.

Users access Microsoft 365 from both their laptop and a corporate Virtual Desktop Infrastructure (VDI) solution.

From Azure AD Identity Protection, you enable a sign-in risk policy.

Users report that when they use the VDI solution, they are regularly blocked when they attempt to access Microsoft 365.

What should you configure?

- A. the Tenant restrictions settings in Azure AD
- B. a trusted location
- C. a Conditional Access policy exclusion
- D. the Microsoft 365 network connectivity settings

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **Paul\_white** 2 weeks, 2 days ago

CORRECT ANSWER SHOULD BE C

upvoted 1 times

 **Paul\_white** 1 week, 5 days ago

NEVER MIND, ITS B. A TRUSTED LOCATION

upvoted 1 times

 **sherifhamed** 2 weeks, 5 days ago

**Selected Answer: B**

B. a trusted location

By configuring a trusted location, you can exempt the VDI solution from the risk policy's scrutiny. This way, users accessing Microsoft 365 through the VDI solution won't trigger the risk policy and won't be regularly blocked when using it.

upvoted 2 times

 **certma2023** 2 months ago

**Selected Answer: B**

Answer B.

Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives.

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>

upvoted 2 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription that contains a user named User1. Azure AD Password Protection is configured as shown in the following exhibit.

**Custom smart lockout**

Lockout threshold ⓘ

15



Lockout duration in seconds ⓘ

600

**Custom banned passwords**

Enforce custom list ⓘ

Yes

No

Custom banned password list ⓘ

3hundred  
Eleven  
Falcon  
Project  
Tailspin

**Password protection for Windows Server Active Directory**

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

Enforced

Audit

User1 attempts to update their password to the following passwords:

F@lcon -

Project22 -

T4il\$pin45dg4 -

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.  
NOTE: Each correct selection is worth one point.

**Answer Area**

[Answer choice] will be accepted as a password.

▼  
Only T4il\$pin45dg4  
Only F@lcon and T4il\$pin45dg4  
Only Project22 and T4il\$pin45dg4  
F@lcon, Project22, and T4il\$pin45dg4

▼  
will be locked out  
will trigger a user risk  
can attempt to sign in again immediately

If User1 enters the same wrong password 15 times, waits 11 minutes, and then enters the same wrong password again, the user [answer choice].

## Answer Area

[Answer choice] will be accepted as a password.

Only T4il\$pin45dg4  
Only F@lcon and T4il\$pin45dg4  
Only Project22 and T4il\$pin45dg4  
F@lcon, Project22, and T4il\$pin45dg4

will be locked out  
will trigger a user risk  
can attempt to sign in again immediately

### Correct Answer:

If User1 enters the same wrong password 15 times, waits 11 minutes, and then enters the same wrong password again, the user [answer choice].

ExamCheater1993 3 weeks, 5 days ago

Picture is correct. The trap is, that this persons enters the SAME password multiple times. This doesn't count to the lockout policy because of smart lock out .

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout>

upvoted 4 times

SandyBridge 3 weeks, 1 day ago

"Smart lockout tracks the last three bad password hashes to avoid incrementing the lockout counter for the same password. If someone enters the same bad password multiple times, this behavior doesn't cause the account to lock out."

From source: <https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout>

upvoted 1 times

amurp35 4 weeks ago

Box 1 - T4il\$pin45dg4

- Each banned password that's found in a user's password is given one point.
- Each remaining character that is not part of a banned password is given one point.
- A password must be at least five (5) points to be accepted.

Box 2 is incorrect

The account locks again after each subsequent failed sign-in attempt, for one minute at first and longer in subsequent attempts.

upvoted 2 times

vercracked\_007 1 month ago

Box 1 - T4il\$pin45dg4

Box 2 will be locked out again

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout>

upvoted 4 times

EM1234 2 weeks, 3 days ago

That link you provided explains how you can change the password protection defaults. Which, I believe, is the point of this question. I think provided answers are correct.

upvoted 1 times

gomezmax 1 month, 1 week ago

1 Box Correct T4il\$pin45dg4

The 2nd Box is incorrect it should be lockout

upvoted 1 times

letters1234 1 month, 2 weeks ago

Answers are correct

Only T4il\$pin45dg4 will be allowed to change, the other two have an exact or within 1 character match to the banned passwords:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#fuzzy-matching-behavior>

Lockout period is 10 minutes (600 seconds) meaning on the 11th minute, the count starts again from 1 and would need another 15 bad passwords within the next 9 minutes to lock the user out.

upvoted 4 times

nsotis28 1 month, 3 weeks ago

Box 1 - only T4il\$pin45dg4

Box 2 - will be locked

upvoted 1 times

hogehogehoge 1 month, 3 weeks ago

Box1:Only F@lcon and T4il\$pin45dg4.

Because "a" is replaced "@", and match this policy.

upvoted 1 times

Romke\_en\_Tomke 4 weeks, 1 day ago

You made me look it up. You are wrong, box 1 is correct. An "a" as @ is considered as a common character substitution.  
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection#configure-custom-banned-passwords>

upvoted 2 times

✉️  **Vaati** 2 months ago

If you fail again after a lockout periode, you are locked again no?

upvoted 2 times

✉️  **spectre786** 1 month, 1 week ago

exactly

upvoted 1 times

You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

Name	Source	Last sign in
User1	Azure AD	Yesterday
User2	Active Directory Domain Services (AD DS)	Two days ago
User3	Active Directory Domain Services (AD DS)	Never

Azure AD Connect has the following settings:

Password Hash Sync: Enabled -

Pass-through authentication: Enabled

You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the internet is lost.

Which users should you identify?

- A. none
- B. User1 only
- C. User1 and User2 only
- D. User1, User2, and User3

**Correct Answer: D**

*Community vote distribution*

B (64%) A (36%)

 MoreCertificatesForMe 1 week, 6 days ago

**Selected Answer: B**

Hash Sync syncs every 2 min, so if on prem communication is down i would not think that the authentication will happen upvoted 1 times

 amurp35 4 weeks ago

**Selected Answer: B**

B. Cloud user won't be affected. Why? Because Pass-through auth is ON for the on-prem soured users. Password Hash Sync is not an auto-fallback kind of a thing. Therefore, those users cannot authenticate without some work on the configuration to enable it, since the authentication happens on-prem.

upvoted 2 times

 AMDf 1 month, 1 week ago

**Selected Answer: B**

Vote for B

upvoted 2 times

 ae88d96 1 month, 1 week ago

**Selected Answer: B**

Correct Answer B, Cloud User won't be affected. Tested on my lab.

upvoted 2 times

 Carine 1 month, 2 weeks ago

User1 is a cloud only user, no ? So i think he will be able to authenticate by Azure AD. So B for me.

upvoted 1 times

 gomezmax 1 month, 3 weeks ago

it Should be A

upvoted 1 times

 Greatone1 1 month, 3 weeks ago

**Selected Answer: A**

A is correct answer

Fail over to password hash synchronization doesn't happen automatically and you must use Azure AD Connect to switch the sign-on method manually.

upvoted 1 times

 **nsotis28** 1 month, 3 weeks ago

For sure A  
certman2023 has shared explanation  
upvoted 1 times

 **certma2023** 2 months ago

**Selected Answer: A**

I would choose A.

According to the MS documentation:

"Does password hash synchronization act as a fallback to Pass-through Authentication?  
No. Pass-through Authentication does not automatically failover to password hash synchronization. To avoid user sign-in failures, you should configure Pass-through Authentication for high availability."  
<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-faq#does-password-hash-synchronization-act-as-a-fallback-to-pass-through-authentication->

Therefore, without any admin actions, authentication won't be possible for any user until the admin make some changes on the tenant.

upvoted 3 times

 **amurp35** 4 weeks ago

Correct, except for cloud-only users. Therefore, the correct answer is B.

upvoted 2 times

Your network contains an on-premises Active Directory domain named contoso.com.

For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours.

You plan to sync contoso.com to an Azure AD tenant

You need to recommend a solution to ensure that the logon hour restrictions apply when synced users sign in to Azure AD.

What should you include in the recommendation?

- A. pass-through authentication
- B. conditional access policies
- C. password synchronization
- D. Azure AD Identity Protection policies

**Correct Answer: A**

*Community vote distribution*

A (75%)      B (25%)

 **Casticod** Highly Voted 1 month, 4 weeks ago

**Selected Answer: A**

This requirement can be achieved only if you have Pass through Authentication configured as a sign in option with Azure AD and with Logon hours setting configured in on-premise AD.

Other solution it's PIM but not valid in that question

upvoted 5 times

 **Alscoran** Most Recent 3 days, 20 hours ago

**Selected Answer: A**

From: <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/plan-connect-user-signin>

"Pass-through authentication

With pass-through authentication, the user's password is validated against the on-premises Active Directory controller. The password doesn't need to be present in Microsoft Entra ID in any form. This allows for on-premises policies, such as sign-in hour restrictions, to be evaluated during authentication to cloud services."

upvoted 1 times

 **santi32** 3 weeks, 3 days ago

**Selected Answer: B**

Pass-through authentication (A) simply validates on-premises passwords without enforcing on-premises policies like logon hours. Password synchronization

Conditional access policies in Azure AD allow you to set conditions on when and how users can access Azure AD resources. While Azure AD doesn't directly support the "Logon Hours" feature of on-premises Active Directory, you can set up a conditional access policy to block or allow access based on time and other conditions, effectively replicating the restrictions in Azure AD.

upvoted 2 times

 **Lovell88** 1 day, 7 hours ago

There is no time condition in CA. This isn't correct. Don't trust this answer.

upvoted 1 times

 **DiligentSam** 1 month, 3 weeks ago

Conditional access policies. From ChatGPT

You should recommend using conditional access policies in Azure AD to enforce logon hour restrictions for synced users. Conditional access policies allow you to define access rules based on various conditions, including time of day. By creating a conditional access policy that requires users to sign in during business hours, you can ensure that logon hour restrictions are enforced for synced users in Azure AD.

upvoted 2 times

 **RJTW070** 1 month ago

My first thought was conditional access this confirmed this. I also checked this via AI and it is the same.

upvoted 1 times

 **Greatone1** 2 months ago

I was wrong given answer is correct

upvoted 1 times

 **Greatone1** 2 months ago

I believe answer is b conditional access

upvoted 2 times

Your network contains three Active Directory forests. There are forests trust relationships between the forests.

You create an Azure AD tenant.

You plan to sync the on-premises Active Directory to Azure AD.

You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails.

What should you include in the recommendation?

- A. one Azure AD Connect sync server and one Azure AD Connect sync server in staging mode
- B. three Azure AD Connect sync servers and one Azure AD Connect sync server in staging mode
- C. six Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode
- D. three Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

**Correct Answer:** A

 **nsotis28** 1 month, 3 weeks ago

A

AD connect supports only one instance of Azure AD Connect syncing to Azure AD. You can add directories during configuration  
<https://learn.microsoft.com/en-us/skypeforbusiness/hybrid/cloud-consolidation-aad-connect>

upvoted 2 times

You have a Microsoft 365 subscription.

You have the retention policies shown in the following table.

Name	Location	Retain items for a specific period	Start the retention period based on	At the end of the retention period
Policy1	SharePoint sites	1 years	When items were created	Delete items automatically
Policy2	SharePoint sites	2 years	When items were last modified	Do nothing

Both policies are applied to a Microsoft SharePoint site named Site1 that contains a file named File1.docx.

File1.docx was created on January 1, 2022 and last modified on January 31, 2022. The file was NOT modified again.

When will File1.docx be deleted automatically?

- A. January 1, 2023
- B. January 1, 2024
- C. January 31, 2023
- D. January 31, 2024
- E. never

**Correct Answer: D**

*Community vote distribution*

D (69%) E (31%)

 **Alscoran** 6 days, 16 hours ago

**Selected Answer: D**

Gbartumeu provides the perfect example. Just look at his article and do a find for "suspended". Second hit.  
upvoted 2 times

 **ZZNZ** 2 weeks, 3 days ago

**Selected Answer: E**

E is correct answer: Retention wins over deletion  
upvoted 1 times

 **DiligentSam** 1 week, 1 day ago

Example: At Contoso, an email message is subject to a retention policy for Exchange. A Contoso administrator configured the policy to delete items three years after creation. It also has a retention label applied that retains items five years after creation.

Outcome: The system retains the email message for five years because this retention action takes precedence over the deletion action. As a result, the system permanently deletes the email message at the end of the five years because of the delete action the system suspended while the retention action was in effect.

upvoted 1 times

 **BlindSentry** 2 weeks ago

Answer is D.

Retention wins over deletion for the period of two years then the deletion would take over after the two years.

<https://learn.microsoft.com/en-us/training/modules/explore-retention-policies-labels-microsoft-365/5-examine-principles-retention>  
upvoted 3 times

 **Blagojche** 2 weeks, 3 days ago

Correct Answer is E

Given the retention policies:

Policy 1: Retains items for 1 year based on when they were created, and then deletes them automatically.

Policy 2: Retains items for 2 years based on when they were last modified, and then does nothing.

The file File1.docx was created on January 1, 2022, and last modified on January 31, 2022.

According to Policy 1, the file would be deleted one year after its creation date, which would be January 1, 2023. However, Policy 2 retains the file for two years after its last modification date, which would be January 31, 2024.

Since Policy 2 has a longer retention period and it is set to "Do Nothing" at the end of the retention period, the deletion action from Policy 1 will

not take place. Therefore, File1.docx will not be deleted automatically.

So, the correct answer is E. never.

upvoted 1 times

smiff 3 weeks ago

**Selected Answer: E**

rules

retention takes precedence over deletion

longest retention wins

do nothing means that the file will remain as is until the user delete it (no retention policy applied)

upvoted 1 times

amurp35 4 weeks ago

**Selected Answer: D**

D is correct. Source: <https://learn.microsoft.com/en-us/purview/retention?tabs=table-overridden#the-principles-of-retention-or-what-takes-precedence>

quote: "Example for this first principle: An email message is subject to a retention policy for Exchange that is configured to delete items three years after they are created, and it also has a retention label applied that is configured to retain items five years after they are created."

The email message is retained for five years because this retention action takes precedence over deletion. The email message is permanently deleted at the end of the five years because of the delete action that was suspended while the retention action was in effect.

upvoted 2 times

gbartumeu 1 month ago

**Selected Answer: D**

An example from Microsoft explains it very clear:

An email message is subject to a retention policy for Exchange that is configured to delete items three years after they are created, and it also has a retention label applied that is configured to retain items five years after they are created.

The email message is retained for five years because this retention action takes precedence over deletion. The email message is permanently deleted at the end of the five years because of the delete action that was suspended while the retention action was in effect.

Soruce: <https://learn.microsoft.com/en-us/purview/retention?tabs=table-removed>

upvoted 2 times

vercracked\_007 1 month ago

E - Retention wins over deletion

<https://learn.microsoft.com/en-us/purview/retention?tabs=table-overridden#the-principles-of-retention-or-what-takes-precedence>

upvoted 1 times

letters1234 1 month, 2 weeks ago

**Selected Answer: E**

<https://learn.microsoft.com/en-us/purview/retention?tabs=table-overridden#the-principles-of-retention-or-what-takes-precedence>

"At a high level, you can be assured that retention always takes precedence over permanent deletion, and the longest retention period wins. These two simple rules always decide how long an item will be retained."

Possibly E due to the "at end of retention" setting being no action, i.e., retain. Unless the polices change, it would not be deleted.

upvoted 2 times

hogehogehoge 1 month, 4 weeks ago

**Selected Answer: D**

I think D is correct. Please check this URL. <https://learn.microsoft.com/en-us/purview/retention?tabs=table-overridden>

upvoted 3 times

Vaati 2 months ago

Could someone explain? im thinking E

upvoted 1 times

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

You plan to publish a sensitivity label named Label1.

To which groups can you publish Label1?

- A. Group1 only
- B. Group1 and Group2 only
- C. Group1 and Group4 only
- D. Group1, Group2, and Group3 only
- E. Group1, Group2, Group3, and Group4

**Correct Answer: A**

*Community vote distribution*

D (86%) 14%

✉️  **amurp35** Highly Voted 4 weeks ago

**Selected Answer: D**

The correct answer is D. You can apply sensitivity labels to Microsoft 365 Groups, SharePoint sites, Distribution Groups, and Mail-enabled Security Groups but not regular Security Groups.

<https://learn.microsoft.com/en-us/purview/sensitivity-labels#what-label-policies-can-do>  
upvoted 6 times

✉️  **mhmyz** Most Recent 3 weeks, 4 days ago

**Selected Answer: E**

The correct answer is E.

"When you configure a label policy, you can:

Choose which users and groups see the labels. Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD."

<https://learn.microsoft.com/en-us/purview/sensitivity-labels>

upvoted 1 times

✉️  **RJTW070** 1 month ago

According to the Microsoft Learn article Assign sensitivity labels to groups, you can publish sensitivity labels to groups that are either security groups or Microsoft 365 groups. Therefore, you can publish Label1 to the following groups in your subscription:

You cannot publish Label1 to a distribution group, which is not supported for sensitivity labels.

upvoted 1 times

✉️  **rfree** 1 month ago

This site explicitly says to meet this Condition "The group is a Microsoft 365 group."

[https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-assign-sensitivity-labels?WT.mc\\_id=Portal-Microsoft\\_AAD\\_IAM](https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-assign-sensitivity-labels?WT.mc_id=Portal-Microsoft_AAD_IAM)  
The "Group writeback state" oddly includes options Security, Mail Enabled Security and Distribution.

upvoted 1 times

✉️  **spectre786** 1 month, 2 weeks ago

Correct : D

You can publish labels to users but only to groups that have email addresses (Distribution groups, Microsoft 365 groups, and mail-enabled security groups). You can't publish a label to a security group. The group can have assigned or dynamic membership.

upvoted 2 times

✉️  **gomezmax** 1 month, 3 weeks ago

(A) it is Correct only applied into the Email

upvoted 1 times

✉️  **gomezmax** 1 month, 3 weeks ago

Correct

upvoted 1 times

 **Greatone1** 2 months ago

Correct answer is D

upvoted 1 times

 **certma2023** 2 months ago

Answer D.

According to the documentation:

"Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD."

<https://learn.microsoft.com/en-us/purview/sensitivity-labels>

upvoted 1 times

**HOTSPOT -**

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

Name	Priority	Action
Rule1	0	Notify users by using email and policy tips. Customize the policy tip as Rule1 tip. Disable user overrides.
Rule2	1	Notify users by using email and policy tips. Customize the policy tip as Rule2 tip. Restrict access to the content. Disable user overrides.
Rule3	2	Notify users by using email and policy tips. Customize the policy tip as Rule3 tip. Restrict access to the content. Enable user overrides.
Rule4	3	Notify users by using email and policy tips. Customize the policy tip as Rule4 tip. Restrict access to the content. Disable user overrides.

Site1 contains the files shown in the following table.

Name	Matched DLP rule
File1.docx	Rule1, Rule2, Rule3
File2.docx	Rule1, Rule3, Rule4

Which policy tips are shown for each file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

File1.docx:

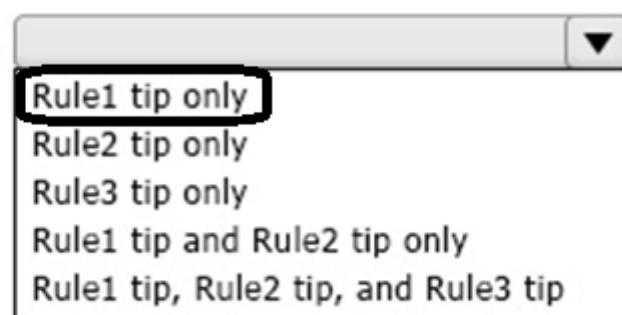
Rule1 tip only  
 Rule2 tip only  
 Rule3 tip only  
 Rule1 tip and Rule2 tip only  
 Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

Rule1 tip only  
 Rule3 tip only  
 Rule4 tip only  
 Rule1 tip and Rule4 tip only  
 Rule1 tip, Rule3 tip, and Rule4 tip

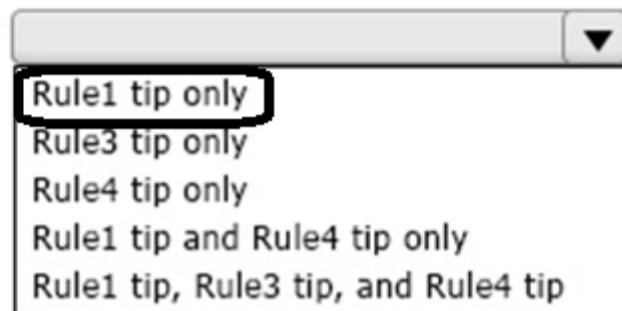
## Answer Area

File1.docx:



Correct Answer:

File2.docx:



✉ **hogehogehoge** Highly Voted 1 month, 4 weeks ago

File1.docx:rule2 only. And File2.docx:rule4 only.

When content is evaluated against rules, the rules are processed in priority order. If content matches multiple rules, the first rule evaluated that has the most restrictive action is enforced. For example, if content matches all of the following rules, Rule 3 is enforced because it's the highest priority, most restrictive rule:

<https://learn.microsoft.com/en-us/purview/dlp-policy-reference>

upvoted 14 times

✉ **rfree** Most Recent 3 weeks ago

As its not asking which rules are applied, but which rules are Shown.

upvoted 1 times

✉ **rfree** 3 weeks ago

Great catch Hoge3x, but the very next paragraph states "Rules 1, 2, and 4 would be evaluated, but not applied. In this example, matches for all of the rules are recorded in the audit logs and shown in the DLP reports, even though only the most restrictive rule is applied." So reading the question again "Which tips are SHOWN", I believe its all for each.

File1 rule 1,2 and 3. File 2 rule 1,3 and 4

upvoted 3 times

✉ **amurp35** 4 weeks ago

Agree with hoge

upvoted 1 times

✉ **letters1234** 1 month, 2 weeks ago

Agree with Hoge, specific reference in the doc:

<https://learn.microsoft.com/en-us/purview/dlp-policy-reference#the-priority-by-which-rules-are-evaluated-and-applied>

upvoted 4 times

✉ **Greatone1** 2 months ago

Rule 1 Tip Only" for both

upvoted 1 times

You have a Microsoft 365 subscription.  
You configure a data loss prevention (DLP) policy.  
You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.  
You need to prevent the users from bypassing the DLP policy.  
What should you configure?

- A. actions
- B. incident reports
- C. exceptions
- D. user overrides

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **Greatone1** 1 month, 4 weeks ago

**Selected Answer: D**

Explanation:

A DLP policy can be configured to allow users to override a policy tip and report a false positive.

upvoted 4 times

You have a Microsoft 365 E5 tenant.

You create a retention label named Retention1 as shown in the following exhibit.

## Create retention label

**Review and finish**

**Name**  
Name  
6Months  
[Edit](#)

**Retention settings**

<b>Retention period</b> 6 months <a href="#">Edit</a>	<b>Retention action</b> Retain and Delete <a href="#">Edit</a>
---	--

**Based on**  
Based on when it was created  
[Edit](#)

[?](#) [Feedback](#)

[Back](#) [Create label](#) [Cancel](#)

When users attempt to apply Retention1, the label is unavailable.

You need to ensure that Retention1 is available to all the users.

What should you do?

- Create a new label policy.
- Modify the Authority type setting for Retention1.
- Modify the Business function/department setting for Retention1.
- Use a file plan CSV template to import Retention1.

**Correct Answer: A**

*Community vote distribution*

A (100%)

**ZZNZ** 2 weeks, 3 days ago

**Selected Answer: A**

wrong image : <https://www.examtopics.com/discussions/microsoft/view/65184-exam-ms-101-topic-3-question-105-discussion/>  
upvoted 2 times

**spectre786** 1 month, 2 weeks ago

Can someone explain why it first says that the retention label is named Retention1 then on the image we can see that the name is 6Months ? Is it the wrong picture ?

upvoted 1 times

**letters1234** 1 month, 2 weeks ago

From Greatone1's link:

Making retention labels available to people in your organization so that they can classify content is a two-step process:

- Create the retention labels.
- Publish the retention labels by using a retention label policy.

upvoted 1 times

**Greatone1** 1 month, 4 weeks ago

**Selected Answer: A**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide>

upvoted 1 times

You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.

[Home](#) > [sensitivity](#)

[Labels](#) [Label policies](#) [Auto-labeling \(preview\)](#)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

<a href="#">+ Create a label</a> <a href="#">Publish labels</a> <a href="#">Refresh</a>				
Name ↑	Order	Created by	Last modified	
Label1	... 0 - highest	Prvi	04/24/2020	
— Label2	... 1	Prvi	04/24/2020	
Label3	... 0 - highest	Prvi	04/24/2020	
Label4	... 0 - highest	Prvi	04/24/2020	
— Label5	... 5	Prvi	04/24/2020	
Label6	0 - highest	Prvi	04/24/2020	

Which labels can users apply to content?

- A. Label1, Label2, and Label5 only
- B. Label3, Label4, and Label6 only
- C. Label1, Label3, Label4, and Label6 only
- D. Label1, Label2, Label3, Label4, Label5, and Label6

**Correct Answer:** D

*Community vote distribution*

C (100%)

 **amurp35** 4 weeks ago

**Selected Answer: C**

correct answer is C. The parent label becomes a container and cannot be assigned by a user, rather the user must choose the child label.  
upvoted 1 times

 **letters1234** 1 month, 2 weeks ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/purview/sensitivity-labels#sublabels-grouping-labels>  
upvoted 2 times

 **gomezmax** 1 month, 3 weeks ago

Should be C. Label1, Label3, Label4, and Label6 only  
upvoted 1 times

 **f7d3be6** 1 month, 3 weeks ago

Respuesta C Por ejemplo, en Confidencial, su organización puede usar varias etiquetas diferentes para tipos específicos de esa sensibilidad. En este ejemplo, la etiqueta principal Confidencial es simplemente una etiqueta de texto sin configuración de protección y, dado que tiene subetiquetas, no se puede aplicar al contenido. En su lugar, los usuarios deben elegir Confidencial para ver las subetiquetas y, a continuación, pueden elegir una subetiqueta para aplicar al contenido.  
upvoted 1 times

 **Greatone1** 1 month, 4 weeks ago

**Selected Answer: C**

C is the correct answer

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>  
upvoted 2 times

 **hogehogehoge** 1 month, 4 weeks ago

**Selected Answer: C**

C is correct. Because user can then apply that sublabel to content and containers, but can't apply just the parent label.  
<https://learn.microsoft.com/en-us/purview/sensitivity-labels>

upvoted 3 times

**HOTSPOT -**

Your company has a Microsoft 365 E5 tenant

Users at the company use the following versions of Microsoft Office:

Microsoft 365 Apps for enterprise

Office for the web -

Office 2016 -

Office 2019 -

The company currently uses the following Office file types:

.docx

.xlsx

.doc

.xls

You plan to use sensitivity labels.

You need to identify the following:

Which versions of Office require an add-in to support the sensitivity labels.

Which file types support the sensitivity labels.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Office versions that require an add-in to support the sensitivity labels:

- Office 2016 only
- Office 2019 only
- Office for the web only
- Office 2016 and Office 2019 only
- Microsoft 365 Apps for enterprise only
- Microsoft 365 Apps for enterprise and Office for the web only

Office file types that support the sensitivity labels:

- .doc only
- .docx only
- .xls only
- .xlsx only
- .doc and .xls
- .docx and .xlsx
- .doc, .docx, .xls, and .xlsx

**Answer Area**

Office versions that require an add-in to support the sensitivity labels:

- Office 2016 only
- Office 2019 only
- Office for the web only
- Office 2016 and Office 2019 only
- Microsoft 365 Apps for enterprise only
- Microsoft 365 Apps for enterprise and Office for the web only**

**Correct Answer:**

Office file types that support the sensitivity labels:

- .doc only
- .docx only
- .xls only
- .xlsx only
- .doc and .xls
- .docx and .xlsx**
- .doc, .docx, .xls, and .xlsx

 **letters1234** 1 month, 2 weeks ago

365 versions of Office (365 Apps) have it built in. Meaning only the 2016/2019 currently require the AIP UL add-in (which is being deprecated soon).

<https://techcommunity.microsoft.com/t5/security-compliance-and-identity/sensitivity-labeling-now-built-into-office-apps-for-windows-to/ba-p/844506>

<https://learn.microsoft.com/en-us/purview/sensitivity-labels-office-apps#labeling-client-for-desktop-apps>

Office 2016 is out of mainstream support (meaning no new features/functions added) and wouldn't expect them to develop the integrated label handling since it's in security patching only mode.

<https://learn.microsoft.com/en-us/lifecycle/products/microsoft-office-2016>

Would go with 2016 & 2019, however not sure how much longer this question will be around considering the add-in is being deprecated.

upvoted 4 times

✉️  **RJTW070** 1 month ago

According to the information I found, the Office versions that require an add-in to support the sensitivity labels are the standalone editions of Office, sometimes called "Office Perpetual". These editions do not have the built-in labeling client that is available for subscription editions of Office<sup>1</sup>. The add-in component that is required for these editions is the Azure Information Protection (AIP) unified labeling client<sup>2</sup>. However, this add-in is now in maintenance mode and will be retired in April 2024<sup>2</sup>. Therefore, it is recommended to move to built-in labeling for Office apps if possible

upvoted 3 times

✉️  **RJTW070** 1 month ago

So I will go for Office 2016 and 2019 the second answer is correct

upvoted 3 times

✉️  **Milad666** 1 week, 3 days ago

Second Answer is not correct, AIP Support all those File ! Just Google it !

<https://learn.microsoft.com/en-us/azure/information-protection/rms-client/clientv2-admin-guide-file-types>

upvoted 1 times

✉️  **Greatone1** 2 months ago

Given answer is correct.

upvoted 1 times

**HOTSPOT -**

You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)

## Create retention label

The screenshot shows the 'Create retention label' wizard at the 'Review and finish' step. On the left, a vertical progress bar indicates steps completed (Name, Retention settings) and the final step (Finish). The main area displays the retention label configuration:

- Name:** Name: 6Months, Edit link
- Retention settings:**
  - Retention period: 6 months, Edit link
  - Retention action: Retain and Delete, Edit link
- Based on:** Based on when it was created, Edit link

On the right, there are three icons: a question mark, a message bubble, and a refresh symbol. At the bottom are 'Back', 'Create label' (highlighted in blue), and 'Cancel' buttons.

You create a label policy as shown in the Label Policy exhibit. (Click the Label Policy tab.)

Auto-labeling > Create auto-labeling policy

The screenshot shows the 'Create auto-labeling policy' wizard at the 'Apply label to content matching this query' step. On the left, a vertical progress bar indicates steps completed (Name, Info to label, Create content query) and the final step (Finish). The main area displays a content query configuration:

**Conditions:** ProjectX

At the bottom are 'Add condition' and 'Next' (highlighted in blue) buttons. On the right, there are three icons: a question mark, a message bubble, and a refresh symbol. A 'Back' button is also present.

The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input type="radio"/>
Any sent email message that contains the word ProjectX will be retained for six months.	<input type="radio"/>	<input type="radio"/>
Users are required to manually apply a label to email messages that contain the word ProjectX.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input checked="" type="radio"/>
Any sent email message that contains the word ProjectX will be retained for six months.	<input checked="" type="radio"/>	<input type="radio"/>
Users are required to manually apply a label to email messages that contain the word ProjectX.	<input type="radio"/>	<input checked="" type="radio"/>

 **spectre786** Highly Voted  1 month, 1 week ago

Should be N/Y/N  
upvoted 5 times

You have a Microsoft 365 subscription.

Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de-fghij.

You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs.

What should you create to ensure that the DLP policy can detect the customer IDs?

- A. a PowerShell script
- B. a sensitivity label
- C. a sensitive information type
- D. a retention label

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **sherifhamed** 2 weeks, 5 days ago

**Selected Answer: C**

The correct answer is C. a sensitive information type.

A sensitive information type is a predefined or custom entity that can be used to identify and protect sensitive data in Microsoft 365.  
upvoted 2 times

 **RJTW070** 1 month ago

Yes correctYou have a Microsoft 365 subscription.

Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de-fghij.

You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs.

What should you create to ensure that the DLP policy can detect the customer IDs?

upvoted 1 times

 **Greatone1** 2 months ago

Answer is correct

<https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide>

upvoted 1 times

You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:

Retention period: 7 years -

Start the retention period based on: When items were created

You need to prevent the removal of the label once the label is applied to a file.

What should you select in the retention label settings?

- A. Retain items forever or for a specific period
- B. Mark items as a regulatory record
- C. Mark items as a record
- D. Retain items even if users delete

**Correct Answer: A**

*Community vote distribution*

B (90%) 10%

✉️  **jt2214** 3 weeks ago

**Selected Answer: B**

B all the way  
upvoted 1 times

✉️  **Jslei** 1 month ago

**Selected Answer: B**

def B  
<https://learn.microsoft.com/en-us/purview/records-management?view=o365-worldwide#compare-restrictions-for-what-actions-are-allowed-or-blocked>  
upvoted 1 times

✉️  **gbartumeu** 1 month ago

**Selected Answer: B**

The key point is here:  
"You need to prevent the removal of the label once the label is applied to a file."

"Retain forever" would prevent the removal of the item, but the label can be unassigned and then removed. By selecting "Record" you ensure no one can edit, unassign or delete the item and the label (except Admins).

If even Admins cannot remove the label once it is applied then it should be "Regulatory Record".

upvoted 1 times

✉️  **letters1234** 1 month, 2 weeks ago

**Selected Answer: B**

Regulatory Record Labels can be used in situations where you absolutely need to ensure that the record isn't altered. They really aren't for the faint-hearted – once you apply one there is no going back – the record and its metadata are permanently locked.  
upvoted 2 times

✉️  **Greatone1** 1 month, 3 weeks ago

**Selected Answer: B**

Sorry I meant B  
upvoted 4 times

✉️  **Greatone1** 1 month, 3 weeks ago

**Selected Answer: A**

Correct answer is A  
<https://www.examtopics.com/discussions/microsoft/view/80391-exam-ms-101-topic-3-question-121-discussion/>  
upvoted 1 times



Box1:Exchange email.

Box2:either a credit card number or the Retention label1 label applied

upvoted 1 times

 **letters1234** 1 month, 2 weeks ago

"Suppose you need to act on credit card information in messages. The actions you take once it's found aren't the subject of this article, but you can learn more about that in -\*\*-Mail flow rule actions in Exchange Online.-\*\*-"

<https://learn.microsoft.com/en-us/exchange/security-and-compliance/data-loss-prevention/dlp-rule-application>

upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

#### PROVISION FROM ACTIVE DIRECTORY



##### Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

##### Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

#### USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com.

You need to ensure that User2 can access the resources in Azure AD.

Solution: From the on-premises Active Directory domain, you assign User2 the Allow logon locally user right. You instruct User2 to sign in as user2@fabrikam.com.

Does this meet the goal?

A. Yes

B. No

#### Correct Answer: B

*Community vote distribution*

B (100%)

**Greatone1** 1 month, 2 weeks ago

This is not a permissions issue.

The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

upvoted 1 times

**Greatone1** 1 month, 4 weeks ago

**Selected Answer: B**

Correct answer should be no

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint Administrator role.

Does this meet the goal?

A. Yes

B. No

**Correct Answer:** B

✉️ 🚩 **Shadowcatest** 5 days, 22 hours ago

No.

SharePoint Administrator role have access to the SharePoint admin center and can create and manage sites, designate site admins, manage sharing settings, and manage Microsoft 365 groups, including creating, deleting, and restoring groups, and changing group owners.

upvoted 1 times

✉️ 🚩 **DiligentSam** 3 weeks, 5 days ago

My Answer is B

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Security Administrator role.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: A**

*Community vote distribution*

B (63%)

A (38%)

✉  **tzzz1986**  4 weeks, 1 day ago

**Selected Answer: B**

Security administrator role does not seem to have accesss in Teams, Sharepoint. Reference: <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator>

upvoted 5 times

✉  **Alscoran** 3 days, 19 hours ago

Its not asking for rights to the other products. Its asking for access to Defender settings that protect those products. I say A.

upvoted 1 times

✉  **PhoenixMan**  1 day ago

I think the right answer is A

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/m365d-permissions?view=o365-worldwide>

upvoted 1 times

✉  **jt2214** 4 days, 14 hours ago

**Selected Answer: A**

I agree with Darekms0 based on

<https://www.examtopics.com/discussions/microsoft/view/76446-exam-ms-101-topic-2-question-50-discussion/>

upvoted 1 times

✉  **Darekms0** 1 week ago

**Selected Answer: A**

<https://www.examtopics.com/discussions/microsoft/view/76446-exam-ms-101-topic-2-question-50-discussion/>

upvoted 2 times

✉  **Paul\_white** 1 week, 5 days ago

ANSWER FOR ME IS A

upvoted 2 times

✉  **Greatone1** 1 month, 2 weeks ago

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide>

upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange Administrator role.

Does this meet the goal?

A. Yes

B. No

**Correct Answer:** B

 **DiligentSam** 3 weeks, 5 days ago

I think the answer is No

Because you are just assigned a Exchange Online Admin Role.

upvoted 1 times

**HOTSPOT****Overview**

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named A. Datum Corporation.

**Environment****On-Premises Environment**

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins, Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

**Cloud Environment**

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure AD Premium P2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

- Password hash synchronization is enabled.
- Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk Administrator
Admin3	Security Administrator
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.

The Azure AD tenant has Security defaults enabled.

## Problem Statements

-  
Litware identifies the following issues:

- Admin1 cannot create conditional access policies.
- Admin4 receives an error when attempting to use SSPR.
- Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

## Requirements

## Planned Changes

-  
Litware plans to implement the following changes:

- Implement Microsoft Intune.
- Implement Microsoft Teams.
- Implement Microsoft Defender for Office 365.
- Ensure that users can install Office 365 apps on their device.
- Convert all the Windows 10 Pro devices to Windows 10 Enterprise ES.
- Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

## Technical Requirements

-  
Litware identifies the following technical requirements:

- Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
- Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
- Litware users must be able to invite A. Datum users to participate in the following activities:
  - Join Microsoft Teams channels.
  - Join Microsoft Teams chats.
  - Access shared files.
  - Just in time access to critical administrative roles must be required.
- Microsoft 365 incidents and advisories must be reviewed monthly.
- Office 365 service status notifications must be sent to Admin2.
- The principle of least privilege must be used.

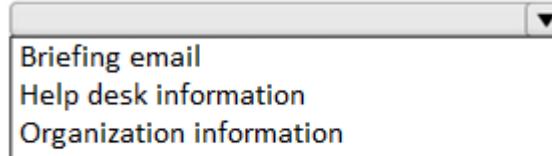
You need to configure the Office 365 service status notifications and limit access to the service and feature updates. The solution must meet the technical requirements.

What should you configure in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.

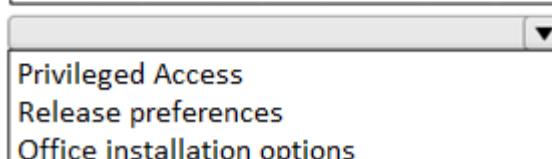
NOTE: Each correct selection is worth one point.

**Answer Area**

To configure the notifications:

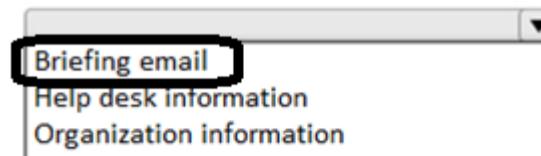


To limit access:



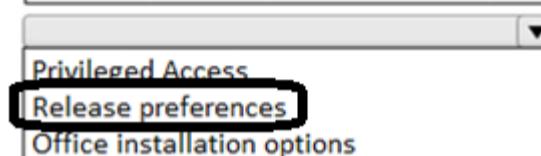
**Answer Area**

To configure the notifications:



**Correct Answer:**

To limit access:



**Casticod** Highly Voted 1 month, 2 weeks ago

The first answer is wrong:

1. Organization information: <https://admin.microsoft.com/> --> Settings --> Org Settings --> Organization information --> Technical contact
2. Release preferences  
<https://www.examtopics.com/discussions/microsoft/view/81376-exam-ms-100-topic-8-question-1-discussion/>

upvoted 5 times

**Overview -**

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named A. Datum Corporation.

**Environment -****On-Premises Environment -**

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins, Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

**Cloud Environment -**

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure AD Premium P2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

- Password hash synchronization is enabled.
- Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk Administrator
Admin3	Security Administrator
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.

The Azure AD tenant has Security defaults enabled.

**Problem Statements -**

Litware identifies the following issues:

- Admin1 cannot create conditional access policies.
- Admin4 receives an error when attempting to use SSPR.
- Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

Requirements -

Planned Changes -

Litware plans to implement the following changes:

- Implement Microsoft Intune.
- Implement Microsoft Teams.
- Implement Microsoft Defender for Office 365.
- Ensure that users can install Office 365 apps on their device.
- Convert all the Windows 10 Pro devices to Windows 10 Enterprise ES.
- Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

Technical Requirements -

Litware identifies the following technical requirements:

- Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
- Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
- Litware users must be able to invite A. Datum users to participate in the following activities:
  - Join Microsoft Teams channels.
  - Join Microsoft Teams chats.
  - Access shared files.
  - Just in time access to critical administrative roles must be required.
- Microsoft 365 incidents and advisories must be reviewed monthly.
- Office 365 service status notifications must be sent to Admin2.
- The principle of least privilege must be used.

You need to configure Azure AD Connect to support the planned changes for the Montreal Users and Seattle Users OUs.

What should you do?

- A. From PowerShell, run the Add-ADSyncConnectorAttributeInclusion cmdlet.
- B. From the Microsoft Azure AD Connect wizard, select Manage federation.
- C. From the Microsoft Azure AD Connect wizard, select Customize synchronization options.
- D. From PowerShell, run the Start-ADSyncSyncCycle cmdlet.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **Casticod** 1 month, 2 weeks ago

**Selected Answer: C**

Correct <https://www.examtopics.com/discussions/microsoft/view/89165-exam-ms-100-topic-13-question-2-discussion/>  
upvoted 1 times

**Overview -**

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

**Existing Environment -****Active Directory Environment -**

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

**Network Infrastructure -**

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as DNS servers.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

**Requirements -****Planned Changes -**

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

- Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
- Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

**Technical Requirements -**

Fabrikam identifies the following technical requirements:

- All users must be able to exchange email messages successfully during Project1 by using their current email address.

- Users must be able to authenticate to cloud services if Active Directory becomes unavailable.
- A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.
- Microsoft 365 Apps for enterprise applications must be installed from a network share only.
- Disruptions to email access must be minimized.

#### Application Requirements -

Fabrikam identifies the following application requirements:

- An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
- The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

#### Security Requirements -

Fabrikam identifies the following security requirements:

- After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
- The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.
- After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
- The principle of least privilege must be used.

You are evaluating the required processes for Project1.

You need to recommend which DNS record must be created while adding a domain name for the project.

Which DNS record should you recommend?

- A. host (A)
- B. alias (CNAME)
- C. text (TXT)
- D. host (AAAA)

**Correct Answer: B**

*Community vote distribution*

C (100%)

 **AMDF** 1 month, 1 week ago

**Selected Answer: C**

Vote for C

upvoted 2 times

 **Casticod** 1 month, 2 weeks ago

**Selected Answer: C**

Not necessary Cname record to add Email Only TXT o MX Record are Valid. Correct C <https://learn.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide#step-1-add-a-txt-or-mx-record-to-verify-you-own-the-domain>

upvoted 4 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Teams Administrator role.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: B**

**HOTSPOT**

Your network contains an on-premises Active Directory domain named contoso.com.

Your company purchases Microsoft 365 subscription and establishes a hybrid deployment of Azure AD by using password hash synchronization. Password writeback is disabled in Azure AD Connect.

You create a new user named User10 on-premises and a new user named User20 in Azure AD.

You need to identify where an administrator can reset the password of each new user.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User10:	<input type="checkbox"/> Azure AD only	<input type="checkbox"/> On-premises Active Directory only	<input type="checkbox"/> On-premises Active Directory or Azure AD
User20:	<input type="checkbox"/> Azure AD only	<input type="checkbox"/> On-premises Active Directory only	<input type="checkbox"/> On-premises Active Directory or Azure AD

**Answer Area****Correct Answer:**

User10:	<input checked="" type="checkbox"/> Azure AD only	<input checked="" type="checkbox"/> On-premises Active Directory only	<input checked="" type="checkbox"/> On-premises Active Directory or Azure AD
User20:	<input checked="" type="checkbox"/> Azure AD only	<input checked="" type="checkbox"/> On-premises Active Directory only	<input checked="" type="checkbox"/> On-premises Active Directory or Azure AD

  **Greatone1** 1 week, 4 days ago

Answers are correct

<https://www.examtopics.com/discussions/microsoft/view/49675-exam-ms-100-topic-3-question-37-discussion/>

upvoted 2 times

## HOTSPOT

You have an Azure AD tenant that contains the groups shown in the following exhibit.

<input type="checkbox"/>	Name	Group type	Membership type	Source	Security enabled
<input type="checkbox"/>	GR Group1	Microsoft 365	Assigned	Cloud	Yes
<input type="checkbox"/>	GR Group2	Microsoft 365	Assigned	Cloud	No
<input type="checkbox"/>	GR Group3	Security	Assigned	Cloud	Yes
<input type="checkbox"/>	GR Group4	Security	Dynamic	Cloud	Yes
<input type="checkbox"/>	GR Group5	Security	Assigned	Windows Server AD	Yes

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

## Answer Area

You can add an Azure AD cloud user to [answer choice].

Group1 only  
Group1 and Group3 only  
Group1, Group2, and Group3 only  
Group1, Group3, and Group4 only  
Group1, Group2, Group3, Group4, and Group5

You can add Group5 to [answer choice].

Group1 only  
Group3 only  
Group1, and Group3 only  
Group1, Group3, and Group4 only  
Group1, Group2, Group3, and Group4

## Answer Area

You can add an Azure AD cloud user to [answer choice].

Group1 only  
Group1 and Group3 only  
Group1, Group2, and Group3 only  
Group1, Group3, and Group4 only  
Group1, Group2, Group3, Group4, and Group5

## Correct Answer:

You can add Group5 to [answer choice].

Group1 only  
Group3 only  
Group1, and Group3 only  
Group1, Group3, and Group4 only  
Group1, Group2, Group3, and Group4

**AMDF** Highly Voted 1 month, 1 week ago

- 1) Group 1, Group 2 and Group 3
- 2) Group 3 only

upvoted 13 times

You have a Microsoft 365 E5 subscription that is linked to an Azure AD tenant named contoso.com.

You purchase 100 Microsoft 365 Business Voice add-on licenses.

You need to ensure that the members of a group named Voice are assigned a Microsoft 365 Business Voice add-on license automatically.

What should you do?

- A. From the Licenses page of the Microsoft 365 admin center, assign the licenses.
- B. From the Microsoft Entra admin center, modify the settings of the Voice group.
- C. From the Microsoft 365 admin center, modify the settings of the Voice group.

**Correct Answer: C**

 **Paul\_white** 2 weeks, 1 day ago

CORRECT ANSWER IS B WITHOUT A DOUBT

upvoted 2 times

 **sherifhamed** 2 weeks, 2 days ago

**Selected Answer: B**

<https://www.examtopics.com/discussions/microsoft/view/48720-exam-ms-100-topic-3-question-83-discussion/>

upvoted 3 times

 **sherifhamed** 2 weeks, 5 days ago

**Selected Answer: C**

The correct answer is C. From the Microsoft 365 admin center, modify the settings of the Voice group.

To assign Microsoft 365 Business Voice add-on licenses to a group automatically, you need to use the group-based licensing feature in Azure Active Directory

upvoted 1 times

 **jt2214** 1 month ago

**Selected Answer: B**

Should be B

upvoted 2 times

 **gbartumeu** 1 month ago

**Selected Answer: B**

You can add group members from both (Entra and Microsoft 365 admin centers). However, to assign licenses based on the group it can only be set from Entra Admin (Azure AD).

upvoted 2 times

 **Master\_Tx** 1 month ago

Should be done from Azure / Entra as best practice on dynamic assignment.

upvoted 1 times

 **AMDF** 1 month, 1 week ago

**Selected Answer: B**

Vote for B

upvoted 2 times

 **Casticod** 1 month, 2 weeks ago

**Selected Answer: B**

Only from Entra/azure AD <https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-groups-assign>

Correct B

upvoted 2 times

You have a Microsoft 365 E5 subscription that uses Endpoint security.

You need to create a group and assign the Endpoint Security Manager role to the group.

Which type of group can you use?

- A. Microsoft 365 only
- B. security only
- C. mail-enabled security and security only
- D. mail-enabled security, Microsoft 365, and security only
- E. distribution, mail-enabled security, Microsoft 365, and security

**Correct Answer: D**

 cb0900  1 month, 1 week ago

**Selected Answer: D**

In a test tenant, I was able to add mail-enabled security, M365 and security groups to an EndPoint Security Manager role assignment.

Add Role Assignment -> Admin Groups...

upvoted 6 times

 Darekms0  1 week ago

**Selected Answer: D**

Checked : From endopint manager > tenant admin > roles > open "endpoint decurity manager" > assignments > .... you can choose M365, security & mail-enabled group

upvoted 3 times

 Darekms0 1 week ago

**Selected Answer: B**

Looks like B for me -> <https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept#how-role-assignments-to-groups-work>

upvoted 1 times

 Darekms0 1 week ago

Update it should be D -> From endopint manager > tenant admin > roles > open "endpoint decurity manager" > assignments > .... you can choose M365, security & mail-enabled group

upvoted 2 times

 MarkusSan 1 week ago

**Selected Answer: D**

<https://www.examtopics.com/discussions/microsoft/view/80188-exam-ms-100-topic-5-question-64-discussion/>

upvoted 3 times

 RJTW070 1 month ago

**Selected Answer: B**

To create a group and assign the Endpoint Security Manager role to the group, you can use a role-assignable group. A role-assignable group is a type of Azure AD security group that can be assigned to a role in Microsoft Endpoint Manager1. You can create a role-assignable group by using the Azure portal, PowerShell, or Microsoft Graph2.

upvoted 2 times

 ae88d96 1 month, 1 week ago

**Selected Answer: B**

Correct answer B.

When assigning roles like the Endpoint Security Manager role, you should use a security group. Security groups are specifically designed for managing access control and permissions in Microsoft 365. They can be used to manage access to various resources and assign roles to group members, providing a more streamlined and efficient way of managing permissions.

In this case, using a security-only group is the appropriate choice because it focuses on access management and role assignment, ensuring that the Endpoint Security Manager role is correctly assigned to the group members. Other types of groups, like Microsoft 365, mail-enabled security, or distribution groups, serve different purposes (such as collaboration or email communication) and are not designed for managing access control and role assignments in the same way as security groups are.

upvoted 4 times

**HOTSPOT**

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Department	Job title
User1	IT engineering	Technician
User2	Engineering	Senior executive
User3	Finance	Manager

You create a new administrative unit named AU1 and configure the following AU1 dynamic membership rule.

(user.department -eq "Engineering") and (user.jobTitle -notContains "Executive")

The subscription contains the role assignments shown in the following table.

Name	Role
Admin1	AU1\User Administrator
Admin2	Global Administrator

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
Admin1 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>
Admin1 can reset the password of User2.	<input type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>

**Answer Area**

Statements	Yes	No
Admin1 can reset the password of User1.	<input checked="" type="checkbox"/>	<input type="radio"/>
Admin1 can reset the password of User2.	<input type="radio"/>	<input checked="" type="checkbox"/>
Admin2 can reset the password of User3.	<input checked="" type="checkbox"/>	<input type="radio"/>

**Correct Answer:**

**Casticod** Highly Voted 1 month, 1 week ago

-equal means that the exact name must match, -contain The Contains operator does partial string matches but not item in a collection matches Note the agument and (must match the 2) User 1 and user 2 do not belong as the 2 conditions do not match Therefore user 1 and user 2 do not belong to AU1 and are outside the scope of Admin 1 Option 1 NO Option 2 NO Option 3 YES upvoted 16 times

**cb0900** 1 month, 1 week ago

Agree.

NO

NO

YES

upvoted 2 times

✉️ 🚩 **CloudCanary** 3 weeks, 3 days ago

Definitely N,N,Y, I agree 100%

upvoted 2 times

✉️ 🚩 **PhoenixMan** [Most Recent ⓘ] 23 hours, 25 minutes ago

the answer should be N,N,Y

upvoted 1 times

Question #118

Topic 1

You have a Microsoft 365 subscription.

You need to be notified to your personal email address when a Microsoft Exchange Online service issue occurs.

What should you do?

- A. From the Exchange admin center, create a contact.
- B. From the Microsoft Outlook client, configure an Inbox rule.
- C. From the Microsoft 365 admin center, update the technical contact details.
- D. From the Microsoft 365 admin center, customize the Service health settings.

**Correct Answer: D**

✉️ 🚩 **Greatone1** 1 week, 3 days ago

Correct answer is D

upvoted 1 times

✉️ 🚩 **mhmyz** 3 weeks, 3 days ago

**Selected Answer: D**

D

Service Health can mail only Exchange issue.

Technical contact get mail M365 total issue.

upvoted 1 times

✉️ 🚩 **Master\_Tx** 1 month ago

You can do C and D.

upvoted 1 times

**HOTSPOT**

Your company has an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Privileged Role Administrator
User2	User Administrator
User3	Security Administrator
User4	Billing Administrator

The tenant includes a security group named Admin1. Admin1 will be used to manage administrative accounts. External collaboration settings have default configuration.

You need to identify which users can perform the following administrative tasks:

- Create guest user accounts.
- Add User3 to Admin1.

Which users should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Create guest user accounts:

User2 only  
User3 only  
User4 only  
User2 and User3 only  
User1, User2, and User3 only  
User1, User2, User3, and User4

Add User3 to Admin1:

User2 only  
User3 only  
User4 only  
User2 and User3 only  
User1, User2, and User3 only  
User1, User2, User3, and User4

**Answer Area**

Create guest user accounts:

User2 only  
User3 only  
User4 only  
User2 and User3 only  
User1, User2, and User3 only  
User1, User2, User3, and User4

**Correct Answer:**

Add User3 to Admin1:

User2 only  
User3 only  
User4 only  
User2 and User3 only  
User1, User2, and User3 only  
User1, User2, User3, and User4

 **Contactfornitish** 4 days, 22 hours ago

Default config means all users including those without any role can also invite guests  
only user admin can manage groups

upvoted 1 times

 **Darekms0** 1 week ago

Specify who can invite guests: By default, all users in your organization, including B2B collaboration guest users, can invite external users to B2B collaboration. If you want to limit the ability to send invitations, you can turn invitations on or off for everyone, or limit invitations to certain roles.  
upvoted 1 times

 **Shloeb** 1 week, 1 day ago

Given answer is correct.

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal>

To complete the scenario in this quickstart, you need:

A role that allows you to create users in your tenant directory, such as at least a Guest Inviter role or a User administrator.

upvoted 1 times

 **Greatone1** 1 week, 5 days ago

Answer is 1,2,3,4 and user 2

Sign in to the Azure portal with an account that's been assigned the Global administrator, Guest, inviter, or User administrator role.

upvoted 1 times

 **cb0900** 1 month, 1 week ago

1. With the default configuration all users (user 1, user 2, user 3 and user 4)

2. User admin (user 2 only) can change security group membership

upvoted 2 times

 **Casticod** 1 month, 1 week ago

A Standard user Be able (to default) to create Guest users, The user have access to portal.azure.com. Try for me

In the first option, all users (user 1 user 2 user 3 and user 4)

upvoted 3 times

 **Casticod** 1 month, 1 week ago

watch the question "External collaboration settings have default configuration" Confirm my decision: first option, all users (user 1 user 2 user 3 and user 4)

upvoted 3 times

Question #120

Topic 1

You have a Microsoft 365 subscription.

All users are assigned Microsoft 365 Apps for enterprise licenses.

You need to ensure that reports display the names of users that have activated Microsoft 365 apps and on how many devices.

What should you modify in the Microsoft 365 admin center?

- A. the Reports reader role
- B. Organization information
- C. Org settings for Privacy profile
- D. Org settings for Reports

**Correct Answer: D**

 **cb0900** 1 month, 1 week ago

**Selected Answer: D**

D Uncheck "Display concealed user, group, and site names in all reports".

upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

You need to configure the Org settings to meet the following requirements:

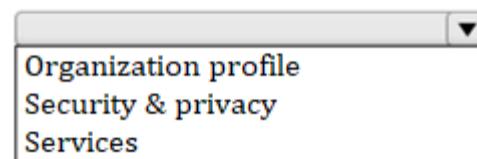
- Sign users out of Microsoft Office 365 web apps after one hour of inactivity.
- Integrate an internal support tool with Office.

Which settings should you configure for each requirement? To answer, select the appropriate options in the answer area.

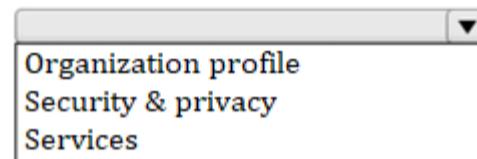
NOTE: Each correct selection is worth one point.

**Answer Area**

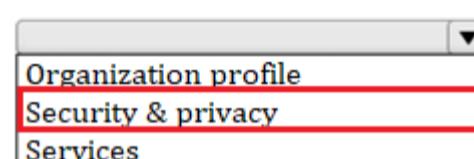
Sign users out after one hour of inactivity:



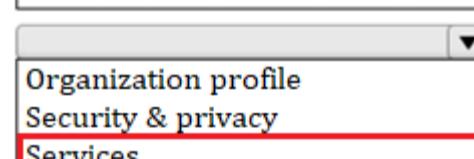
Integrate the internal support tool with Office:

**Answer Area**

Sign users out after one hour of inactivity:

**Correct Answer:**

Integrate the internal support tool with Office:



 **ae88d96** Highly Voted 1 month, 1 week ago

Security & privacy and Organization profile. Tested on my lab.  
upvoted 7 times

 **smiff** Most Recent 2 weeks, 6 days ago

Security and Privacy  
Org Profile

checked on my demo tenant  
upvoted 1 times

 **DiligentSam** 1 month ago

The 2nd Answer is Organization Profile?  
I am not able to find it at Chinese 365 Admin Center in China  
upvoted 1 times

 **Sas2003** 3 weeks, 4 days ago

Yes - "Support integration"  
upvoted 1 times

You have a Microsoft 365 subscription.

You add a domain named contoso.com.

When you attempt to verify the domain, you are prompted to send a verification email to admin@contoso.com.

You need to change the email address used to verify the domain.

What should you do?

- A. Add a TXT record to the DNS zone of the domain.
- B. From the domain registrar, modify the contact information of the domain.
- C. From the Microsoft 365 admin center, change the global administrator of the Microsoft 365 subscription.
- D. Modify the NS records for the domain.

**Correct Answer: B**

**HOTSPOT**

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Device group	Member
1	Group1	Name starts with Comp
2	Group2	Name starts with Comp And OS in Windows 10
3	Group3	OS in Windows Server 2016
Last	Ungrouped devices (default)	Not applicable

You onboard computers to Microsoft Defender for Endpoint as shown in the following table.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer1 and Computer2 members? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Computer1:

- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped devices

Computer2:

- Group1 only
- Group3 only
- Group1 and Group3

**Answer Area**

Computer1:

- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped devices

Correct Answer:

Computer2:

- Group1 only
- Group3 only
- Group1 and Group3

 cb0900 1 month, 1 week ago

Agree, both computers in Group 1. "When a device is matched to more than one group, it's added only to the highest ranked group."

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide#manage-device-groups>  
upvoted 4 times

## HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Security Administrator
Admin3	Security Operator
Admin4	Security Reader
Admin5	Application Administrator

You are implementing Microsoft Defender for Endpoint.

You need to enable role-based access control (RBAC) to restrict access to the Microsoft 365 Defender portal.

Which users can enable RBAC, and which users will no longer have access to the Microsoft 365 Defender portal after RBAC is enabled? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

## Users that can enable RBAC:

- Admin1 only
- Admin1 and Admin2 only
- Admin1, Admin2, and Admin5 only
- Admin1, Admin2, Admin3, and Admin5 only

## Users that will no longer have access to the Microsoft 365 Defender portal:

- Admin5 only
- Admin3 and Admin4 only
- Admin4 and Admin5 only
- Admin3, Admin4, and Admin5 only

## Answer Area

## Users that can enable RBAC:

- Admin1 only
- Admin1 and Admin2 only
- Admin1, Admin2, and Admin5 only
- Admin1, Admin2, Admin3, and Admin5 only

## Correct Answer:

## Users that will no longer have access to the Microsoft 365 Defender portal:

- Admin5 only
- Admin3 and Admin4 only
- Admin4 and Admin5 only
- Admin3, Admin4, and Admin5 only

  cb0900 1 month, 1 week ago

Agree with the answers.

Enable RBAC: Admin1 and Admin 2

No longer have access: Admin 3 and Admin 4

Turning on role-based access control will cause users with read-only permissions (for example, users assigned to Azure AD Security reader role) to lose access until they are assigned to a role.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide#before-you-begin>

<https://www.examtopics.com/discussions/microsoft/view/110910-exam-ms-101-topic-2-question-138-discussion/>  
upvoted 3 times

Your company has a Microsoft 365 E5 subscription.

You onboard a device on the company's network to Microsoft Defender for Endpoint.

In the Microsoft 365 Defender portal, you notice that the device inventory displays many devices that have an Onboarding status of Can be onboarded.

You need to ensure that onboarded devices are prevented from polling the network for device discovery but can still discover devices with which they communicate directly.

What should you configure in the Microsoft 365 Defender portal?

- A. standard discovery
- B. device discovery exclusions
- C. basic discovery
- D. a network assessment job

**Correct Answer:** B

 **jt2214** 4 days, 15 hours ago

**Selected Answer: C**

It's C

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-discovery?view=o365-worldwide#discovery-methods>  
upvoted 1 times

 **netbw** 2 weeks, 3 days ago

**Selected Answer: C**

C. Basic discovery

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-discovery?view=o365-worldwide#discovery-methods>  
upvoted 2 times

 **Sas2003** 3 weeks, 4 days ago

**Selected Answer: B**

I believe the correct answer is B.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-discovery?view=o365-worldwide#discovery-methods>  
upvoted 1 times

 **Sas2003** 3 weeks ago

Oops I meant C

upvoted 2 times

## HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

You need to onboard Device1 and Device2 to Microsoft Defender for Endpoint.

What should you use to onboard each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Device1:

A local script  
 Group Policy  
 Microsoft Intune  
 An app from the Google Play store  
 Integration with Microsoft Defender for Cloud

Device2:

A local script  
 Group Policy  
 Microsoft Intune  
 An app from the Google Play store  
 Integration with Microsoft Defender for Cloud

## Answer Area

Correct Answer:

Device1:

A local script  
 Group Policy  
 Microsoft Intune  
 An app from the Google Play store  
 Integration with Microsoft Defender for Cloud

Device2:

A local script  
 Group Policy  
 Microsoft Intune  
 An app from the Google Play store  
 Integration with Microsoft Defender for Cloud

 **Contactfornitish** 2 days, 4 hours ago

I have reservations for Device 1. Unless integration with Microsoft Defender completed within Intune, Intune can not onboard the device on its own.

<https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure>

Device 2 can be done via Script only though

upvoted 1 times

 **862e76c** 4 weeks, 1 day ago

Agree with the answer

upvoted 1 times

 **cb0900** 1 month ago

I would agree with given answers:

1. Intune
2. Local script

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-install-manually?view=o365-worldwide>  
macOS onboarding for up to 10 devices, local script is the default option.

upvoted 2 times

 **Casticod** 1 month, 1 week ago

option 1 Intune.

Option 2 Integration with Microsoft defender for cloud : <https://techcommunity.microsoft.com/t5/microsoft-defender-vulnerability/unmanaged-device-protection-capabilities-are-now-generally/ba-p/2463796>

upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 subscription.

You need to create two groups named Group1 and Group2. The solution must meet the following requirements:

- Group1 must be mail-enabled and have an associated Microsoft SharePoint Online site.
- Group2 must support dynamic membership and role assignments but must NOT be mail-enabled.

Which types of groups should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Group1:

Distribution  
Dynamic distribution  
Microsoft 365  
Security

Group2:

Distribution  
Dynamic distribution  
Microsoft 365  
Security

**Answer Area**

Group1:

Distribution  
Dynamic distribution  
Microsoft 365  
Security

Group2:

Distribution  
Dynamic distribution  
Microsoft 365  
Security

**vercracked\_007** Highly Voted 1 month ago

Box 1 Microsoft 365  
Box 2 Security

They are swapped  
upvoted 10 times

**jt2214** Most Recent 4 days, 15 hours ago

It's the other way around. Exam topics please fix this. :)  
Box 1 Microsoft 365  
Box 2 Security  
upvoted 1 times

**DiligentSam** 3 weeks, 3 days ago

Support dynamic membership  
why not choose Dynamic Distribution?  
upvoted 1 times

**netbw** 2 weeks, 3 days ago

Because it's gonna be email enabled  
upvoted 1 times

**Casticod** 1 month, 2 weeks ago

To The group 1 I need opinions, given the options I would say Microsoft 365, since a security group is not the same as a mail-enabled security group  
to the group 2 The option Should be Security <https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-create-rule#check-processing-status-for-a-rule>  
upvoted 4 times

Question #128

Topic 1

DRAG DROP

You have a Microsoft 365 subscription.

You need to meet the following requirements:

- Report a Microsoft 365 service issue.
- Request help on how to add a new user to an Azure AD tenant.

What should you use in the Microsoft 365 admin center? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Features	Answer Area
Message center	To report issues regarding a Microsoft 365 service: <input type="text"/>
New service request	To request help on how to add a new user to the tenant: <input type="text"/>
Product feedback	
Service health	

Answer Area
Correct Answer: To report issues regarding a Microsoft 365 service: <input type="text"/> New service request
To request help on how to add a new user to the tenant: <input type="text"/> Message center

 **Casticod** Highly Voted 1 month, 2 weeks ago

option 1 Service Health --> Report Issues

option 2 new service request

upvoted 11 times

 **jt2214** Most Recent 4 days, 15 hours ago

Service Health

New Service Requests

I do this at my organization.

upvoted 1 times

 **Greatone1** 1 week, 4 days ago

Service Health and second answer is new service requests

upvoted 1 times

 **flim322** 1 month ago

<https://www.examtopics.com/discussions/microsoft/view/96073-exam-ms-100-topic-2-question-87-discussion/>

upvoted 1 times

You have a Microsoft 365 E5 subscription that contains the groups shown in the following exhibit.

The screenshot shows the 'Groups | All groups' page in the Azure Active Directory portal. The page title is 'Groups | All groups' with a subtitle 'Contoso Ltd. - Azure Active Directory'. The top navigation bar includes links for 'New group', 'Download groups', 'Refresh', 'Manage view', 'Delete', and 'Got feedback?'. Below the navigation is a search bar with a placeholder 'Search' and a 'Add filter' button. A 'Search mode' toggle is set to 'Contains'. The table below lists four groups:

	Name	Group type	Security enabled	Role assignments allowed
<input type="checkbox"/>	GR Group1	Microsoft 365	No	No
<input type="checkbox"/>	G Group2	Microsoft 365	Yes	No
<input type="checkbox"/>	GR Group3	Security	Yes	No
<input type="checkbox"/>	GR Group4	Security	Yes	Yes

To which groups can you assign Microsoft 365 E5 licenses?

- A. Group1 and Group2 only
- B. Group2 and Group3 only
- C. Group3 and Group4 only
- D. Group1, Group2, and Group3 only
- E. Group2, Group3, and Group4 only

**Correct Answer: C**

CloudCanary 3 weeks, 2 days ago

**Selected Answer: E**

Microsoft 365 Groups with Security Enabled can be assigned with licences.  
upvoted 1 times

cb0900 1 month ago

**Selected Answer: E**

Licenses can be assigned to any security group, including M365 security enabled.  
<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/licensing-whatis-azure-portal?context=azure%2Factive-directory%2Fusers-groups-roles%2Fcontext%2Fugr-context#features>

Similar q from sc-300:

<https://www.examtopics.com/discussions/microsoft/view/51472-exam-sc-300-topic-1-question-1-discussion/>  
upvoted 4 times

**HOTSPOT**

You have a Microsoft 365 subscription.

From the Microsoft 365 admin center, you open the Microsoft 365 Apps usage report as shown in the following exhibit.

Username ⓘ	Last activation date (UTC)	Last activity date (UTC)	Choose columns
431B8D0D1D05D877FDC4416			
2F2747649D4150B686307383			
659213C0E1D99EA1A4AD56D		Wednesday, August 3, 2022	
FE185622F642B0381DB633EC			
988D39ED225FC80FF2A5684			

You need ensure that the report meets the following requirements:

- The Username column must display the actual name of each user.
- Usage of the Microsoft Teams mobile app must be displayed.

What should you modify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

The Username column must display the actual name of each user:

Privacy profile in Org settings  
Reports in Org settings  
The membership of the Reports Reader role

Usage of the Teams mobile app must be displayed:

Microsoft Teams in Org settings  
The columns in the report  
The Teams license assignment

**Answer Area**

The Username column must display the actual name of each user:

Privacy profile in Org settings  
**Reports in Org settings**  
The membership of the Reports Reader role

Usage of the Teams mobile app must be displayed:

**Microsoft Teams in Org settings**  
The columns in the report  
The Teams license assignment

**Correct Answer:**

Usage of the Teams mobile app must be displayed:

 cb0900  1 month ago

1. Reports in Org settings (uncheck 'Display concealed user, group and site names in all reports').
2. Columns in the report ('Activity on Teams app' column).

upvoted 5 times

 Casticod  1 month, 1 week ago

Valid option for me in Part Two "The columns in reports"

For me neither the first nor the third are valid. The second is incomplete. For me, you can only know the use of Teams Mobile, from the analytics section of the Teams administrator or in the usage section. The second option (The columns in the reports) can refer to the reports section in the 365 administration portal but it is undoubtedly poorly described.

upvoted 2 times

Question #131

Topic 1

Your company has on-premises servers and an Azure AD tenant.

Several months ago, the Azure AD Connect Health agent was installed on all the servers.

You review the health status of all the servers regularly.

Recently, you attempted to view the health status of a server named Server1 and discovered that the server is NOT listed on the Azure AD Connect Servers list.

You suspect that another administrator removed Server1 from the list.

You need to ensure that you can view the health status of Server1.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. From Windows PowerShell, run the Register-AzureADConnectHealthSyncAgent cmdlet.
- B. From Azure Cloud shell, run the Connect-AzureAD cmdlet.
- C. From Server1, reinstall the Azure AD Connect Health agent.
- D. From Server1, change the Azure AD Connect Health services Startup type to Automatic.
- E. From Server1, change the Azure AD Connect Health services Startup type to Automatic (Delayed Start).

**Correct Answer: AC**

 **jt2214** 1 month ago

- A. Running the Register-AzureADConnectHealthSyncAgent cmdlet from Windows PowerShell helps to register or re-register the Azure AD Connect Health Sync Agent on Server1, ensuring that it appears on the list of monitored servers.
- C. Reinstalling the Azure AD Connect Health agent on Server1 will also register it with Azure AD Connect Health, making it appear on the list of monitored servers.

upvoted 3 times

## DRAG DROP

Your company has an Azure AD tenant named contoso.onmicrosoft.com.

You purchase a domain named contoso.com from a registrar and add all the required DNS records.

You create a user account named User1. User1 is configured to sign in as user1@contoso.onmicrosoft.com.

You need to configure User1 to sign in as user1@contoso.com.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

**Actions**

- Modify the username of User1.
- Modify the email address of User1.
- Verify the custom domain.
- Add contoso.com as a SAN for an X.509 certificate.
- Run Update-MgDomain -DomainId contoso.com.
- Add a custom domain name.

**Answer Area**

1		
2		
3		

**Correct Answer:**

- Answer Area**
- 1 Add a custom domain name.
  - 2 Verify the custom domain.
  - 3 Modify the username of User1.

**DiligentSam** 1 week, 5 days ago

<https://www.examtopics.com/discussions/microsoft/view/49929-exam-ms-100-topic-2-question-7-discussion/>  
upvoted 2 times

**Paul\_white** 2 weeks ago

GIVEN ANSWER IS CORRECT !!!!  
upvoted 1 times

**spectre786** 1 week, 6 days ago

Could you please comment on all questions from 122 to 236, whenever there is no existing comment already ? Thank you for your help.  
upvoted 1 times

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You need to access service health alerts from a mobile phone.

What should you use?

- A. the Microsoft Authenticator app
- B. the Microsoft 365 Admin mobile app
- C. Intune Company Portal
- D. the Intune app

**Correct Answer: B**

 **DiligentSam** 3 weeks ago

Option B is correct

upvoted 2 times

 **862e76c** 4 weeks, 1 day ago

Agree with the answer

upvoted 2 times

**HOTSPOT**

Your company has a Microsoft 365 subscription that contains the domains shown in the following exhibit.

## Domains

+ Add domain    Buy domain    Refresh

Domain name ↑	Status	Choose columns
<input type="checkbox"/> contoso221018.onmicrosoft.com (Default)	<span>Healthy</span>	
<input type="checkbox"/> contoso.com	<span>Incomplete setup</span>	
<input type="checkbox"/> east.contoso221018.onmicrosoft.com	<span>No services selected</span>	

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

**Answer Area**

An administrator can create usernames that contain the [answer choice].

contoso221018.onmicrosoft.com domain only  
contoso221018.onmicrosoft.com domain and all its subdomains only  
contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only  
contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

Exchange Online can receive inbound email messages sent to the [answer choice].

contoso221018.onmicrosoft.com domain only  
contoso221018.onmicrosoft.com domain and all its subdomains only  
contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only  
contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

**Answer Area**

An administrator can create usernames that contain the [answer choice].

contoso221018.onmicrosoft.com domain only  
contoso221018.onmicrosoft.com domain and all its subdomains only  
contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only  
contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

**Correct Answer:**

Exchange Online can receive inbound email messages sent to the [answer choice].

contoso221018.onmicrosoft.com domain only  
contoso221018.onmicrosoft.com domain and all its subdomains only  
contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only  
contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

 **Casticod** Highly Voted 1 month, 2 weeks ago

Tested

option 1 contoso@221018.onmicrosoft.com and eastcontoso@221018.onmicrosoft.com

Option 2 contoso@221018.onmicrosoft.com only

upvoted 11 times

 **mhmyz** Most Recent 3 weeks, 3 days ago

"No Service Selected" is completed step1 but incomplete step2.

<https://learn.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide>

upvoted 1 times

**DRAG DROP**

You have a Microsoft 365 subscription.

You need to review reports to identify the following:

- The storage usage of files stored in Microsoft Teams
- The number of active users per team

Which report should you review for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Report	Requirements
The device usage report in Teams	
The OneDrive usage report	The storage usage of files stored in Microsoft Teams: <input type="text"/>
The SharePoint site usage report	
The Teams usage report in Teams	Number of active users per Microsoft Team: <input type="text"/>
The User activity report in Teams	

Requirements
Correct Answer: The storage usage of files stored in Microsoft Teams: <input type="text"/> The SharePoint site usage report
Number of active users per Microsoft Team: <input type="text"/> The User activity report in Teams

  **Casticod** Highly Voted 1 month, 2 weeks ago

First option: correct  
Second option Teams usage report  
Should be the number of active users of a team is shown in the team activity report. User report gives user activity  
upvoted 9 times

  **Blagojche** Most Recent 2 weeks ago

Teams Usage provides the report of active users (including guests) per Team, check in M365 Admin Center, Reports, Usage, Microsoft Teams, Teams Usage  
upvoted 1 times

**HOTSPOT**

You work at a company named Contoso, Ltd.

Contoso has a Microsoft 365 subscription that is configured to use the DNS domains shown in the following table.

Name	Can enroll devices
Contoso.com	Yes
Contoso.onmicrosoft.com	Yes

Contoso purchases a company named Fabrikam, Inc.

Contoso plans to add the following domains to the Microsoft 365 subscription:

- fabrikam.com
- east.fabrikam.com
- west.contoso.com

You need to ensure that the devices in the new domains can register by using Autodiscover.

How many domains should you verify, and what is the minimum number of enterprise registration DNS records you should add? To answer, select the appropriate options in the answer area.

**Answer Area**

Domains:

1
2
3

Enterprise registration DNS records:

1
2
3

## Answer Area

Domains:

1
2
3

Correct Answer:

Enterpriseregistration DNS records:

1
2
3

cb0900 Highly Voted 1 month ago

1. 1 domain. Sub-domains don't need to be verified, so just fabrikam.com.
2. 3 Enterpriseregistration DNS records.

<https://www.examtopics.com/discussions/microsoft/view/51183-exam-ms-100-topic-4-question-48-discussion/>  
upvoted 5 times

Darekms0 Most Recent 1 week ago

<https://www.examtopics.com/discussions/microsoft/view/51183-exam-ms-100-topic-4-question-48-discussion/>  
upvoted 2 times

Greatone1 1 week, 4 days ago

Should be 1 and second is 3  
upvoted 2 times

Question #137

Topic 1

You have a Microsoft 365 E5 subscription.

You need to recommend a solution for monitoring and reporting application access. The solution must meet the following requirements:

- Support KQL for querying data.
- Retain report data for at least one year.

What should you include in the recommendation?

- A. a security report in Microsoft 365 Defender
- B. Endpoint analytics
- C. Microsoft 365 usage analytics
- D. Azure Monitor workbooks

Correct Answer: D

Momskii 1 month ago

Selected Answer: D

D. Azure Monitor workbooks allow you to create custom dashboards and reports using KQL queries and provide the flexibility to monitor various aspects of your applications and infrastructure, including application access. Azure Monitor also offers the ability to retain data for extended periods, making it suitable for meeting the one-year data retention requirement.

upvoted 3 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

You need to configure a group naming policy.

Which portal should you use, and to which types of groups will the policy apply? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area****Portal:**

- The Microsoft 365 admin center
- The Microsoft 365 Defender portal
- The Microsoft Entra admin center
- The Microsoft Purview compliance portal

**Group types:**

- Microsoft 365 only
- Security only
- Security and mail-enabled security only
- Microsoft 365 and distribution only
- Microsoft 365, mail-enabled security, and distribution only
- Security, Microsoft 365, mail-enabled security, and distribution

**Answer Area****Portal:**

- The Microsoft 365 admin center
- The Microsoft 365 Defender portal
- The Microsoft Entra admin center**
- The Microsoft Purview compliance portal

**Correct Answer:****Group types:**

- Microsoft 365 only**
- Security only
- Security and mail-enabled security only
- Microsoft 365 and distribution only
- Microsoft 365, mail-enabled security, and distribution only
- Security, Microsoft 365, mail-enabled security, and distribution

  **Casticod** 1 month, 1 week ago

Correct

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-quickstart-naming-policy>

upvoted 3 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type	Security enabled	Role assignments allowed
Group1	Microsoft 365	No	No
Group2	Microsoft 365	No	No
Group3	Security	Yes	Yes
Group4	Security	Yes	No
Group5	Security	Yes	No
Group6	Distribution	No	No

Which groups can be members of Group1 and Group4? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Group1:

- None of the groups
- Group2 only
- Group2 and Group4 only
- Group2, Group4, Group5, and Group6 only
- Group2, Group3, Group4, Group5, and Group6

Group4:

- None of the groups
- Group5 only
- Group3 and Group5 only
- Group1, Group2, Group3, and Group5 only
- Group1, Group2, Group3, Group5, and Group6

**Answer Area**

Group1:

- None of the groups
- Group2 only
- Group2 and Group4 only
- Group2, Group4, Group5, and Group6 only
- Group2, Group3, Group4, Group5, and Group6

Correct Answer:

Group4:

- None of the groups
- Group5 only
- Group3 and Group5 only
- Group1, Group2, Group3, and Group5 only
- Group1, Group2, Group3, Group5, and Group6

 **flim322** 1 month ago

Group 4: Group 5 only  
For the role role-assignable groups, group nesting isn't supported. A group can't be added as a member of a role-assignable group.  
upvoted 1 times

 **cb0900** 1 month ago

Group 1: None (M365 can only contain users).  
Group 4: Group 3 and group 5.

Tested group 4 scenario in a lab as well.

upvoted 3 times

 **vercracked\_007** 1 month ago

Tested this.  
Group 4: Group 3 and 5 Only

Even if a role is linked to the group. It can be a member of another group.

upvoted 4 times

 **vercracked\_007** 1 month ago

The other way around wont work. Group 4 cant be a member of group 5  
upvoted 1 times

 **vercracked\_007** 1 month ago

Sorry, group 3  
upvoted 1 times

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that includes the users shown in the following table.

Name	Usage location	Membership
User1	United States	Group1, Group2
User2	Not set	Group2
User3	Not set	Group1
User4	Canada	Group1

Group2 is a member of Group1.

You assign a Microsoft Office 365 Enterprise E3 license to Group1.

How many Office 365 E3 licenses are assigned?

- A. 1
- B. 2
- C. 3
- D. 4

**Correct Answer: C**

 **Darekms0** 1 week ago

**Selected Answer: C**

<https://www.examtopics.com/discussions/microsoft/view/49561-exam-ms-100-topic-2-question-11-discussion/>  
upvoted 2 times

 **cb0900** 1 month ago

**Selected Answer: C**

When Azure AD assigns group licenses, any users without a specified usage location inherit the location of the directory.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-groups-resolve-problems#usage-location-isnt-allowed>

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-groups-assign>  
upvoted 4 times

 **JensV** 1 month ago

C is correct. User 3 inherits the tenant default location.

User 2 gets no license because group in group is not supported.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced#limitations-and-known-issues>

upvoted 2 times

 **Lud0** 1 month ago

**Selected Answer: B**

Usage location is mandatory to affect license.

upvoted 2 times

 **Lud0** 1 month, 1 week ago

Answer should be B: 2.

Usage location is mandatory to affect license :

Some Microsoft services aren't available in all locations because of local laws and regulations. Before you can assign a license to a user, you must specify the Usage location property for the user.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-groups-resolve-problems#usage-location-isnt-allowed>  
upvoted 2 times

**HOTSPOT**

You have a Microsoft 365 subscription that contains the administrative units shown in the following table.

Name	Members
AU1	Group1, User2
AU2	Group2, User3, User4

The groups contain the members shown in the following table.

Name	Members
Group1	User1
Group2	User2, User4

The users are assigned the roles shown in the following table.

Name	Role	Scope
User1	None	Not applicable
User2	Password Administrator	AU1
User3	License Administrator	Organization
User4	None	Not applicable

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User2 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>
User2 can reset the password of User4.	<input type="radio"/>	<input type="radio"/>
User3 can assign licenses to User1.	<input type="radio"/>	<input type="radio"/>

**Answer Area**

Statements	Yes	No
User2 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can reset the password of User4.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can assign licenses to User1.	<input checked="" type="radio"/>	<input type="radio"/>

**Correct Answer:**

 cb0900  1 month ago

N - user1 is not a direct member of AU1

N - user 4 is not a member of AU1

Y - user 3 is a license admin for the Org.

Adding a group to an administrative unit brings the group itself into the management scope of the administrative unit, but not the members of the group

<https://learn.microsoft.com/en-us/azure/active-directory/roles/administrative-units#groups>

upvoted 13 times

Question #142

Topic 1

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Reports Reader
User2	Exchange Administrator
User3	User Experience Success Manager

Which users can review the Adoption Score in the Microsoft 365 admin center?

- A. User1 only
- B. User2 only
- C. User1 and User2 only
- D. User1 and User3 only
- E. User1, User2, and User3

**Correct Answer: E**

👤 **Casticod** Highly Voted 1 month, 2 weeks ago

**Selected Answer: E**

Correct <https://learn.microsoft.com/en-us/microsoft-365/admin/adoption/adoption-score?view=o365-worldwide#adoption-score-prerequisites>  
upvoted 5 times

👤 **Greatone1** Most Recent 1 week, 2 days ago

Adoption Score is only available in the Microsoft 365 admin center and can only be accessed by IT professionals who have one of the following roles:

Global Administrator  
Exchange Administrator  
SharePoint Administrator  
Skype for Business Administrator  
Teams Service Administrator  
Teams Communications Administrator  
Global Reader  
Reports Reader  
Usage Summary Reports Reader  
User Experience Success Manager  
Organizational Messages Writer Role

upvoted 2 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type	Role
Group1	Security	Helpdesk Administrator
Group2	Security	None
Group3	Microsoft 365	User Administrator

The subscription contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

In Azure AD, you configure the External collaboration settings as shown in the following exhibit.

## Guest user access

Guest user access restrictions ⓘ

[Learn more](#)

- Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

## Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- Only users assigned to specific admin roles can invite guest users
- No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

[Learn more](#)

## External user leave settings

Allow external users to remove themselves from your organization (recommended) ⓘ

[Learn more](#)

## Collaboration restrictions

- Allow invitations to be sent to any domain (most inclusive)
- Deny invitations to the specified domains
- Allow invitations only to the specified domains (most restrictive)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
User1 can invite guest users.	<input type="radio"/>	<input type="radio"/>
User2 can invite guest users.	<input type="radio"/>	<input type="radio"/>
User3 can invite guest users.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
User1 can invite guest users.	<input type="radio"/>	<input checked="" type="radio"/>
Correct Answer: User2 can invite guest users.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can invite guest users.	<input checked="" type="radio"/>	<input type="radio"/>

 **INSOMEA** Highly Voted 1 month ago

correct

upvoted 5 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

You have an Azure AD tenant named contoso.com that contains the following users:

- Admin1
- Admin2
- User1

Contoso.com contains an administrative unit named AU1 that has no role assignments. User1 is a member of AU1.

You create an administrative unit named AU2 that does NOT have any members or role assignments.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
You can add Admin1 as a member of AU1.	<input type="radio"/>	<input type="radio"/>
You can add User1 as a member of AU2.	<input type="radio"/>	<input type="radio"/>
You can assign Admin2 the User administrator role for AU1.	<input type="radio"/>	<input type="radio"/>

**Answer Area**

Statements	Yes	No
You can add Admin1 as a member of AU1.	<input checked="" type="checkbox"/>	<input type="radio"/>
You can add User1 as a member of AU2.	<input checked="" type="checkbox"/>	<input type="radio"/>
You can assign Admin2 the User administrator role for AU1.	<input type="radio"/>	<input checked="" type="checkbox"/>

✉  **Greatone1** 1 week, 4 days ago

Should be Y,Y,Y  
upvoted 2 times

✉  **cb0900** 1 month ago

Y  
Y  
Y

<https://www.examtopics.com/discussions/microsoft/view/96500-exam-ms-100-topic-3-question-100-discussion/>  
upvoted 4 times

✉  **Paul\_white** 2 weeks ago

THANK YOU BROTHER  
upvoted 1 times

**HOTSPOT**

Your company has a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Security Administrator, Guest Inviter
User3	<i>None</i>
User4	Password Administrator

External collaboration settings have default configuration.

You need to identify which users can perform the following administrative tasks:

- Modify the password protection policy.
- Create guest user accounts.

Which users should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Modify the password protection policy:

User1 only  
User1 and User2 only  
User1, User2, and User4 only  
User1, User2, User3, and User4

Create new guest users in Azure AD:

User1 only  
User1 and User2 only  
User1, User2, and User4 only  
User1, User2, User3, and User4

**Answer Area**

Modify the password protection policy:

User1 only  
User1 and User2 only  
User1, User2, and User4 only  
User1, User2, User3, and User4

**Correct Answer:**

Create new guest users in Azure AD:

User1 only  
User1 and User2 only  
User1, User2, and User4 only  
User1, User2, User3, and User4

 **rfree** 4 weeks, 1 day ago

2. am thinking Users 1, 2 and 4 as 3 has no roles.

A role that allows you to create users in your tenant directory, such as the Global Administrator role or a limited administrator directory role such as Guest Inviter or User Administrator.

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal>

upvoted 1 times

 **JensV** 1 month ago

Also the Security Administrator can "Configure custom banned password list or on-premises password protection." <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator>

And yes with tenant default everyone can invite guests.

1. User 1 and User 2

2. All users

upvoted 2 times

✉️ **Casticod** 1 month, 1 week ago

Try in my lab tenant, Standard user (not assigned rol) to be able to create a Guest user.

upvoted 2 times

✉️ **siulas** 1 month, 1 week ago

1. Correct.

2. All users

<https://www.examtopics.com/discussions/microsoft/view/50897-exam-ms-100-topic-3-question-79-discussion/>

upvoted 3 times

✉️ **siulas** 1 month, 1 week ago

1. User1 and User2 only

2. All users

upvoted 4 times

✉️ **cb0900** 1 month ago

Agree:

1. User 1 and User 2

2. All users

Tested in a lab.

upvoted 2 times

✉️ **Casticod** 1 month, 1 week ago

I think The same

1. User1 and User2 only

2. All users

upvoted 3 times

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Microsoft 365 admin role	Microsoft Exchange Online admin role
User1	Global Administrator	None
User2	Exchange Administrator	None
User3	Service Support Administrator	None
User4	None	Organization Management

You plan to use Exchange Online to manage email for a DNS domain.

An administrator adds the DNS domain to the subscription.

The DNS domain has a status of Incomplete setup.

You need to identify which user can complete the setup of the DNS domain. The solution must use the principle of least privilege.

Which user should you identify?

- A. User1
- B. User2
- C. User3
- D. User4

**Correct Answer:** A

 **Greatone1** 1 week, 4 days ago

Given answer is correct

<https://www.examtopics.com/discussions/microsoft/view/55314-exam-ms-100-topic-3-question-76-discussion/>

upvoted 1 times

 **862e76c** 4 weeks, 1 day ago

Agree with the answer

upvoted 3 times

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Passwordless authentication	Multi-factor authentication (MFA) method registered
User1	Not configured	Microsoft Authenticator app (push notification)
User2	Configured	Microsoft Authenticator app (push notification)
User3	Not configured	Mobile phone
User4	Not configured	Email

You plan to create a Conditional Access policy that will use GPS-based named locations.

Which users can the policy protect?

- A. User2 and User4 only
- B. User1, User2, User3, and User4
- C. User1 only
- D. User1 and User3 only

**Correct Answer:** C

 **faeem** 2 weeks, 6 days ago

Correct. GPS location doesn't work with passwordless authentication methods.

Multiple Conditional Access policies may prompt users for their GPS location before all are applied. Because of the way Conditional Access policies are applied, a user may be denied access if they pass the location check but fail another policy. For more information about policy enforcement, see the article Building a Conditional Access policy.

Important

Users may receive prompts every hour letting them know that Microsoft Entra ID is checking their location in the Authenticator app. The preview should only be used to protect very sensitive apps where this behavior is acceptable or where access needs to be restricted to a specific country/region. Therefore, user 1 has MFA registered app but not setup for passwordless authentication.

upvoted 2 times

 **Vincent1966** 1 month ago

GPS location doesn't work with passwordless authentication methods and when the location condition of a Conditional Access policy is configured, users will be prompted by the Authenticator app to share their GPS location.

upvoted 4 times

## HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Role
User1	Group1	User Administrator
User2	Group1	None
User3	Group2	None
User4	None	Global Administrator

You enable self-service password reset (SSPR) for Group1. You configure security questions as the only authentication method for SSPR.

Which users can use SSPR, and which users must answer security questions to reset their password? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Users that can use SSPR:

- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

Users that must answer security questions to reset their password:

- User1 only
- User2 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

## Answer Area

Users that can use SSPR:

- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, and User4 only**
- User1, User2, User3, and User4

Correct Answer:

Users that must answer security questions to reset their password:

- User1 and User2 only**
- User1, User2, and User3 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

 **Vincent1966** (Highly Voted) 1 month ago

Box 1: 1,2 and 4 - Admins are always enabled for self-service password reset

Box 2: 2 - Admins are required to use two authentication methods to reset their password.

upvoted 5 times

 **vercracked\_007** (Most Recent) 1 month ago

Box 1 - user1 en user 2 only - because member of group 1

Box 2 - User 2 only, User 1 is a admin and needs to use authenticator app or e-mail as well.

upvoted 2 times

 **Casticod** 1 month, 1 week ago

Checking it again, in the second response it should be User1 user2 and user4 Since user 1 and user 4 are administrators and user 2 is a member of the group assigned for SSPR.

By default, administrator accounts are enabled for self-service password reset, and a strong default two-gate password reset policy is enforced. This policy may be different from the one you have defined for your users, and this policy can't be changed. You should always test password reset functionality as a user without any Azure administrator roles assigned.

With a two-gate policy, administrators don't have the ability to use security questions.

The two-gate policy requires two pieces of authentication data, such as an email address, authenticator app, or a phone number.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-password-policy-differences>  
upvoted 2 times

✉️ **Casticod** 1 month, 1 week ago

Sorry error in the responses.

Option 1: User1, user2, and user4 (user 1and 4 by admins, user 2 for group assignement)

Option 2: User 2 Only (the admins can't use the security Questions)

upvoted 3 times

✉️ **Casticod** 1 month, 1 week ago

I think user 1 and 2 for both. If you select a group, only enable SSPR for this group and nested. The rest of users don't have access to SSPR  
upvoted 2 times

✉️ **Casticod** 1 month, 1 week ago

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr#enable-self-service-password-reset>

upvoted 2 times

Question #149

Topic 1

Your network contains an Active Directory forest named contoso.local.

You have a Microsoft 365 subscription.

You plan to implement a directory synchronization solution that will use password hash synchronization.

From the Microsoft 365 admin center, you successfully verify the contoso.com domain name.

You need to prepare the environment for the planned directory synchronization solution.

What should you do first?

- A. From the Microsoft 365 admin center, verify the contoso.local domain name.
- B. From the public DNS zone of contoso.com, add a new mail exchanger (MX) record.
- C. From Active Directory Domains and Trusts, add contoso.com as a UPN suffix.
- D. From Active Directory Users and Computers, modify the UPN suffix for all users.

**Correct Answer: C**

✉️ **DiligentSam** 1 week, 6 days ago

Given Answer is correct

upvoted 1 times

✉️ **spectre786** 1 week, 6 days ago

Could you please comment on all questions from 122 to 236, only when there is no existing comment already ? Thank you for your help.  
upvoted 1 times

✉️ **EM1234** 2 weeks ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide#what-if-i-only-have-a-local-on-premises-domain>

upvoted 1 times

You have a Microsoft 365 ES subscription.

On Monday, you create a new user named User1.

On Tuesday, User1 signs in for the first time and perform the following actions:

- Signs in to Microsoft Exchange Online from an anonymous IP address.
- Signs in to Microsoft SharePoint Online from a device in New York City.
- Establishes Remote Desktop connections to hosts in Berlin and Hong Kong, and then signs in to SharePoint Online from the Remote Desktop connections.

Which types of sign-in risks will Azure AD Identity Protection detect for User1?

- A. anonymous IP address and atypical travel only
- B. anonymous IP address only
- C. unfamiliar sign-in properties and atypical travel only
- D. anonymous IP address and unfamiliar sign-in properties only
- E. anonymous IP address, atypical travel, and unfamiliar sign-in properties

**Correct Answer: B**

✉️  **Demoster** 1 month ago

**Selected Answer: B**

Correct answer. Atypical travel and Unfamiliar sign-in properties have learning period.

The system has an initial learning period of the earliest of 14 days or 10 logins, during which it learns a new user's sign-in behavior.

upvoted 3 times

✉️  **JensV** 1 month ago

B is correct as the other two indicators are still in learning mode for a newly created user

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#atypical-travel>  
The system has an initial learning period of the earliest of 14 days or 10 logins, during which it learns a new user's sign-in behavior.

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#unfamiliar-sign-in-properties>  
Newly created users are in "learning mode" period where the unfamiliar sign-in properties risk detection is turned off while our algorithms learn the user's behavior.

upvoted 1 times

✉️  **vercracked\_007** 1 month ago

should be E

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#risk-types-and-detection>  
upvoted 2 times

✉️  **vercracked\_007** 1 month, 1 week ago

Should be A i think

upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Group	MFA Status
User1	Group1	Enabled
User2	Group1, Group2	Enforced

You have the named locations shown in the following table.

Named location	IP range
Montreal	133.107.0.0/16
Toronto	193.77.10.0/24

You create a conditional access policy that has the following configurations:

- Users or workload identities:
  - Include: Group1
  - Exclude: Group2
- Cloud apps or actions: Include all cloud apps
- Conditions:
  - Include: Any location
  - Exclude: Montreal
- Access control: Grant access, Require multi-factor authentication

User1 is on the multi-factor authentication (MFA) blocked users list.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	<input type="radio"/>	<input type="radio"/>
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	<input type="radio"/>	<input type="radio"/>

**Answer Area**

**Correct Answer:**

- Statements
- User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.
- User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.
- User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.

Yes	No
<input checked="" type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>

**Darekms0** 18 hours, 58 minutes ago

<https://www.examtopics.com/discussions/microsoft/view/55435-exam-ms-100-topic-4-question-36-discussion/> NNY  
upvoted 1 times

 **netbw** 2 weeks, 2 days ago

Answer is correct. User1 can connect from Montreal.  
upvoted 1 times

 **BlackCat9588** 3 weeks, 3 days ago

NNY?  
MFA of user1 is blocked  
upvoted 1 times

 **BlackCat9588** 3 weeks, 2 days ago

Exclude: Montreal  
upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	
User1	Group1	Microsoft Authenticator app (push notification)
User2	Group2	Microsoft Authenticator app (push notification)
User3	Group1, Group2	None

Each user has an Android device with the Microsoft Authenticator app installed and has set up phone sign-in.

The subscription has the following Conditional Access policy:

- Name: Policy1
- Assignments
- Users and groups: Group1, Group2
- Cloud apps or actions: All cloud apps
- Access controls
- Grant: Require multi-factor authentication
- Enable policy: On

From Microsoft Authenticator settings for the subscription, the Enable and Target settings are configured as shown in the exhibit. (Click the Exhibit tab.)

# Microsoft Authenticator settings

...

X

**i** Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting 27th of February 2023. [Learn more](#)

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. [Learn more](#).

**Enable and Target**    [Configure](#)

Enable

**Include**    [Exclude](#)

Target  All users  Select groups

[Add groups](#)

Name	Type	Registration	Authentication mode	
Group1	Group	Optional	Passwordless	<input type="button"/>
Group2	Group	Optional	Passwordless	<input type="button"/>

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
User1 can sign in by using number matching in the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>
User2 can sign in by using a username and password.	<input type="radio"/>	<input type="radio"/>
User3 can sign in by using number matching in the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>

## Answer Area

Statements	Yes	No
User1 can sign in by using number matching in the Microsoft Authenticator app.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in by using a username and password.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can sign in by using number matching in the Microsoft Authenticator app.	<input type="radio"/>	<input checked="" type="radio"/>

## Correct Answer:

 **MarkusSan** 1 week, 2 days ago

Answer look correct to me

upvoted 1 times

 **Harau** 1 week, 4 days ago

YYN

User 2 can use username and password, since passwordless is optional

upvoted 1 times

 **MarkusSan** 1 week, 2 days ago

User 2 cannot use username and password only, because of Conditional Access Policy 1: Grant, require MFA for Group1 and Group2

upvoted 2 times

Question #153

Topic 1

HOTSPOT

You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Report Reader
User2	User Administrator
User3	Security Administrator
User4	Global Administrator

From the Sign-ins blade of the Microsoft Entra admin center, for which users can User1 and User2 view the sign-ins? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

User1 can view the sign-ins for the following users:

- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

User2 can view the sign-ins for the following users:

- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

#### Answer Area

User1 can view the sign-ins for the following users:

- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4**

#### Correct Answer:

User2 can view the sign-ins for the following users:

- User1 only**
- User1 and User2 only**
- User1, User2, and User3 only
- User1, User2, User3, and User4

 **cb0900** Highly Voted  1 month ago

User 1 - can view sign-in logs for user 1, user 2, user3, and user4. Correct

User 2 - can only view sign-in logs for user2. This isn't listed as a possible answer, suspect the options are slightly wrong.

<https://www.examtopics.com/discussions/microsoft/view/60216-exam-ms-100-topic-4-question-50-discussion/>

<https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-access-activity-logs>

upvoted 6 times

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com.

Corporate policy states that user passwords must not include the word Contoso.

What should you do to implement the corporate policy?

- A. From the Microsoft Entra admin center, create a conditional access policy.
- B. From the Microsoft Entra admin center, configure the Password protection settings.
- C. From the Microsoft 365 admin center, configure the Password policy settings.
- D. From Azure AD Identity Protection, configure a sign-in risk policy.

**Correct Answer: B**

 **DiligentSam** 3 weeks, 1 day ago

<https://www.examtopics.com/discussions/microsoft/view/45311-exam-ms-100-topic-3-question-66-discussion/>  
upvoted 3 times

 **GLL** 3 weeks, 2 days ago

correct  
upvoted 1 times

 **CloudCanary** 3 weeks, 2 days ago

**Selected Answer: B**

Correct

<https://learn.microsoft.com/es-es/azure/active-directory/authentication/tutorial-configure-custom-password-protection>  
upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- User passwords must be 10 characters or more.

Solution: Implement pass-through authentication and modify the password settings from the Default Domain Policy in Active Directory.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

 **Paul\_white** 2 weeks ago

ANSWER IS B !!!!!!

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- User passwords must be 10 characters or more.

Solution: Implement password hash synchronization and configure password protection in the Azure AD tenant.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

 **Hard1k** Highly Voted 1 month ago

**Selected Answer: A**

s, the solution meets the goal.

Password hash synchronization synchronizes user password hashes from Active Directory to Azure AD. This allows users to authenticate to Microsoft 365 services even if Active Directory is unavailable.

Password protection in Azure AD allows you to configure password requirements, such as minimum length and complexity. You can also use password protection to block specific words or phrases from being used in passwords.

By implementing password hash synchronization and configuring password protection in the Azure AD tenant, you can meet the following requirements:

Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.  
User passwords must be 10 characters or more.

upvoted 9 times

 **Milad666** 1 week, 2 days ago

WRONG! User that syncronized with PHS will just inherit Policies and attributes from Active Directory. So Solution dosnt meet the goal.  
upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- User passwords must be 10 characters or more.

Solution: Implement pass-through authentication and configure password protection in the Azure AD tenant.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: B**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- User passwords must be 10 characters or more.

Solution: Implement password hash synchronization and modify the password settings from the Default Domain Policy in Active Directory.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: A**

 **Vincent1966** 1 month ago

The Default Domain Policy should only set the following: Password Policy. Domain Account Lockout Policy. Domain Kerberos Policy  
upvoted 1 times

**HOTSPOT**

You have a hybrid deployment of Azure AD that contains the users shown in the following table.

Name	Description
User1	Azure AD Connect sync account
User2	Contributor for Azure AD Connect Health
User3	Application administrator in Azure AD

You need to identify which users can perform the following tasks:

- View sync errors in Azure AD Connect Health.
- Configure Azure AD Connect Health settings.

Which user should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

**View sync errors in Azure AD Connect Health:**

A dropdown menu containing three options: User1, User2, and User3. The menu has a small downward arrow icon at the top right corner.

**Configure Azure AD Connect Health settings:**

A dropdown menu containing three options: User1, User2, and User3. The menu has a small downward arrow icon at the top right corner.

**Answer Area**

**View sync errors in Azure AD Connect Health:**

A dropdown menu containing three options: User1, User2, and User3. The User2 option is highlighted with a black rectangular box and a white circle inside it.

**Correct Answer:**

**Configure Azure AD Connect Health settings:**

A dropdown menu containing three options: User1, User2, and User3. The User1 option is highlighted with a black rectangular box and a white circle inside it.

 **cb0900**  1 month ago

View sync errors - user 2

Configure AADConnect - user 2

<https://www.examtopics.com/discussions/microsoft/view/83065-exam-ms-100-topic-3-question-88-discussion/>

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-health-operations>

upvoted 7 times

Question #160

*Topic 1*

Your company has three main offices and one branch office. The branch office is used for research.

The company plans to implement a Microsoft 365 tenant and to deploy multi-factor authentication.

You need to recommend a Microsoft 365 solution to ensure that multi-factor authentication is enforced only for users in the branch office.

What should you include in the recommendation?

- A. Azure AD password protection
- B. a Microsoft Intune device configuration profile
- C. a Microsoft Intune device compliance policy
- D. Azure AD conditional access

**Correct Answer:** D

 **DiligentSam** 1 week, 6 days ago

correct

upvoted 1 times

 **Paul\_white** 2 weeks ago

D IS VERIFIED CORRECT !!!!

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain.

You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD.

Solution: From Azure AD Connect, you modify the filtering settings.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

✉  **jt2214** 5 days, 13 hours ago

**Selected Answer: A**

<https://www.examtopics.com/discussions/microsoft/view/59313-exam-ms-100-topic-3-question-22-discussion/>  
upvoted 1 times

✉  **Paul\_white** 2 weeks ago

ANSWER IS A !!!!!

upvoted 1 times

✉  **Sas2003** 3 weeks, 4 days ago

**Selected Answer: A**

No error just remove filtering or U exclusion  
upvoted 1 times

✉  **jakke91** 4 weeks, 1 day ago

A indeed

<https://www.examtopics.com/discussions/microsoft/view/59313-exam-ms-100-topic-3-question-22-discussion/>  
upvoted 2 times

✉  **vercracked\_007** 1 month ago

Should this nog be A?

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-sync-configure-filtering>  
upvoted 3 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	None

You create an administrative unit named AU1 that contains the members shown in the following exhibit.

**AU1**

[Members](#)    [Role assignments](#)

Add users and groups, or select and remove them. The administrators assigned to this unit will manage these users and groups. Adding groups doesn't add users to the unit, it lets the assigned admins manage group settings.

Add users	Add groups	Upload users	...	Filter	Search this list	
<input type="checkbox"/> Members	Email address	Last sign-in	Member type			
<input type="checkbox"/> User1	User1@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:25 PM	User			
<input type="checkbox"/> User3	User3@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:27 PM	User			

The User Administrator role has the assignments shown in the following exhibit.

## User Administrator

Run As

General Assigned Permissions

You can assign this role to users and groups, and select users and groups to remove or manage them.

[Learn more about assigning admin roles](#)

Add users Add groups

<input type="checkbox"/>	Admin name	Last sign-in	Scope <a href="#">(i)</a>
<input type="checkbox"/>	<b>Group1</b>	Unavailable for groups	Organization
<input type="checkbox"/>	<b>Group2</b>	Unavailable for groups	AU1

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
User1 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>
User2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>
User2 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
User1 can reset the password of User3.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can reset the password of User3.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>

Correct Answer:

**VikC** 4 days, 10 hours ago

Y/Y/N

User Administrator Cannot change the credentials or reset MFA for members and owners of a role-assignable group, and User2 is a member of a role assigned group.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#user-administrator>  
upvoted 1 times

✉️ **Ranger\_DanMT** 2 weeks, 2 days ago

I think this is the correct answer, the only "no" answer would be if User 3 could reset the password of user 1 or user 2.  
upvoted 1 times

Question #163

Topic 1

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant includes a user named User1.

You enable Azure AD Identity Protection.

You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege.

To which role should you add User1?

- A. Security Reader
- B. Global Administrator
- C. Owner
- D. User Administrator

**Correct Answer: A**

✉️ **Paul\_white** 2 weeks ago

SECURITY READER  
upvoted 1 times

✉️ **DiligentSam** 3 weeks, 4 days ago

Should be A  
upvoted 1 times

✉️ **cb0900** 1 month ago

**Selected Answer: A**

<https://www.examtopics.com/discussions/microsoft/view/49685-exam-ms-100-topic-3-question-29-discussion/>

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#permissions>  
upvoted 1 times

**HOTSPOT**

Your company has an Azure AD tenant named contoso.onmicrosoft.com that contains the users shown in the following table.

Name	Role
User1	Password Administrator
User2	Security Administrator
User3	User Administrator
User4	None

You need to identify which users can perform the following administrative tasks:

- Reset the password of User4.
- Modify the value for the manager attribute of User4.

Which users should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Reset the password of User4:

User1 only  
User2 only  
User1 and User2 only  
User1 and User3 only  
User1, User2, and User3

Modify the value for the manager attribute of User4:

User2 only  
User3 only  
User1 and User3 only  
User2 and User3 only  
User1, User2, and User3

## Answer Area

Reset the password of User4:

A dropdown menu with the following options:  
User1 only  
User2 only  
User1 and User2 only  
**User1 and User3 only**  
User1, User2, and User3

Correct Answer:

Modify the value for the manager attribute of User4:

A dropdown menu with the following options:  
User2 only  
**User3 only**  
User1 and User3 only  
User2 and User3 only  
User1, User2, and User3

cb0900 1 month ago

Answers are correct.

Reset pwd of User4: User1 and User3

Modify value or User4: User3

<https://www.examtopics.com/discussions/microsoft/view/53490-exam-ms-100-topic-3-question-62-discussion/>

upvoted 1 times

Question #165

Topic 1

You have a Microsoft 365 E5 subscription.

Users have Android or iOS devices and access Microsoft 365 resources from computers that run Windows 11 or MacOS.

You need to implement passwordless authentication. The solution must support all the devices.

Which authentication method should you use?

- A. Windows Hello
- B. FIDO2 compliant security keys
- C. Microsoft Authenticator app

Correct Answer: C

DiligentSam 3 weeks, 4 days ago

I think The MS recommand MFA by using Authenticator App

upvoted 1 times

cb0900 1 month ago

**Selected Answer: C**

Agree with C. Authenticator App.

B would work too. I guess as they mention Android and iOS they're looking for the app as an answer.

<https://www.examtopics.com/discussions/microsoft/view/81291-exam-ms-100-topic-5-question-73-discussion/>

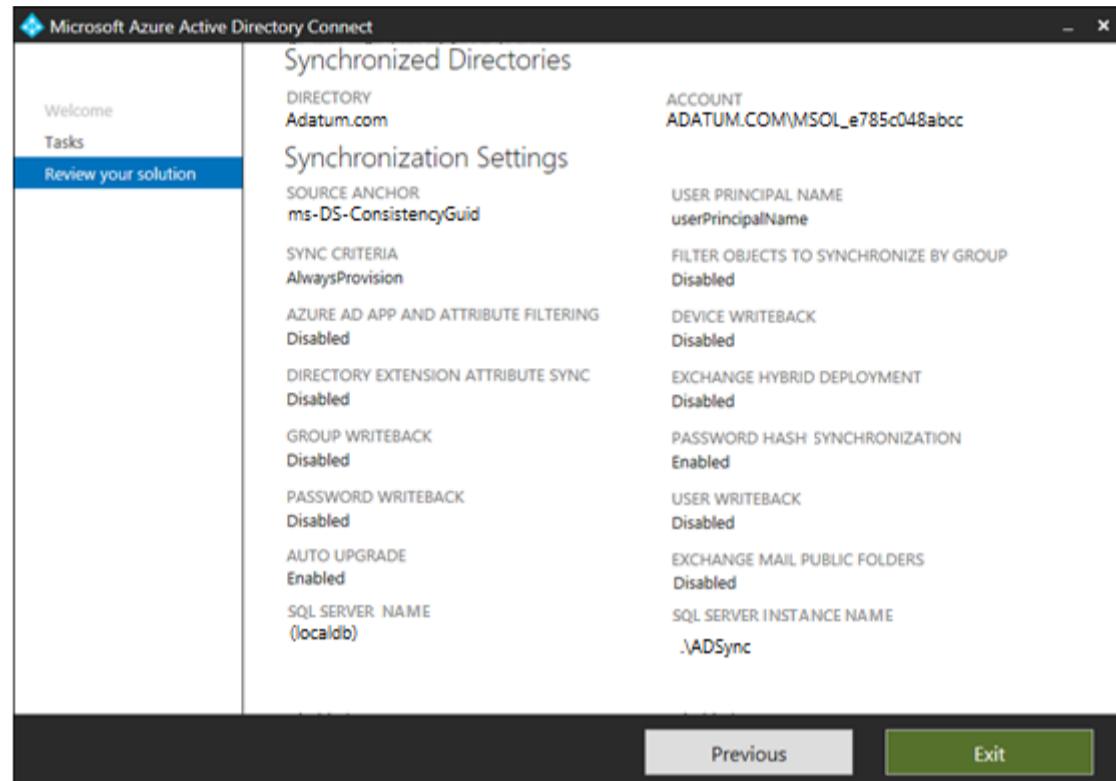
upvoted 3 times

## HOTSPOT

Your company has a hybrid deployment of Microsoft 365.

An on-premises user named User1 is synced to Azure AD.

Azure AD Connect is configured as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

## Answer Area

User1 [answer choice].

▼  
cannot change her password from any Microsoft portals  
can change her password by using self-service password reset feature only  
can change her password from the Microsoft 365 admin center only

If the password for User1 is changed in Active Directory, [answer choice].

▼  
the password hash will be synchronized to Azure AD  
a new randomly generated password will be assigned to User1  
the password hash in Azure AD will be unchanged

## Answer Area

User1 [answer choice].

▼  
cannot change her password from any Microsoft portals  
can change her password by using self-service password reset feature only  
can change her password from the Microsoft 365 admin center only

## Correct Answer:

If the password for User1 is changed in Active Directory, [answer choice].

▼  
the password hash will be synchronized to Azure AD  
a new randomly generated password will be assigned to User1  
the password hash in Azure AD will be unchanged

OliverCiecwierz 1 month ago

Answer is correct.

1. No mention of SSPR or whether the user is able to access admin center.

2. Hash from on-prem will sync to Azure AD

<https://oxfordcomputertraining.com/glossary/what-is-password-hash-synchronization/>

upvoted 3 times

Paul\_white 2 weeks ago

GIVEN ANSWER IS VERY CORRECT !!!!!!

upvoted 1 times



**HOTSPOT**

- You have a Microsoft 365 E5 subscription and an Azure AD tenant named contoso.com.

All users have computers that run Windows 11, are joined to contoso.com, and are protected by using BitLocker Drive Encryption (BitLocker).

You plan to create a user named Admin1 that will perform following tasks:

- View BitLocker recovery keys.
- Configure the usage location for the users in contoso.com.

You need to assign roles to Admin to meet the requirements. The solution must use the principle of least privilege.

Which two roles should you assign? To answer, select the appropriate options in the answer area.

## Answer Area

### Devices

- Cloud Device Administrator ⓘ
- Desktop Analytics Administrator ⓘ
- Intune Administrator ⓘ
- Printer Administrator ⓘ
- Printer Technician ⓘ
- Windows 365 Administrator ⓘ

### Global

- Global Administrator ⓘ

### Identity

- Application Administrator ⓘ
- Application Developer ⓘ
- Authentication Administrator ⓘ
- Cloud Application Administrator ⓘ
- Conditional Access Administrator ⓘ
- Domain Name Administrator ⓘ
- External Identity Provider Administrator ⓘ
- Guest Inviter ⓘ
- Helpdesk Administrator ⓘ
- Hybrid Identity Administrator ⓘ
- License Administrator ⓘ
- Password Administrator ⓘ

## Answer Area

### Devices

- Cloud Device Administrator ⓘ
- Desktop Analytics Administrator ⓘ
- Intune Administrator ⓘ
- Printer Administrator ⓘ
- Printer Technician ⓘ
- Windows 365 Administrator ⓘ

### Global

- Global Administrator ⓘ

### Identity

- Application Administrator ⓘ
- Application Developer ⓘ
- Authentication Administrator ⓘ
- Cloud Application Administrator ⓘ
- Conditional Access Administrator ⓘ
- Domain Name Administrator ⓘ
- External Identity Provider Administrator ⓘ
- Guest Inviter ⓘ
- Helpdesk Administrator ⓘ
- Hybrid Identity Administrator ⓘ
- License Administrator ⓘ
- Password Administrator ⓘ

Correct Answer:

✉️  **DiligentSam** 3 weeks, 4 days ago

correct

upvoted 1 times

✉️  **OliwerCiecwierz** 1 month ago

Answer is correct as Helpdesk Administrator has action of: microsoft.directory/bitlockerKeys/key/read - Read bitlocker metadata and key on devices

and License Administrator has:

microsoft.directory/users/usageLocation/update - Update usage location of users

upvoted 3 times

**HOTSPOT**

You have a Microsoft 365 Enterprise E5 subscription.

You add a cloud-based app named App1 to the Azure AD enterprise applications list.

You need to ensure that two-step verification is enforced for all user accounts the next time they connect to App1.

Which three settings should you configure from the policy? To answer, select the appropriate settings in the answer area,

NOTE: Each correct selection is worth one point.

**Answer Area****New**

...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more](#)

**Name \***

App1 policy

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.  
[Learn more](#)

**What does this policy apply to?**

Users and groups

**Include** None All users Select users and groups**Assignments**Users or workload identities (i)

All users

Cloud apps or actions (i)

No cloud apps, actions, or authentication contexts selected

Conditions (i)

0 conditions selected

**⚠** Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

**Access controls**Grant (i)

0 controls selected

Session (i)

0 controls selected

**Enable policy**

Report-only

On

Off

## Answer Area

### New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more](#)

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.  
[Learn more](#)

Name \*

App1 policy

What does this policy apply to?

Users and groups

Include Exclude

None

All users

Select users and groups

Correct Answer:

Assignments

Users or workload identities ⓘ  
All users

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

⚠ Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Enable policy

Report-only  On Off

cb0900 1 month ago

The given answer is correct:

1. Add the app in Cloud Apps
2. Require MFA in Grant
3. Enable the policy

upvoted 1 times

You have a Microsoft 365 E5 subscription.

You create a Conditional Access policy that blocks access to an app named App1 when users trigger a high-risk sign-in event.

You need to reduce false positives for impossible travel when the users sign in from the corporate network.

What should you configure?

- A. exclusion groups
- B. multi-factor authentication (MFA)
- C. named locations
- D. user risk policies

**Correct Answer: C**

 **862e76c** 4 weeks, 1 day ago

Agree with the answer

upvoted 2 times

You have a Microsoft 365 E5 subscription.

You need to create a mail-enabled contact.

Which portal should you use?

- A. the Microsoft 365 admin center
- B. the SharePoint admin center
- C. the Microsoft Entra admin center
- D. the Microsoft Purview compliance portal

**Correct Answer: C**

 **Demonster** Highly Voted  1 month ago

**Selected Answer: A**

<https://admin.microsoft.com/Adminportal/Home#/Contact>

upvoted 6 times

 **Darekms0** Most Recent  6 days, 23 hours ago

**Selected Answer: A**

A definitely

upvoted 2 times

 **Vincent1966** 1 month ago

A: <https://admin.microsoft.com/#/Contact>

upvoted 4 times

 **vercracked\_007** 1 month, 1 week ago

Should be A

upvoted 4 times

**HOTSPOT**

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Billing Administrator
User3	None

You enable self-service password reset for all users. You set Number of methods required to reset to 1, and you set Methods available to users to Security questions only.

What information must be configured for each user before the user can perform a self-service password reset? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User1:

Email address only  
Phone number only  
Security questions only  
Phone number and email address

User2:

Email address only  
Phone number only  
Security questions only  
Phone number and email address

User3:

Email address only  
Phone number only  
Security questions only  
Phone number and email address

## Answer Area

User1:

- Email address only
- Phone number only
- Security questions only
- Phone number and email address**

User2:

Correct Answer:

- Email address only
- Phone number only
- Security questions only
- Phone number and email address**

User3:

- Email address only
- Phone number only
- Security questions only**
- Phone number and email address

 **Casticod** 1 month, 1 week ago

Correct

By default, administrator accounts are enabled for self-service password reset, and a strong default two-gate password reset policy is enforced. This policy may be different from the one you have defined for your users, and this policy can't be changed. You should always test password reset functionality as a user without any Azure administrator roles assigned.

With a two-gate policy, administrators don't have the ability to use security questions.

The two-gate policy requires two pieces of authentication data, such as an email address, authenticator app, or a phone number.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-password-policy-differences>  
upvoted 4 times

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 E5 subscription.

You plan to implement a hybrid configuration that has the following requirements:

- Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources
- Supports the use of Azure AD Identity Protection

You need to configure Azure AD Connect to support the planned implementation.

Which two options should you select? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Password Hash Synchronization
- B. Password writeback
- C. Directory extension attribute sync
- D. Enable single sign-on
- E. Pass-through authentication

**Correct Answer: AD**

✉️  **Paul\_white** 2 weeks ago

ANSWER IS A & D

upvoted 2 times

✉️  **Vincent1966** 1 month ago

A and C: Best practice: Turn on password hash synchronization.

Detail: Password hash synchronization is a feature used to sync user password hashes from an on-premises Active Directory instance to a cloud-based Azure AD instance. This sync helps to protect against leaked credentials being replayed from previous attacks.

<https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices>

upvoted 1 times

✉️  **Vincent1966** 1 month ago

Must be A and D: SSO

upvoted 8 times

**HOTSPOT**

Your network contains an Active Directory domain and an Azure AD tenant.

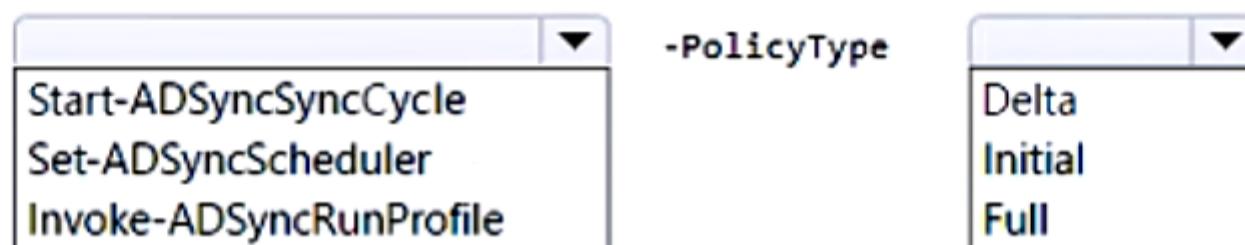
You implement directory synchronization for all 10,000 users in the organization.

You automate the creation of 100 new user accounts.

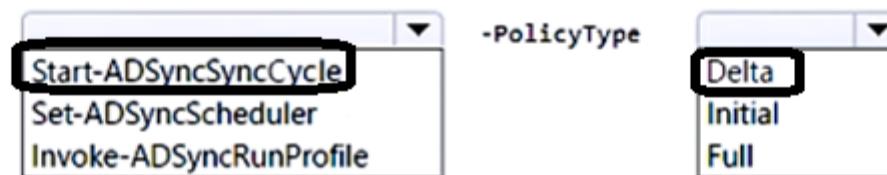
You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.

Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area****Answer Area**

Correct Answer:



✉ **Paul\_white** 2 weeks ago

ANSWER IS CORRECT

upvoted 1 times

✉ **DiligentSam** 3 weeks, 4 days ago

It's correct

I often type this cmdlet. trust me

upvoted 2 times

✉ **cb0900** 1 month ago

Answer is correct.

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-sync-feature-scheduler>

upvoted 2 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Passwordless capable	Multi-factor authentication (MFA) method registered
User1	Group1	Capable	Microsoft Authenticator app (push notification)
User2	Group2	Capable	Microsoft Authenticator app (push notification)
User3	Group1, Group2	Capable	Mobile phone, Windows Hello for Business

Each user has a device with the Microsoft Authenticator app installed.

From Microsoft Authenticator settings for the subscription, the Enable and Target settings are configured as shown in the exhibit. (Click the Exhibit tab.)

## Microsoft Authenticator settings

X

**i** Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting 27th of February 2023. [Learn more](#)

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. [Learn more](#).

**Enable and Target**   [Configure](#)

Enable

**Include**   [Exclude](#)

Target  All users  Select groups

[Add groups](#)

Name	Type	Registration	Authentication mode
Group1	Group	Optional	Passwordless <input checked="" type="button"/> X

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
User1 can use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>
User2 can use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>
User3 can use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>

## Answer Area

Statements	Yes	No
User1 can use number matching during sign-in.	<input checked="" type="checkbox"/>	<input type="radio"/>
User2 can use number matching during sign-in.	<input type="radio"/>	<input checked="" type="checkbox"/>
User3 can use number matching during sign-in.	<input type="radio"/>	<input checked="" type="checkbox"/>

✉  **netbw** 2 weeks, 2 days ago

1 - Y (registered and in scope)  
2 - N (out of scope)  
3 - N (unregistered but in scope)  
upvoted 2 times

✉  **faeem** 3 weeks, 2 days ago

Agree with 1 - Y, 3 - N and 2, is part of group two. The scoping is only for Group one to use passwordless auth mode. So I would go with 2 - N.  
upvoted 1 times

✉  **jt2214** 3 weeks, 3 days ago

I think answer is correct. User 2 is not in group 1 for passwordless. Thoughts?  
upvoted 1 times

✉  **ExamCheater1993** 3 weeks, 4 days ago

Shouldn't this be YYN ?  
upvoted 2 times

**HOTSPOT****Overview**

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named A. Datum Corporation.

**Environment****On-Premises Environment**

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins, Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

**Cloud Environment**

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure AD Premium P2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

- Password hash synchronization is enabled.
- Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk Administrator
Admin3	Security Administrator
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.

The Azure AD tenant has Security defaults enabled.

## Problem Statements

-  
Litware identifies the following issues:

- Admin1 cannot create conditional access policies.
- Admin4 receives an error when attempting to use SSPR.
- Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

## Requirements

## Planned Changes

-  
Litware plans to implement the following changes:

- Implement Microsoft Intune.
- Implement Microsoft Teams.
- Implement Microsoft Defender for Office 365.
- Ensure that users can install Office 365 apps on their device.
- Convert all the Windows 10 Pro devices to Windows 10 Enterprise ES.
- Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

## Technical Requirements

-  
Litware identifies the following technical requirements:

- Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
- Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
- Litware users must be able to invite A. Datum users to participate in the following activities:
  - Join Microsoft Teams channels.
  - Join Microsoft Teams chats.
  - Access shared files.
- Just in time access to critical administrative roles must be required.
- Microsoft 365 incidents and advisories must be reviewed monthly.
- Office 365 service status notifications must be sent to Admin2.
- The principle of least privilege must be used.

You need to ensure that the Microsoft 365 incidents and advisories are reviewed monthly.

Which users can review the incidents and advisories, and which blade should the users use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Users:	<ul style="list-style-type: none"><li>Admin1 only</li><li>Admin1 and Admin3 only</li><li>Admin1, Admin2, and Admin3 only</li><li>Admin1, Admin2, Admin3, and Admin4</li></ul>
Blade:	<ul style="list-style-type: none"><li>Reports</li><li>Service Health</li><li>Message center</li></ul>

**Answer Area**

**Correct Answer:**

Users:	<ul style="list-style-type: none"><li>Admin1 only</li><li><b>Admin1 and Admin3 only</b></li><li>Admin1, Admin2, and Admin3 only</li><li>Admin1, Admin2, Admin3, and Admin4</li></ul>
Blade:	<ul style="list-style-type: none"><li>Reports</li><li><b>Service Health</b></li><li>Message center</li></ul>

 **Demoster** Highly Voted  1 month ago

All admins of Litware can view Service health  
<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

upvoted 5 times

 **Greatone1** Most Recent  1 day, 9 hours ago

<https://www.examtopics.com/discussions/microsoft/view/81381-exam-ms-100-topic-8-question-3-discussion/>  
upvoted 1 times

 **rfree** 1 day, 19 hours ago

Given answer is correct.  
<https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide>  
Monitor and Review may be different things.  
"People who are assigned the global admin or service support admin role can view service health. To allow Exchange, SharePoint, and Skype for Business admins to view service health, they must also be assigned the Service admin role."  
upvoted 1 times

 **Greatone1** 5 days, 7 hours ago

Answer: Admin1, Admin2, Admin3, Admin4 and Service Health  
All can view the service Health Blade.  
upvoted 1 times

 **JensV** 1 month ago

All four Roles have the permission `microsoft.office365.serviceHealth/allEntities/allTasks`  
So all Users can review incidents and advisories  
upvoted 3 times

You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.

From Microsoft 365 Defender portal, you perform a security investigation.

You need to run a PowerShell script on the device to collect forensic information.

Which action should you select on the device page?

- A. Collect investigation package
- B. Go hunt
- C. Initiate Live Response Session
- D. Initiate Automated Investigation

**Correct Answer:** C

 **Vincent1966** 1 month ago

C: Live response is designed to enhance investigations by enabling you to collect forensic data, run scripts, send suspicious entities for analysis, remediate threats, and proactively hunt for emerging threats.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide>  
upvoted 3 times

**HOTSPOT**

You configure an anti-phishing policy as shown in the following exhibit.

<b>Policy setting</b>	<b>Policy name</b> Description Applied to	Managers  If the email is sent to: IrvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com Except if the email is sent to member of: test1ww@M365x289755.onmicrosoft.com	Edit
<b>Impersonation</b>	<b>Users to protect</b> Protect all domains I own Protect specific domains Action > User impersonation Action > Domain impersonation Safety tips > User impersonation Safety tips > Domain impersonation Safety tips > Unusual characters Mailbox intelligence	On - 3 User(s) specified On On - 2 Domain(s) specified Move message to the recipients' Junk Email folders Delete the message before it's delivered Off Off Off Off	Edit
<b>Spoof</b>	<b>Enable antispoofing protection</b> Action	On Quarantine the message	Edit

<b>Advanced settings</b>	<b>Advanced phishing thresholds</b>	3 - More Aggressive	Edit
--------------------------	-------------------------------------	---------------------	------

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

**Answer Area**

If a message is identified as a domain impersonation, [answer choice].

- the message is delivered to the Inbox folder  
the message is moved to the Deleted Items folder  
the messages is moved to the Junk Email folder  
the message is NOT delivered
- Domain impersonation  
Enable antispoofing protection  
Mailbox intelligence

**Correct Answer:****Answer Area**

If a message is identified as a domain impersonation, [answer choice].

- the message is delivered to the Inbox folder  
the message is moved to the Deleted Items folder  
the messages is moved to the Junk Email folder  
the message is NOT delivered
- Domain impersonation  
Enable antispoofing protection  
Mailbox intelligence

 **cb0900** 1 month ago

Answers look correct.

<https://www.examtopics.com/discussions/microsoft/view/71890-exam-ms-101-topic-3-question-5-discussion/>

upvoted 3 times

Question #178

Topic 1

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You notice that it takes several days to notify email recipients when an incoming email message is marked as spam, and then quarantined.

You need to ensure that the email recipients are notified within 24 hours.

What should you do?

- A. Modify the default inbound anti-spam policy.
- B. Modify the DefaultFullAccessPolicy quarantine policy.
- C. Add a custom quarantine policy.
- D. Modify the global settings for quarantine policies.

**Correct Answer: D**

 **cb0900** 1 month ago

**Selected Answer: D**

Answer is correct.

Quarantine policy, Global Settings (Defender portal -> Email & Collaboration -> Policies & rules -> Threat policies -> Quarantine policy). Change 'Send end-user spam notifications' to Daily.

upvoted 3 times

Question #179

Topic 1

You have a Microsoft 365 E5 subscription.

You need to ensure that administrators receive an email when Microsoft 365 Defender detects a sign-in from a risky IP address.

What should you create?

- A. a vulnerability notification rule
- B. an alert
- C. an incident assignment filter
- D. an incident notification rule

**Correct Answer: B**

 **Paul\_white** 2 weeks ago

GIVEN ANSWER IS CORRECT!!!!

upvoted 1 times

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Intune.

Devices are onboarded by using Microsoft Defender for Endpoint.

You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint.

What should you create first?

- A. a device configuration policy
- B. a device compliance policy
- C. a conditional access policy
- D. an endpoint detection and response policy

**Correct Answer: B**

👤 **Paul\_white** 2 weeks ago

GIVEN ANSWER IS CORRECT AS STATED!!!

upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

You need to configure threat protection for Microsoft 365 to meet the following requirements:

- Limit a user named User1 from sending more than 30 email messages per day.
- Prevent the delivery of a specific file based on the file hash.

Which two threat policies should you configure in Microsoft Defender for Office 365? To answer, select the appropriate threat policies in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

## Threat policies

### Templated policies

	Preset Security Policies	Easily configure protection by applying all policies at once using our recommended protection templates
	Configuration analyzer	Identify issues in your current policy configuration to improve your security

### Policies

	Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
	Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
	Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
	Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

### Rules

	Tenant Allow/Block Lists	Manage allow or block entries for your organization.
	Email authentication settings	Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
	DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users
	Advanced delivery	Manage overrides for special system use cases.
	Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first
	Quarantine policies	Apply custom rules to quarantined messages by using default quarantine policies or creating your own

#### Answer Area

## Threat policies

### Templated policies

 Preset Security Policies	Easily configure protection by applying all policies at once using our recommended protection templates
 Configuration analyzer	Identify issues in your current policy configuration to improve your security

### Policies

 Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
 Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
 Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
 Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
 Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

Correct Answer:

### Rules

 Tenant Allow/Block Lists	Manage allow or block entries for your organization.
 Email authentication settings	Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
 DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users
 Advanced delivery	Manage overrides for special system use cases.
 Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first
 Quarantine policies	Apply custom rules to quarantined messages by using default quarantine policies or creating your own

 cb0900 4 weeks, 1 day ago

Answers are correct

1. Anti-spam
2. Tenant allow/block list -> Files. Add file hash

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-allow-block-list-files-configure?view=o365-worldwide#use-the-microsoft-365-defender-portal-to-create-block-entries-for-files-in-the-tenant-allowblock-list>

<https://www.examtopics.com/discussions/microsoft/view/110906-exam-ms-101-topic-2-question-135-discussion/>  
upvoted 2 times

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

A Built-in protection preset security policy is applied to the subscription.

Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Anti-malware
- B. Safe Attachments
- C. Safe Links
- D. Anti-phishing
- E. Anti-spam

**Correct Answer: BC**

 **cb0900** 4 weeks, 1 day ago

**Selected Answer: BC**

Correct, Safe links and Safe attachments.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/preset-security-policies?view=o365-worldwide#use-the-microsoft-365-defender-portal-to-add-exclusions-to-the-built-in-protection-preset-security-policy>

<https://www.examtopics.com/discussions/microsoft/view/93860-exam-ms-101-topic-2-question-112-discussion/>

upvoted 2 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

The subscription has the following two anti-spam policies:

- Name: AntiSpam1
- Priority: 0
- Include these users, groups and domains
- Users: User3
- Groups: Group1
- Exclude these users, groups and domains
- Groups: Group2
- Message limits
- Set a daily message limit: 100
  
- Name: AntiSpam2
- Priority: 1
- Include these users, groups and domains
- Users: User1
- Groups: Group2
- Exclude these users, groups and domains
- Groups: Group3
- Message limits
- Set a daily message limit: 50

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	<input type="radio"/>	<input type="radio"/>
User2 can send a maximum of 50 email messages per day.	<input type="radio"/>	<input type="radio"/>

**Answer Area**

Statements	Yes	No
Correct Answer: User1 can send a maximum of 150 email messages per day.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can send a maximum of 50 email messages per day.	<input checked="" type="radio"/>	<input type="radio"/>

 **Milad666** 2 weeks, 5 days ago

Answer is Correct :

Multiple different types of exceptions aren't additive; they're inclusive. The policy isn't applied only if those recipients that match all of the specified recipient filters. For example, you configure a recipient filter exception with the following values:

Users: roman@contoso.com

Groups: Executives

The policy isn't applied to roman@contoso.com only if he's also a member of the Executives group. If he's not a member of the group, then the policy still applies to him.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/preset-security-policies?view=o365-worldwide#use-the-microsoft-365-defender-portal-to-add-exclusions-to-the-built-in-protection-preset-security-policy>  
upvoted 3 times

✉️ **Casticod** 1 month, 1 week ago

I think NO for boths options.

User 1 and 2 are members of group 1. first apply the policy with the most low priority (policy 1, priority 0)

upvoted 3 times

✉️ **EM1234** 2 weeks ago

User 2 would be excluded from being in group 2

upvoted 1 times

Question #184

Topic 1

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.

You have the policies shown in the following table.

Name	Type
Policy1	Anti-phishing
Policy2	Anti-spam
Policy3	Anti-malware
Policy4	Safe Attachments

All the policies are configured to send malicious email messages to quarantine.

Which policies support a customized quarantine retention period?

- A. Policy1 and Policy2 only
- B. Policy1 and Policy3 only
- C. Policy2 and Policy4 only
- D. Policy3 and Policy4 only

**Correct Answer: A**

✉️ **DiligentSam** 3 weeks, 4 days ago

correct

upvoted 2 times

✉️ **Demonster** 1 month ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-about?view=o365-worldwide#quarantine-retention>  
upvoted 3 times

You have a Microsoft 365 E5 subscription.

Your company's Microsoft Secure Score recommends the actions shown in the following exhibit.

## Microsoft Secure Score

Overview Recommended actions History Metrics & trends

 Export

Rank	Recommended action	Score impact	Points achieved	Status
<input type="checkbox"/>	1 Require multifactor authentication for administrative roles	+4.15%	0/10	<input type="radio"/> To address
<input type="checkbox"/>	2 Ensure all users can complete multifactor authentication	+3.73%	0/9	<input type="radio"/> To address
<input type="checkbox"/>	3 Create Safe Links policies for email messages	+3.73%	0/9	<input type="radio"/> To address
<input type="checkbox"/>	4 Enable policy to block legacy authentication	+3.32%	0/8	<input type="radio"/> To address
<input type="checkbox"/>	5 Turn on Safe Attachments in block mode	+3.32%	0/8	<input type="radio"/> To address
<input type="checkbox"/>	6 Ensure that intelligence for impersonation protection is enabled	+3.32%	0/8	<input type="radio"/> To address
<input type="checkbox"/>	7 Move messages that are detected as impersonated users by mailbox intelligence	+3.32%	0/8	<input type="radio"/> To address
<input type="checkbox"/>	8 Enable impersonated domain protection	+3.32%	0/8	<input type="radio"/> To address

You select Create Safe Links policies for email messages and change Status to Risk accepted in the Status & action plan settings.

How does the change affect the Secure Score?

- A. remains the same
- B. increases by 1 point
- C. increases by 9 points
- D. decreases by 1 point
- E. decreases by 9 points

**Correct Answer: A**

 cb0900 4 weeks, 1 day ago

Agree with the answer - it stays the same.

No points are given for 'Risk Accepted'.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score-improvement-actions?view=o365-worldwide#choose-a-recommended-action-status>

upvoted 2 times

DRAG DROP

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Type	Number of devices	Operating system	Enrollment status
Corporate	150	Windows 11	Azure AD-joined, Microsoft Intune-managed
Bring your own device (BYOD)	25	Windows 11	Unmanaged

You need to onboard the devices to Microsoft Defender for Endpoint. The solution must minimize administrative effort.

What should you use to onboard each type of device? To answer, drag the appropriate onboarding methods to the correct device types. Each onboarding method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Answer Area**

**Onboarding method**

- A local script
- Group Policy
- Integration with Microsoft Defender for Cloud
- Microsoft Intune
- Virtual Desktop Infrastructure (VDI) scripts

**Device Type**

Corporate:

BYOD:

**Device Type**

**Correct Answer:**

Corporate:

BYOD:

 **862e76c** 4 weeks, 1 day ago

Agree with the answer  
upvoted 1 times

 **Casticod** 1 month, 1 week ago

Correct <https://techcommunity.microsoft.com/t5/microsoft-defender-vulnerability/unmanaged-device-protection-capabilities-are-now-generally/ba-p/2463796>  
upvoted 1 times

You have a Microsoft 365 E5 subscription.

You onboard all devices to Microsoft Defender for Endpoint.

You need to use Defender for Endpoint to block access to a malicious website at [www.contoso.com](http://www.contoso.com).

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct answer is worth one point.

- A. Create a web content filtering policy.
- B. Enable Custom network indicators.
- C. Enable automated investigation.
- D. Create an indicator.
- E. Configure an enforcement scope.

**Correct Answer: AB**

 **ExamCheater1993** Highly Voted 4 weeks ago

**Selected Answer: BD**

This is wrong. You should first enable Enable Custom Network indicators and then create an indicator.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-ip-domain?view=o365-worldwide#create-an-indicator-for-ips-urls-or-domains-from-the-settings-page>

upvoted 5 times

 **rfree** Most Recent 1 week, 5 days ago

Web content filtering only seems to block Categories, not a single site. BD

upvoted 1 times

 **Paul\_white** 2 weeks ago

BD IS THE RIGHT ANSWER

upvoted 1 times

 **Ranger\_DanMT** 2 weeks ago

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-worldwide>  
Answer is actually correct.

upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

At 08:00, you create an incident notification rule that has the following configurations:

- Name: Notification1
- Notification settings
- Notify on alert severity: Low
- Device group scope: All (3)
- Details: First notification per incident
- Recipients: User1@contoso.com, User2@contoso.com

At 08:02, you create an incident notification rule that has the following configurations:

- Name: Notification2
- Notification settings
- Notify on alert severity: Low, Medium
- Device group scope: DeviceGroup1, DeviceGroup2
- Recipients: User1@contoso.com

In Microsoft 365 Defender, alerts are logged as shown in the following table.

Time	Alert name	Severity	Impacted assets
08:05	Activity1	Low	Device1
08:07	Activity1	Low	Device1
08:08	Activity1	Medium	Device1
08:15	Activity2	Medium	Device2
08:16	Activity2	Medium	Device2
08:20	Activity1	High	Device1
08:30	Activity3	Medium	Device2
08:35	Activity2	High	Device2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	<input type="radio"/>	<input type="radio"/>
User2@contoso.com will receive an incident notification email for the alert at 08:07.	<input type="radio"/>	<input type="radio"/>
User1@contoso.com will receive an incident notification email for the alert at 08:20.	<input type="radio"/>	<input type="radio"/>

**Answer Area****Statements**

User1@contoso.com will receive two incident notification emails for the alert at 08:05.

 Yes No**Correct Answer:**

User2@contoso.com will receive an incident notification email for the alert at 08:07.

User1@contoso.com will receive an incident notification email for the alert at 08:20.

**vercracked\_007** Highly Voted 1 month ago

Should this not be YYN  
two different notification rules  
upvoted 5 times

**jt2214** Most Recent 5 days, 21 hours ago

I'm going to agree with Paul\_white based on the link he provided. N/N/N

<https://www.examtopics.com/discussions/microsoft/view/81762-exam-ms-101-topic-2-question-101-discussion/#>  
upvoted 1 times

**Paul\_white** 2 weeks ago

Correct answer is NO, NO, NO  
<https://www.examtopics.com/discussions/microsoft/view/81762-exam-ms-101-topic-2-question-101-discussion/#>  
upvoted 2 times

**Milad666** 1 week, 1 day ago

Correct Answer is : Y N N

Y, N, N

User1 will receive two incident notifications from "notification1" and "notification2"  
User2 already received incident notification on device1 from the incident at 8:05  
User1 will not receive at 8:20 as the severity is high and doesn't apply  
upvoted 1 times

**ninjanaja** 1 month ago

My answer: YNN  
upvoted 4 times

**HOTSPOT**

You have Microsoft 365 subscription.

You create an alert policy as shown in the following exhibit.

## Policy1

 [Edit policy](#) [Delete policy](#)

Status On

---

### Name your alert



Description Severity  
[Add a description](#) Low

Category Policy contains tags  
Threat management -

---

### Create alert settings



Conditions Aggregation  
Activity is FileMalwareDetected Aggregated

Scope Threshold  
All users 20

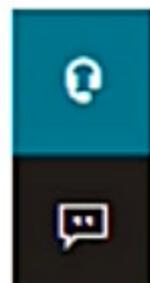
Window  
2 hours

---

### Set your recipients



Recipients Daily notification limit  
User1@sk220912outlook.onmicrosoft.com 100



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

#### Answer Area

Policy1 will trigger an alert if malware is detected in [answer choice].

Exchange Online only  
SharePoint only  
SharePoint or OneDrive only  
Exchange Online, SharePoint, or OneDrive

The maximum number of email messages that Policy1 will generate per day is [answer choice].

5  
12  
20  
100

#### Answer Area

Policy1 will trigger an alert if malware is detected in [answer choice].

Exchange Online only  
SharePoint only  
**SharePoint or OneDrive only**  
Exchange Online, SharePoint, or OneDrive

#### Correct Answer:

The maximum number of email messages that Policy1 will generate per day is [answer choice].

**5**  
12  
20  
100

  ninjanaja 1 month ago

I think  
"Onedrive and Sharepoint Only" and "12"  
upvoted 4 times

  Casticod 1 month, 1 week ago

Should Be Onedrive and Sharepoint Only and 20.  
In this question about ms-100 its the same question with other values... <https://www.examtopics.com/discussions/microsoft/view/48787-exam-ms-101-topic-2-question-64-discussion/>  
upvoted 4 times

  Casticod 1 month, 1 week ago

ups sorry, the second option should be 12  
The policy triggers when there are 20 activities within 120 min (2 hours)  
So every 2 hours, the policy checks and if there are more than 20 activities, it sends 1 alert. Since we have 24hours/day, the policy can send a maximum of 1alert/2hours or 12alerts/24hours.  
upvoted 5 times

You have a Microsoft 365 E5 tenant.

You need to create a policy that will trigger an alert when unusual Microsoft Office 365 usage patterns are detected.

What should you use to create the policy?

- A. the Microsoft Apps admin center
- B. the Microsoft Purview compliance portal
- C. the Microsoft 365 admin center
- D. the Microsoft 365 Defender portal

**Correct Answer: D**

✉  **jt2214** 5 days, 20 hours ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide>

upvoted 1 times

✉  **Paul\_white** 2 weeks ago

CORRECT ANSWER IS B

upvoted 1 times

✉  **DiligentSam** 3 weeks ago

Why not D?

upvoted 2 times

✉  **siulas** 1 month, 1 week ago

**Selected Answer: B**

<https://www.examtopics.com/discussions/microsoft/view/94443-exam-ms-101-topic-2-question-107-discussion/>

upvoted 4 times

You have a Microsoft 365 subscription.

You plan to use Adoption Score and need to ensure that it can obtain device and software metrics.

What should you do?

- A. Enable privileged access.
- B. Enable Endpoint analytics.
- C. Configure Support integration.
- D. Run the Microsoft 365 network connectivity test on each device.

**Correct Answer: B**

 **DiligentSam** 1 week, 6 days ago

<https://www.examtopics.com/discussions/microsoft/view/98504-exam-ms-100-topic-2-question-85-discussion/>  
upvoted 1 times

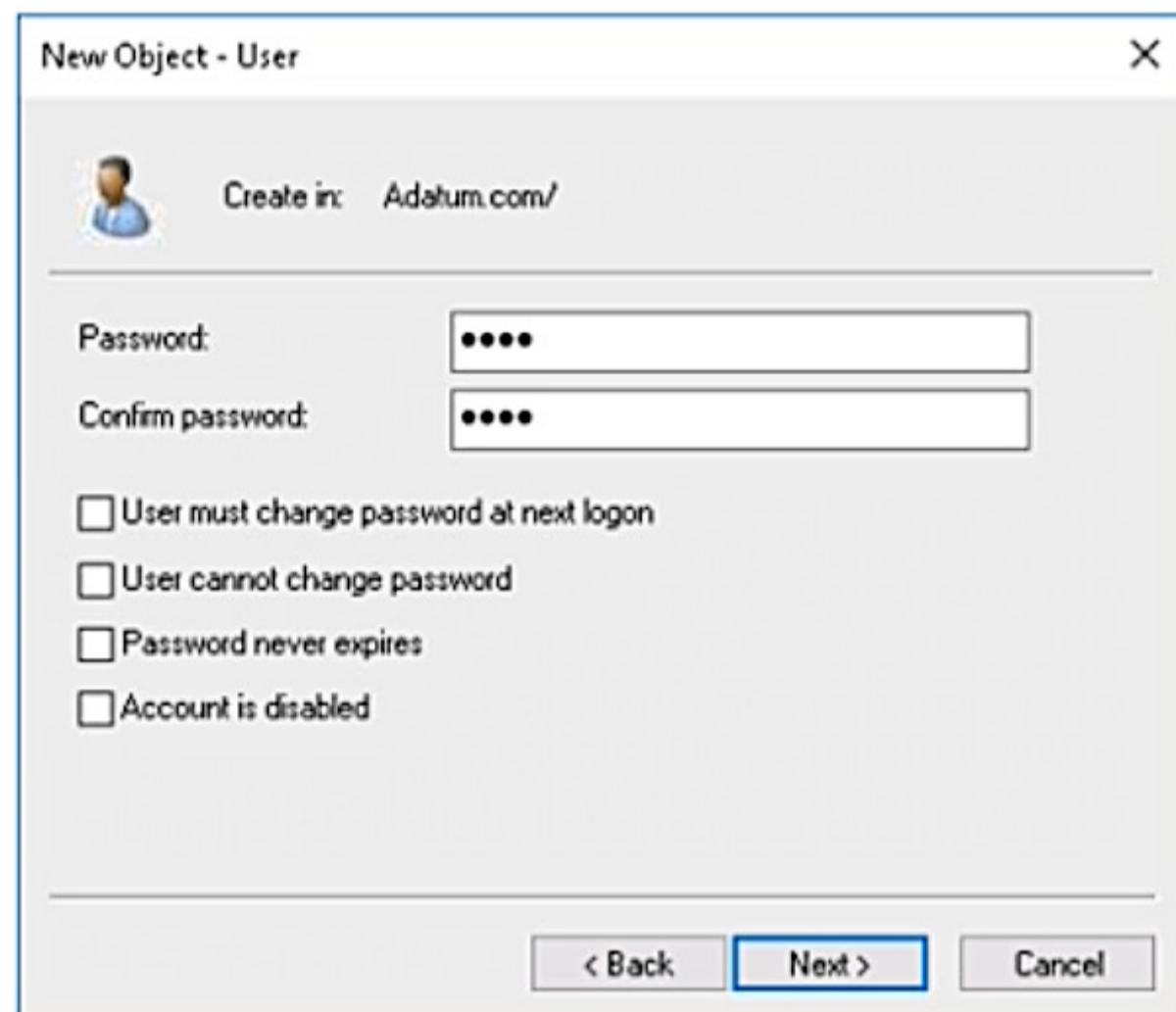
 **Paul\_white** 2 weeks ago

CORRECT!!!  
upvoted 2 times

**HOTSPOT**

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure AD by using the Azure AD Connect Express Settings. Password writeback is disabled.

You create a user named User1 and enter Pass in the Password field as shown in the following exhibit.



The Azure AD password policy is configured as shown in the following exhibit.

## Password policy

**Set the password policy for all users in your organization.**

**Days before passwords expire** 90

**Days before a user is notified about expiration** 14

You confirm that User1 is synced to Azure AD.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
User1 can sign in to Azure AD.	<input type="radio"/>	<input type="radio"/>
User1 can change the password immediately by using the My Apps portal.	<input type="radio"/>	<input type="radio"/>
From Azure AD, User1 must change the password every 90 days.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
User1 can sign in to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can change the password immediately by using the My Apps portal.	<input type="radio"/>	<input checked="" type="radio"/>
From Azure AD, User1 must change the password every 90 days.	<input checked="" type="radio"/>	<input type="radio"/>

✉  **Casticod** Highly Voted 1 month, 1 week ago

YES NO NO

If password writeback is disabled, the password policies in Azure AD and on-premises Active Directory will be enforced independently.

By default, the Azure AD password policy requires users to change their passwords every 90 days. However, if you have a hybrid environment and are synchronizing passwords from on-premises Active Directory to Azure AD, the on-premises password policy will apply to your users. In this case, the password expiration period will be determined by your on-premises Active Directory policy settings, not by Azure AD.

If you want to enforce a consistent password expiration policy for both on-premises and cloud users, you should configure the password policies in both environments to have the same settings.

<https://www.examtopics.com/discussions/microsoft/view/48898-exam-ms-100-topic-3-question-69-discussion/>  
upvoted 12 times

✉  **ninjanaja** Highly Voted 1 month ago

Because " Password writeback is disabled."

YNN

upvoted 5 times

✉  **Ranger\_DanMT** Most Recent 1 week, 3 days ago

Yes i can verify we don't buy the licensing for SSPR writeback but passwords still expire. Password expire = Y

upvoted 1 times

✉  **Ranger\_DanMT** 1 week, 3 days ago

I misread. should be YNN

upvoted 1 times

✉  **rfree** 1 week, 3 days ago

Question states, Azure Pword Policy has set password expiry to 90 days. So YNY, Yes you must change the Azure password. It will not sync back to AD, but still must be changed in Azure. Correct?

upvoted 1 times

✉  **agittunc** 2 days, 5 hours ago

No as it's a hybrid environment it should be changed from AD.

upvoted 1 times

**HOTSPOT**

Your company uses Microsoft Defender for Endpoint.

The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.

Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

The alerts visible in the Microsoft Defender for Endpoint alerts queue are shown in the following table.

Name	Device
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:

- Triggering IOC: Any IOC
- Action: Hide alert
- Suppression scope: Alerts on ATP1 device group

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>
After you create the suppression rule, Alert3 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>

**Answer Area**

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	<input checked="" type="radio"/>	<input type="radio"/>
After you create the suppression rule, Alert3 is visible in the alerts queue.	<input checked="" type="radio"/>	<input type="radio"/>
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	<input type="radio"/>	<input checked="" type="radio"/>

Answer Y-Y-N is correct. Existing alerts are not suppressed after the rule is created:

When a suppression rule is created, it will take effect from the point when the rule is created. The rule will not affect existing alerts already in the queue, prior to the rule creation. The rule will only be applied on alerts that satisfy the conditions set after the rule is created.

Link: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwide#suppress-alerts>  
upvoted 1 times

✉️ **DiligentSam** 3 weeks, 4 days ago

Given answers seem correct  
upvoted 2 times

✉️ **cb0900** 3 weeks, 6 days ago

Given answers seem correct.

Q1/Q2. Both Y. The alerts were generated before the suppression rule was enabled. The alerts remain.  
Q3. N

<https://www.examtopics.com/discussions/microsoft/view/49354-exam-ms-101-topic-2-question-24-discussion/>  
upvoted 3 times

Question #194

Topic 1

You have a Microsoft 365 E5 tenant.

You configure sensitivity labels.

Users report that the Sensitivity button is unavailable in Microsoft Word for the web. The Sensitivity button is available in Microsoft 365 Word.

You need to ensure that the users can apply the sensitivity labels when they use Word for the web.

What should you do?

- A. Enable sensitivity labels for files in Microsoft SharePoint and OneDrive.
- B. Publish the sensitivity labels.
- C. Copy policies from Azure Information Protection to the Microsoft Purview compliance portal.
- D. Create an auto-labeling policy.

**Correct Answer: B**

✉️ **Greatone1** 1 week, 2 days ago

Enable sensitivity labels for files in Microsoft SharePoint Online and OneDrive is the correct answer 🌟  
upvoted 1 times

✉️ **cb0900** 3 weeks, 6 days ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/purview/sensitivity-labels-sharepoint-onedrive-files?view=o365-worldwide>

Enable built-in labeling for supported Office files in SharePoint and OneDrive so that users can apply your sensitivity labels in Office for the web. When this feature is enabled, users see the Sensitivity button on the ribbon so they can apply labels, and see any applied label name on the status bar.

upvoted 3 times

✉️ **siulas** 1 month, 1 week ago

**Selected Answer: A**

<https://www.examtopics.com/discussions/microsoft/view/82514-exam-ms-101-topic-2-question-103-discussion/>  
upvoted 4 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

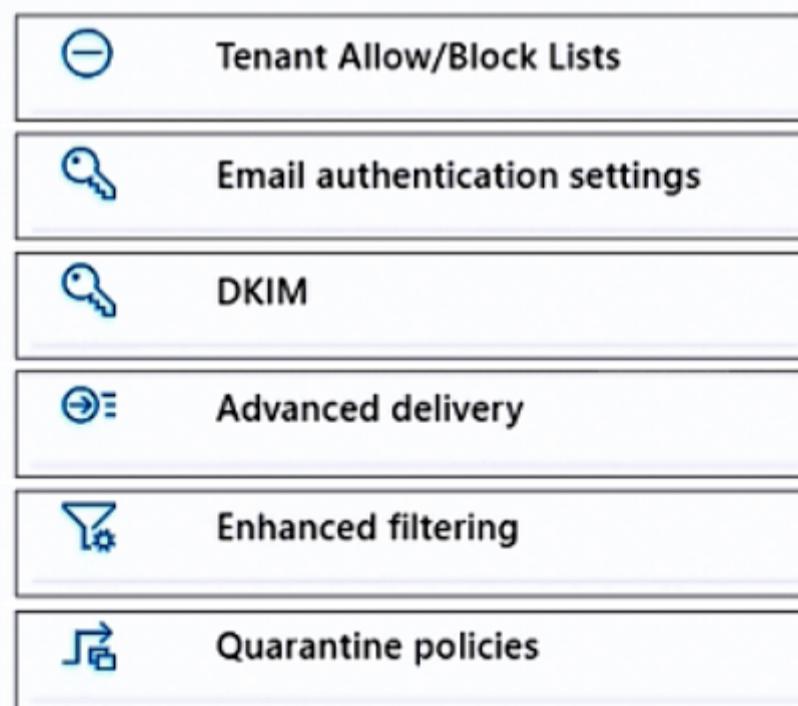
You plan to use a mailbox named Mailbox1 to analyze malicious email messages.

You need to configure Microsoft Defender for Office 365 to meet the following requirements:

- Ensure that incoming email is NOT filtered for Mailbox1.
- Detect impersonation and spoofing attacks on all other mailboxes in the subscription.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area****Policies****Rules**

## Answer Area

### Policies

-  Anti-phishing
-  Anti-spam
-  Anti-malware
-  Safe Attachments
-  Safe Links

Correct Answer:

### Rules

-  Tenant Allow/Block Lists
-  Email authentication settings
-  DKIM
-  Advanced delivery
-  Enhanced filtering
-  Quarantine policies

 **siulas** Highly Voted 1 month, 1 week ago

Advanced Delivery

Anti-phishing

<https://www.examtopics.com/discussions/microsoft/view/94445-exam-ms-101-topic-2-question-111-discussion/>

upvoted 8 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

You plan to implement identity protection by configuring a sign-in risk policy and a user risk policy.

Which type of risk is detected by each policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

**Sign-in risk policy:**

Atypical travel  
Leaked credentials  
Possible attempt to access Primary Refresh Token (PRT)

**User risk policy:**

Leaked credentials  
Malicious IP address  
Suspicious browser

**Answer Area**

**Sign-in risk policy:**

Atypical travel  
**Leaked credentials**  
Possible attempt to access Primary Refresh Token (PRT)

**Correct Answer:**

**User risk policy:**

**Leaked credentials**  
**Malicious IP address**  
Suspicious browser

 **Kizzik** Highly Voted 1 month ago

Sign in risk policy: Atypical travel  
User risk policy: Leaked credentials

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#sign-in-risk-detections>  
upvoted 11 times

 **Greatone1** Most Recent 6 days, 9 hours ago

I believe that it's worth the investment. Examtopics has helped me pass as many exams as I have fingers!!  
upvoted 1 times

 **jt2214** 1 week, 1 day ago

I believe that it's worth the investment. Examtopics has helped me to successfully pass all of my exams.  
upvoted 2 times

 **Cazz123** 2 weeks, 2 days ago

I wonder how exam Topics come up with the answers they provide. I am starting to question if this is actually worth my money.  
upvoted 3 times

 **DiligentSam** 2 weeks, 6 days ago

Correct  
upvoted 1 times

 **DiligentSam** 2 weeks, 6 days ago

I mean Kizzik's Answer is correct  
upvoted 1 times

Question #197

Topic 1

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to configure Microsoft Defender for Office 365 to meet the following requirements:

- A user's email sending patterns must be used to minimize false positives for spoof protection.
- Documents uploaded to Microsoft Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365.

What should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

A user's email sending patterns must be used to minimize false positives for spoof protection:

Domains to protect  
Mailbox intelligence  
Users to protect

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using  
Defender for Office 365:

Global settings for safe attachments  
The Safe Attachments policy settings  
The Safe Links policy settings

#### Answer Area

A user's email sending patterns must be used to minimize false positives for spoof protection:

Domains to protect  
Mailbox intelligence  
Users to protect

#### Correct Answer:

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using  
Defender for Office 365:

Global settings for safe attachments  
The Safe Attachments policy settings  
The Safe Links policy settings

 **cb0900** 3 weeks, 6 days ago

Given answers are correct.

1. Mailbox intelligence determines user email patterns.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about?view=o365-worldwide#mailbox-intelligence-impersonation-protection>

2. Global settings for safe attachments is where you toggle protection for SharePoint, OneDrive and Teams.

upvoted 4 times

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

You plan to perform device discovery and authenticated scans of network devices.

You install and register the network scanner on a device named Device1.

What should you do next?

- A. Connect Defender for Endpoint to Microsoft Intune.
- B. Apply for Microsoft Threat Experts - Targeted Attack Notifications.
- C. Create an assessment job.
- D. Download and run an onboarding package.

**Correct Answer: C**

 cb0900 3 weeks, 6 days ago

**Selected Answer: C**

<https://www.examtopics.com/discussions/microsoft/view/94572-exam-ms-101-topic-3-question-141-discussion/>

upvoted 2 times

 Hard1k 1 month, 1 week ago

**Selected Answer: C**

The answer is C. Create an assessment job.

Once you have installed and registered the network scanner on Device1, you need to create an assessment job. An assessment job is a scheduled scan of network devices.

upvoted 4 times

You have a Microsoft 365 subscription.

You need to receive a notification each time a user in the service desk department grants Full Access permissions for a user mailbox.

What should you configure?

- A. a data loss prevention (DLP) policy
- B. an alert policy
- C. an audit search
- D. an insider risk management policy

**Correct Answer: B**

 Hard1k 1 month, 1 week ago

**Selected Answer: B**

The answer is B. an alert policy.

An alert policy is used to send notifications when certain events occur, such as when a user grants Full Access permissions for a user mailbox.

upvoted 3 times

You have a Microsoft 365 E5 subscription.

You need to be alerted when Microsoft 365 Defender detects high-severity incidents.

What should you use?

- A. a custom detection rule
- B. a threat policy
- C. an alert policy
- D. a notification rule

**Correct Answer: C**

 **jbuexamtopics** 3 days, 3 hours ago

**Selected Answer: D**

Notification Rule

<https://www.examtopics.com/discussions/microsoft/view/94056-exam-ms-101-topic-2-question-115-discussion/>  
upvoted 1 times

 **agittunc** 2 days, 5 hours ago

Check the link, it's C. not D.  
upvoted 1 times

 **Greatone1** 1 week, 6 days ago

notification rule is the correct answer   
upvoted 1 times

 **Blagojche** 2 weeks, 2 days ago

The correct answer is D. a notification rule.

Notification rules in Microsoft 365 Defender allow you to receive alerts when certain conditions are met, such as when high-severity incidents are detected. This can help you stay informed about potential security issues and respond quickly.

Options A, B, and C do not directly address the requirement of receiving alerts for high-severity incidents  
upvoted 1 times

 **Hard1k** 1 month, 1 week ago

**Selected Answer: C**

The answer is C. an alert policy.

An alert policy is used to send notifications when certain events occur, such as when Microsoft 365 Defender detects a high-severity incident.  
upvoted 3 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

All corporate Windows 11 devices are managed by using Microsoft Intune and onboarded to Microsoft Defender for Endpoint.

You need to meet the following requirements:

- View an assessment of the device configurations against the Center for Internet Security (CIS) v1.0.0 benchmark.
- Protect a folder named C:\Folder1 from being accessed by untrusted applications on the devices.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

To view the device configuration assessment:

Add a connected application.
Create a baseline assessment profile.
Filter the Vulnerable devices report.

To protect C:\Folder1, enable:

Controlled folder access
Exploit protection
Removable storage protection

**Answer Area**

To view the device configuration assessment:

Add a connected application.
<b>Create a baseline assessment profile.</b>
Filter the Vulnerable devices report.

Correct Answer:

To protect C:\Folder1, enable:

<b>Controlled folder access</b>
Exploit protection
Removable storage protection

You have a Microsoft 365 subscription that contains the alerts shown in the following table.

Name	Severity	Status	Comment	Category
Alert1	Medium	Active	Comment1	Threat management
Alert2	Low	Resolved	Comment2	Other

Which properties of the alerts can you modify?

- A. Status only
- B. Status and Comment only
- C. Status and Severity only
- D. Status, Severity, and Comment only
- E. Status, Severity, Comment and Category

**Correct Answer: B**

 **DiligentSam** 3 weeks, 4 days ago

Agree with cb0900

upvoted 1 times

 **cb0900** 3 weeks, 6 days ago

**Selected Answer: B**

Checked in a test tenant.

<https://www.examtopics.com/discussions/microsoft/view/65982-exam-ms-101-topic-2-question-73-discussion/>

upvoted 2 times

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.

All the devices in your organization are onboarded to Microsoft Defender for Endpoint.

You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours.

What should you do?

- A. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.
- B. From Alerts queue, create a suppression rule and assign an alert.
- C. From Advanced hunting, create a query and a detection rule.
- D. From the Microsoft Purview compliance portal, create an audit log search.

**Correct Answer: C**

 **cb0900** 3 weeks, 6 days ago

**Selected Answer: C**

<https://www.examtopics.com/discussions/microsoft/view/33967-exam-ms-101-topic-2-question-27-discussion/>

upvoted 1 times

 **Hard1k** 1 month, 1 week ago

**Selected Answer: C**

C. From Advanced hunting, create a query and a detection rule.

Advanced hunting allows you to create custom queries to search for specific events in your environment. You can then use these queries to create detection rules that will generate alerts when certain events occur.

upvoted 3 times

**HOTSPOT**

You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint.

You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 11
Device3	iOS
Device4	Android

You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant. Noncompliant devices must be blocked from accessing corporate resources.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Devices that can be onboarded to Microsoft Defender for Endpoint:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1 and Device4 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3, and Device4

Endpoint security policies that must be configured:

- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

**Answer Area**

Devices that can be onboarded to Microsoft Defender for Endpoint:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1 and Device4 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3, and Device4

**Correct Answer:**

Endpoint security policies that must be configured:

- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

 **Casticod** Highly Voted 1 month, 1 week ago

I believe the answer to the second question is device configuration policy, device compliance policy and conditional access.  
<https://www.examtopics.com/discussions/microsoft/view/65484-exam-ms-101-topic-2-question-86-discussion/>  
upvoted 12 times

 **DiligentSam** 3 weeks, 4 days ago

Agree with Casticod

upvoted 1 times

 **ExamCheater1993** 3 weeks, 4 days ago

I agree with this guy.

upvoted 3 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

You configure a new alert policy as shown in the following exhibit.

**How do you want the alert to be triggered?**

- Every time an activity matches the rule
- When the volume of matched activities reaches a threshold

More than or equal to  activities

During the last  minutes

On

- When the volume of matched activities becomes unusual

On

You need to identify the following:

- How many days it will take to establish a baseline for unusual activity
- Whether alerts will be triggered during the establishment of the baseline

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

How many days it will take to establish the baseline:

Whether the alerts will be triggered during the establishment of the baseline:

 Alerts will be triggered.  
 Alerts will not be triggered.  
 Alerts will be triggered only after the process to establish the baseline has been running for one day.**Answer Area**

How many days it will take to establish the baseline:

  
  
  
**Correct Answer:**

Whether the alerts will be triggered during the establishment of the baseline:

 Alerts will be triggered.  
 Alerts will not be triggered.  
 Alerts will be triggered only after the process to establish the baseline has been running for one day.

Given answers correct.  
7 days to establish a baseline  
Alerts will not be triggered.

<https://www.examtopics.com/discussions/microsoft/view/74695-exam-ms-101-topic-2-question-97-discussion/>

<https://learn.microsoft.com/en-us/purview/alert-policies?view=o365-worldwide#alert-policy-settings>

upvoted 4 times

You have a Microsoft 365 E5 tenant.

You create a retention label named Retention1 as shown in the following exhibit.

## Create retention label

The screenshot shows the 'Create retention label' wizard in progress. On the left, a vertical checklist indicates steps completed: Name (checkmark), File plan descriptors (checkmark), Label Settings (checkmark), Period (checkmark), and Finish (blue dot). The main area is titled 'Review and finish'. It displays the retention label configuration:

- Name**: Name is Retention1, with an [Edit](#) link.
- File plan descriptors**:
  - Retention settings**:
    - Retention period: 6 months
    - Retention action: Retain and Delete
    - [Edit](#)
  - Based on**: Based on when it was created
  - [Edit](#)

At the bottom are 'Back' and 'Create label' buttons.

You apply Retention1 to all the Microsoft OneDrive content.

On January 1, 2020, a user stores a file named File1 in OneDrive.

On January 10, 2020, the user modifies File1.

On February 1, 2020, the user deletes File1.

When will File1 be removed permanently and unrecoverable from OneDrive?

- A. February 1, 2020
- B. July 1, 2020
- C. July 10, 2020
- D. August 1, 2020

**Correct Answer: B**

**Paul\_white** 1 week, 6 days ago

GIVEN ANSWER IS CORRECT

upvoted 2 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains a SharePoint site named Site1. Site1 contains the files shown in the following table.

Name	Number of IP addresses in the file
File1	2
File2	5

You have the users shown in the following table.

Name	Role
User1	Site owners for Site1
User2	Site members for Site1
Admin1	SharePoint admins

You create a data loss prevention (DLP) policy with an advanced DLP rule and apply the policy to Site1. The DLP rule is configured as shown in the following exhibit.

**Edit rule**

**Conditions**

We'll apply this policy to content that matches these conditions.

**Content contains**

Default Any of these

Sensitive info types

IP Address High confidence Instance count 3 to Any

Add Create group

+ Add condition

**Actions**

Use actions to protect content when the conditions are met.

**Restrict access or encrypt the content in Microsoft 365 locations**

Restrict access or encrypt the content in Microsoft 365 locations

Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files. By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.

Block everyone.

Block only people outside your organization.

Block only people who were given access to the content through the "Anyone with the link" option.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

#### Answer Area

Statements	Yes	No
User1 can open File2.	<input type="radio"/>	<input type="radio"/>
User2 can open File1.	<input type="radio"/>	<input type="radio"/>
Admin1 can open File2.	<input type="radio"/>	<input type="radio"/>

#### Answer Area

Statements	Yes	No
User1 can open File2.	<input checked="" type="checkbox"/>	<input type="radio"/>
User2 can open File1.	<input checked="" type="checkbox"/>	<input type="radio"/>
Admin1 can open File2.	<input type="radio"/>	<input checked="" type="checkbox"/>

Correct Answer:

 **OliwerCiecwierz** 4 days, 18 hours ago

Answer is correct. 1. File2 meet rules but Owner can open. 2, File1 don't meet rules 3. Because File2 meet rules only Owner can open, even Admin is blocked

upvoted 1 times

 **Casticod** 1 month, 1 week ago

Possible incomplete question: <https://www.examtopics.com/discussions/microsoft/view/108499-exam-ms-101-topic-3-question-163-discussion/>  
upvoted 2 times

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named site1.

You need to ensure that site1 meets the following requirements:

- Retains all data for 10 years
- Prevents the sharing of data outside the organization

Which two items should you create and apply to site1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a retention policy
- B. a data loss prevention (DLP) policy
- C. a retention label policy
- D. a sensitive info type
- E. a retention label
- F. a sensitivity label

**Correct Answer: AB**

 **Paul\_white** 1 week, 6 days ago

A, B IS THE RIGHT ANSWER

upvoted 3 times

You have a Microsoft 365 E5 subscription.

From the Microsoft Purview compliance portal, you create a new data loss prevention (DLP) policy named DLP1 that protects financial data from being shared by using Microsoft Teams messages. You apply DLP1 to the users in the finance department.

An incident is raised when a finance department user named User1 shares financial data in a Teams channel that includes external members.

When User1 uses Teams to send the same message in a 1:1 chat or a private channel, the message is blocked as expected.

You need to ensure that User1 is prevented from sharing financial data in Teams channels that include external members.

What should you do?

- A. Edit the settings of the team that contains the channel.
- B. Edit the Locations settings of DLP1.
- C. Modify the licenses assigned to User1.
- D. Edit the policy rules of DLP1.

**Correct Answer: D**

 **AlfaExamPro** Highly Voted 2 weeks, 3 days ago

**Selected Answer: B**

because DLP rules talk about DLP threshold, action etc  
DLP location more specific to set up DLP scope/location  
upvoted 5 times

 **GLL** Most Recent 1 week, 4 days ago

Edit the Locations settings of DLP1  
upvoted 1 times

You have a Microsoft 365 subscription.

You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.

To which location can the policy be applied?

- A. Exchange email
- B. OneDrive accounts
- C. SharePoint sites
- D. Teams chat and channel messages

**Correct Answer: A**

 **Greatone1** 1 week, 3 days ago

Headers equals email or exchange  
upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of Microsoft 365 role group
Admin1	Content Explorer List Viewer Content Explorer Content Viewer
Admin2	Security Administrator Content Explorer List Viewer

You have labels in Microsoft 365 as shown in the following table.

Name	Type
Label1	Sensitivity
Label2	Retention

The content in Microsoft 365 is assigned labels as shown in the following table.

Name	Type	Label
File1	File in SharePoint	Label1
Mail1	Email message in Exchange Online	Label2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area****Statements****Yes****No**

Admin1 can view the contents of File1 by using Content explorer.



Admin2 can view the contents of File1 by using Content explorer.



Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.

**Answer Area****Statements****Yes****No**

Admin1 can view the contents of File1 by using Content explorer.



**Correct Answer:**

Admin2 can view the contents of File1 by using Content explorer.



Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.



 **Paul\_white** 1 week, 6 days ago

GIVEN ANSWER IS CORRECT YES, NO, YES

<https://www.examtopics.com/discussions/microsoft/view/102906-exam-ms-101-topic-2-question-127-discussion/>  
upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains two users named user1@contoso.com and user2@contoso.com and a Microsoft SharePoint site named Site1.

You create a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Name	Content contains	User notifications	Priority
Rule1	4 or more IP addresses	User1@contoso.com	0
Rule2	2 or more IP addresses	User1@contoso.com	1
Rule3	3 or more IP addresses	User2@contoso.com	2

DLP1 is applied to Site1.

You have the files shown in the following table.

Name	Number of IP addresses in the file
File1.xlsx	2
File2.doc	3
File3.pptx	4
File4.txt	6

You copy the files to Site1.

How many notifications will each user receive? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User1@contoso.com:

 0  
 1  
 2  
 3  
 4  
 5  
 6  
 7  
 8

User2@contoso.com:

 0  
 1  
 2  
 3  
 4  
 5  
 6  
 7  
 8

**Answer Area**

User1@contoso.com:

0
1
2
3
4
5
6
7
8

**Correct Answer:**

User2@contoso.com:

0
1
2
3
4
5
6
7
8

✉ **Paul\_white** 1 week, 6 days ago

PERSONALLY I WILL GOT WITH USER1 = 3, AND USER 2 = 0. THE RANKING SAYS IT ALL

<https://www.examtopics.com/discussions/microsoft/view/67917-exam-ms-101-topic-3-question-107-discussion/>  
upvoted 1 times

✉ **Greatone1** 2 weeks ago

5 and 2 from ms 101

Reference:

<https://docs.microsoft.com/en-gb/exchange/security-and-compliance/mail-flow-rules/inspect-message-attachments>

upvoted 1 times

✉ **DiligentSam** 3 weeks ago

i think

user 1 receive 3 notification

User2 receive 3 notification

upvoted 1 times

✉ **faeem** 3 weeks ago

For user2, there are 3 files with 3 or more IP's. Why would user2 not receive 3 notifications?

upvoted 1 times

✉ **BlackCat9588** 3 weeks, 1 day ago

It should be 3 & 0 ?

upvoted 1 times

✉ **kavikumar** 3 weeks ago

It should be 4 & 3 ..right?

upvoted 3 times

✉ **BlackCat9588** 2 weeks, 5 days ago

Txt file is not under scope. User 1 =3.

Rule 3 cannot be appear as Rule 2 is fully cover with Rule 2.

So, I think User 2 =0

upvoted 2 times

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's Microsoft SharePoint site.

What should you do?

- A. From the SharePoint admin center, modify the sharing settings.
- B. From the SharePoint site, create an alert.
- C. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.
- D. From the Microsoft 365 Defender portal, create an alert policy.

**Correct Answer:** C

✉  **Paul\_white** 1 week, 6 days ago

ANSWER IS A!!!!

upvoted 1 times

✉  **Paul\_white** 1 week, 6 days ago

D. From the Microsoft 365 Defender portal, create an alert policy.

upvoted 1 times

✉  **Greatone1** 2 weeks ago

A. From the Microsoft 365 Defender portal, create an alert policy

upvoted 2 times

✉  **DiligentSam** 2 weeks, 4 days ago

Ref:

<https://www.examtopics.com/discussions/microsoft/view/94880-exam-ms-101-topic-2-question-118-discussion/>

upvoted 1 times

✉  **Hard1k** 1 month, 1 week ago

**Selected Answer: D**

D. From the Microsoft 365 Defender portal, create an alert policy.

An alert policy can be used to send notifications when certain events occur, such as when a file or folder is shared from a SharePoint site.

upvoted 4 times

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

From Microsoft Defender for Endpoint, you turn on the Allow or block file advanced feature.

You need to block users from downloading a file named File1.exe.

What should you use?

- A. a suppression rule
- B. an indicator
- C. a device configuration profile

**Correct Answer: B**

 **Paul\_white** 1 week, 6 days ago

To block users from downloading a file named File1.exe in Microsoft Defender for Endpoint, you should use an \*\*indicator\*\* (B). An indicator in Microsoft Defender for Endpoint is a security tool that allows you to block or allow files, URLs, domains, and IP addresses. Here's how you can do it:

1. Sign in to the Microsoft 365 Defender portal.
2. Under Endpoints, go to Settings.
3. Under the Rules heading, you will find the Indicators option.
4. Here, you can add the file (File1.exe) that you want to block.

Please note that a suppression rule (A) is used to stop alerts from being triggered by known safe files and behaviors. A device configuration profile (C) is used to manage settings and features on devices in your organization.

upvoted 1 times

 **ninjanaja** 1 month ago

**Selected Answer: B**

Correct Answer

<https://www.examtopics.com/discussions/microsoft/view/68006-exam-ms-101-topic-2-question-32-discussion/>

upvoted 4 times

 **Hard1k** 1 month, 1 week ago

**Selected Answer: C**

C. a device configuration profile.

A device configuration profile is used to configure settings on devices that are enrolled in Microsoft Defender for Endpoint. You can use a device configuration profile to block users from downloading a file by adding the file to the Block list.

upvoted 1 times

 **Paul\_white** 1 week, 6 days ago

PLEASE STOP MISLEADING PEOPLE

upvoted 1 times

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Exchange Administrator

You need to compare the permissions of each role. The solution must minimize administrative effort.

Which portal should you use?

- A. the Microsoft Purview compliance portal
- B. the Microsoft 365 admin center
- C. the Microsoft 365 Defender portal
- D. the Microsoft Entra admin center

**Correct Answer: A**

 **Casticod** Highly Voted 1 month, 1 week ago

**Selected Answer: B**

Should be B

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/admin-roles-page?view=o365-worldwide#compare-roles>

upvoted 5 times

 **DiligentSam** 3 weeks, 2 days ago

Check it in my tenant

Role - Role assignments - Azure AD / Intune / Billing - Choosing 2 Role - click button "compare Roles"

upvoted 1 times

 **ExamCheater1993** 4 weeks ago

Checked it in a tenant, this guy is right.

upvoted 2 times

 **Vincent1966** 1 month ago

I agree B: <https://admin.microsoft.com/#/rbac/directory/compare>

upvoted 2 times

 **AK\_1234** Most Recent 1 week, 2 days ago

D- Entra Admin center

upvoted 1 times

 **Greatone1** 1 week, 6 days ago

Answer is Entra Admin center

<https://www.examtopics.com/discussions/microsoft/view/122192-exam-sc-300-topic-1-question-62-discussion/>

upvoted 1 times

 **Hard1k** 1 month, 1 week ago

**Selected Answer: D**

D. the Microsoft Entra admin center.

The Microsoft Entra admin center is the new unified portal for managing Azure AD and Microsoft 365 identities. It provides a single pane of glass for managing users, groups, roles, and permissions.

To compare the permissions of each role in Azure AD, you can use the Role assignments blade in the Microsoft Entra admin center. This blade shows all of the roles that are assigned to each user, and you can easily compare the permissions of each role.

upvoted 1 times

 **smiff** 2 weeks, 5 days ago

yes it is possible, but when it comes to built-in comparison feature, admin center is the answer, you can try

upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

You plan to create the data loss prevention (DLP) policies shown in the following table.

Name	Apply to location
DLP1	Exchange email
DLP2	SharePoint sites
DLP3	OneDrive accounts

You need to create DLP rules for each policy.

Which policies support the sender is condition and the file extension is condition? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Sender is condition:

DLP1 only  
DLP2 only  
DLP3 only  
DLP2 and DLP3 only  
DLP1, DLP2, and DLP3

File extension is condition:

DLP1 only  
DLP2 only  
DLP3 only  
DLP2 and DLP3 only  
DLP1, DLP2, and DLP3

**Answer Area**

Sender is condition:

**DLP1 only**  
DLP2 only  
DLP3 only  
DLP2 and DLP3 only  
DLP1, DLP2, and DLP3

File extension is condition:

DLP1 only  
DLP2 only  
DLP3 only  
**DLP2 and DLP3 only**  
**DLP1, DLP2, and DLP3**

**Correct Answer:**

 **DiligentSam** 2 weeks, 6 days ago

Correct

upvoted 1 times

 **cb0900** 2 weeks, 6 days ago

Given answers are correct.

<https://learn.microsoft.com/en-us/purview/dlp-policy-reference?view=o365-worldwide#dlp-platform-limitations-for-conditions>

<https://www.examtopics.com/discussions/microsoft/view/94555-exam-ms-101-topic-3-question-152-discussion/>

upvoted 2 times

You have a Microsoft 365 E5 subscription that contains a user named User1.

You create a retention label named Retention1 that is published to all locations.

You need to ensure that User1 can label email messages by using Retention1 as soon as possible.

Which cmdlet should you run in Microsoft Exchange Online PowerShell?

- A. Start-ManagedFolderAssistant
- B. Start-MpScan
- C. Start-AppBackgroundTask
- D. Start-Process

**Correct Answer: A**

 **Paul\_white** 1 week, 6 days ago

A seems to be most likely correct, based on what the MS PowerShell reference says: <https://learn.microsoft.com/en-us/powershell/module/exchange/start-managedfolderassistant?view=exchange-ps>

upvoted 1 times

 **AlfaExamPro** 2 weeks, 3 days ago

<https://www.examtopics.com/discussions/microsoft/view/110773-exam-ms-101-topic-3-question-167-discussion/>

upvoted 1 times

You have a Microsoft 365 E5 tenant.

You create an auto-labeling policy to encrypt emails that contain a sensitive info type. You specify the locations where the policy will be applied.

You need to deploy the policy.

What should you do first?

- A. Run the policy in simulation mode.
- B. Configure Azure Information Protection analytics.
- C. Review the sensitive information in Activity explorer.
- D. Turn on the policy.

**Correct Answer: A**

 **Paul\_white** 1 week, 6 days ago

Simulation mode is unique to auto-labeling policies and woven into the workflow. You can't automatically label documents and emails until your policy has run at least one simulation.

<https://www.examtopics.com/discussions/microsoft/view/56712-exam-ms-101-topic-3-question-92-discussion/>

upvoted 2 times

**HOTSPOT**

From the Microsoft Purview compliance portal, you create a retention policy named Policy1.

You need to prevent all users from disabling the policy or reducing the retention period.

How should you configure the Azure PowerShell command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

-Identity "Policy1"  
\$true  
-enabled  
-Force  
-RestrictiveRetention  
-RetentionPolicyTagLinks  
-SystemTag

**Correct Answer:**

-Identity "Policy1"  
\$true  
-enabled  
-Force  
-RestrictiveRetention  
-RetentionPolicyTagLinks  
-SystemTag

**DiligentSam** 2 weeks, 4 days ago

The Given answer is correct  
upvoted 1 times

**cb0900** 2 weeks, 6 days ago

Supplied answer correct.

<https://www.examtopics.com/discussions/microsoft/view/52125-exam-ms-101-topic-3-question-81-discussion/>  
upvoted 1 times

You have a Microsoft 365 E5 subscription. The subscription contains users that have the following types of devices:

- Windows 10
- Android
- iOS

On which devices can you configure the Endpoint DLP policies?

- A. Windows 10 only
- B. Windows 10 and Android only
- C. Windows 10 and iOS only
- D. Windows 10, Android, and iOS

**Correct Answer: A**

 **Paul\_white** 1 week, 6 days ago

A SI CORRECT

<https://www.examtopics.com/discussions/microsoft/view/93905-exam-ms-101-topic-1-question-100-discussion/>  
upvoted 1 times

 **jt2214** 4 weeks, 1 day ago

**Selected Answer: A**

A.Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10/11 and macOS (the three latest released major versions) devices. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer. You can then enforce protective actions on those items via DLP policies.

<https://learn.microsoft.com/en-us/purview/endpoint-dlp-learn-about>  
upvoted 2 times

**HOTSPOT**

Your company has a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Office 365 role group
User1	<i>None</i>	Compliance Data Administrator
User2	Global Administrator	<i>None</i>

You create a retention label named Label1 that has the following configurations:

- Retains content for five years
- Automatically deletes all content that is older than five years

You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:

- Applies to content that contains the word Merger
- Specifies the OneDrive accounts and SharePoint sites locations

You run the following command.

```
Set-RetentionCompliancePolicy Policy1 -RestrictiveRetention $true -Force
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	<input type="radio"/>	<input type="radio"/>
User2 can remove SharePoint sites from Policy1.	<input type="radio"/>	<input type="radio"/>
User2 can add the word Acquisition to Policy1.	<input type="radio"/>	<input type="radio"/>

**Answer Area**

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can remove SharePoint sites from Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can add the word Acquisition to Policy1.	<input checked="" type="radio"/>	<input type="radio"/>

 **DiligentSam** 3 weeks, 2 days ago

Correct

upvoted 2 times

 **vercracked\_007** 1 month ago

Correct, can add not remove

upvoted 2 times

 **Casticod** 1 month, 1 week ago

correct

Note: the second is no because: Set-RetentionCompliancePolicy Policy1 `"RestrictiveRetention \$true`

<https://www.examtopics.com/discussions/microsoft/view/50018-exam-ms-101-topic-3-question-21-discussion/>

upvoted 3 times

Question #222

*Topic 1*

You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.

During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint.

You need to prevent the user from sharing the credit card information by using email and SharePoint.

What should you configure?

- A. the locations of the DLP policy
- B. the conditions of the DLP policy rule
- C. the user overrides of the DLP policy rule
- D. the status of the DLP policy

**Correct Answer:** A

 **Greatone1** 5 days, 12 hours ago

The answer is correct

<https://www.examtopics.com/discussions/microsoft/view/16568-exam-ms-101-topic-3-question-40-discussion/>

upvoted 1 times

 **Paul\_white** 1 week, 6 days ago

A IS CORRECT

<https://www.examtopics.com/discussions/microsoft/view/16568-exam-ms-101-topic-3-question-40-discussion/>

upvoted 1 times

**HOTSPOT**

From the Microsoft Purview compliance portal, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)

The screenshot shows a SharePoint 'Documents' library. At the top, there's a blue header bar with the SharePoint logo and a 'Site1' title. Below the header is a toolbar with 'Search Documents', 'New', 'Upload', 'Quick edit', 'Sync', and other navigation icons. The main area is titled 'Documents' and lists three files:

Name	Modified	Modified By
File1.docx	About a minute ago	Prvi
File2.docx	A few seconds ago	Prvi
File3.docx	A few seconds ago	Prvi

Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User1:

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

**Answer Area**

User1:

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

Correct Answer:

User2:

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

✉ **Paul\_white** 1 week, 6 days ago

USER1: FILE1 & 2  
USER2: FILE 1 & 2

<https://www.examtopics.com/discussions/microsoft/view/67675-exam-ms-101-topic-2-question-89-discussion/>  
upvoted 1 times

✉ **JensV** 3 weeks, 3 days ago

File 2 sends a warning, but can be viewed by both users  
Access to File 3 is restricted and only Prvi has access  
upvoted 1 times

✉ **ninjanaja** 1 month ago

File1 and File2 for both users.  
upvoted 2 times

Question #224

Topic 1

You have a Microsoft 365 subscription that uses retention policies.

You implement a preservation lock on a retention policy that is assigned to all executive users.

Which two actions can you perform on the retention policy after you implemented the preservation lock? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Add locations to the policy.
- B. Reduce the duration of policy.
- C. Remove locations from the policy.
- D. Extend the duration of the policy.
- E. Disable the policy.

**Correct Answer: AD**

✉ **Paul\_white** 1 week, 6 days ago

YOU CAN ONLY ADD LOCATIONS AND EXTEND THE DURATION  
upvoted 1 times

✉ **DiligentSam** 2 weeks, 1 day ago

<https://www.examtopics.com/discussions/microsoft/view/67142-exam-ms-101-topic-3-question-36-discussion/>  
upvoted 1 times

✉ **Milad666** 2 weeks, 3 days ago

Answer is Wrong. Correct Answer BCE  
MS Doc :

"Preservation Lock locks a retention policy or retention label policy so that no one—including a global admin—can turn off the policy, delete the policy, or make it less restrictive. This configuration might be needed for regulatory requirements and can help safeguard against rogue administrators."

<https://learn.microsoft.com/en-us/purview/retention-preservation-lock>  
upvoted 1 times

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso.com	Member
User2	User2@sub.contoso.com	Member
User3	User3@adatum.com	Member
User4	User4@outlook.com	Guest
User5	User5@gmail.com	Guest

You create and assign a data loss prevention (DLP) policy named Policy1. Policy1 is configured to prevent documents that contain Personally Identifiable Information (PII) from being emailed to users outside your organization.

To which users can User1 send documents that contain PII?

- A. User2 only
- B. User2 and User3 only
- C. User2, User3, and User4 only
- D. User2, User3, User4, and User5

**Correct Answer: B**

 **DiligentSam** 1 week, 6 days ago

User 2 and User 3  
their type are member. so they are user insider your ORG.  
upvoted 1 times

 **Paul\_white** 1 week, 6 days ago

B IS CORRECT

<https://www.examtopics.com/discussions/microsoft/view/48738-exam-ms-101-topic-3-question-32-discussion/>

upvoted 1 times

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365 and contains a mailbox named Mailbox1.

You plan to use Mailbox1 to collect and analyze unfiltered email messages.

You need to ensure that Defender for Office 365 takes no action on any inbound emails delivered to Mailbox1.

What should you do?

- A. Configure a retention policy for Mailbox1.
- B. Create a mail flow rule.
- C. Configure Mailbox1 as a SecOps mailbox.
- D. Place a litigation hold on Mailbox1.

**Correct Answer: D**

 **siulas** Highly Voted 1 month, 1 week ago

**Selected Answer: C**

<https://www.examtopics.com/discussions/microsoft/view/94552-exam-ms-101-topic-3-question-148-discussion/>  
upvoted 9 times

 **TBGarner** Most Recent 2 weeks, 5 days ago

**Selected Answer: C**

SecOps mailbox allows you to collect unfiltered messages.  
upvoted 3 times

**HOTSPOT**

- You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1.

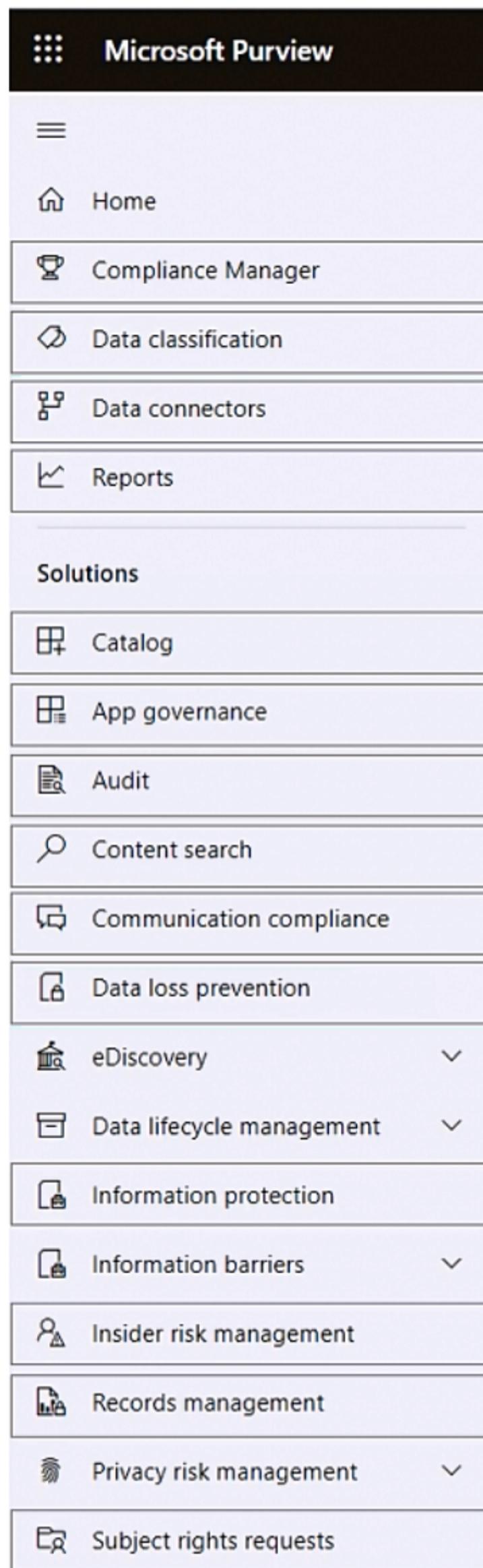
You need to perform the following tasks:

- Create a sensitive info type named SIT1 based on a regular expression.
- Add a watermark to all new documents that are matched by SIT1.

Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

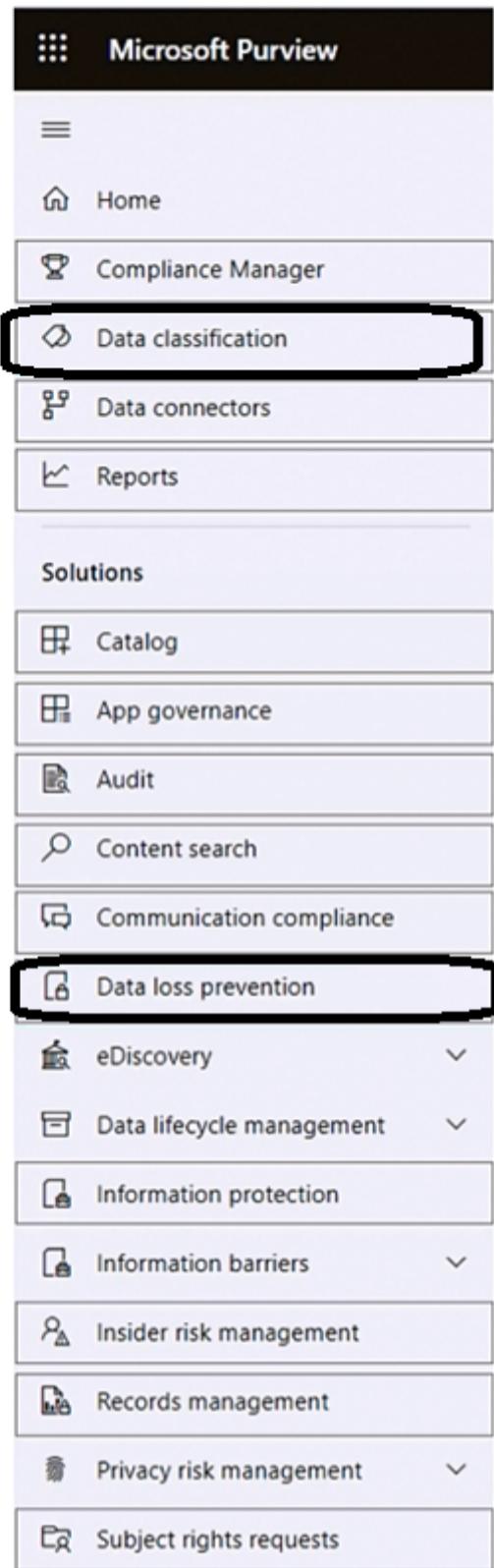
### Answer Area



The image shows the Microsoft Purview navigation menu. At the top is a black header bar with the Microsoft Purview logo. Below the header is a light gray sidebar containing a vertical list of menu items. The items are organized into sections: 'Home', 'Compliance Manager', 'Data classification', 'Data connectors', 'Reports', 'Solutions', and several expanded sections under 'Information protection'.

- Home
- Compliance Manager
- Data classification
- Data connectors
- Reports
- Solutions
  - Catalog
  - App governance
  - Audit
  - Content search
  - Communication compliance
  - Data loss prevention
  - eDiscovery
  - Data lifecycle management
  - Information protection
    - Information barriers
    - Insider risk management
    - Records management
    - Privacy risk management
    - Subject rights requests

Answer Area



Correct Answer:

Paul\_white 1 week, 6 days ago

<https://www.examtopics.com/discussions/microsoft/view/110776-exam-ms-101-topic-3-question-169-discussion/>  
upvoted 1 times

kavikumar 3 weeks, 2 days ago

Data Classification to create the sensitive info type  
Information Protection to apply the label\watermark

<https://www.examtopics.com/discussions/microsoft/view/110776-exam-ms-101-topic-3-question-169-discussion/>  
upvoted 4 times

You have a Microsoft 365 subscription.

You have a data loss prevention (DLP) policy that blocks sensitive data from being shared in email messages.

You need to modify the policy so that when an email message containing sensitive data is sent to both external and internal recipients, the message is only prevented from being delivered to the external recipients.

What should you modify?

- A. the policy rule exceptions
- B. the DLP policy locations
- C. the policy rule conditions
- D. the policy rule actions

**Correct Answer:** C

✉️👤 GLL 1 week, 4 days ago

Should be D the action  
upvoted 1 times

✉️👤 Paul\_white 1 week, 6 days ago

D POLICY RULE ACTION

To modify the data loss prevention (DLP) policy so that when an email message containing sensitive data is sent to both external and internal recipients, the message is only prevented from being delivered to the external recipients, you should modify:

\*\*D. the policy rule actions\*\*

Here's the rationale:

1. \*\*Policy Rule Actions\*\*: In a DLP policy, you can specify the actions to take when a policy violation is detected. In this case, you want to block the message from being delivered to external recipients while allowing it to be delivered to internal recipients.

2. \*\*Policy Rule Conditions\*\*: The conditions define what triggers the policy. In this scenario, you don't need to modify the conditions; you want to focus on what happens when a violation occurs.

So, to achieve the desired behaviour, you should modify the policy rule actions to block the message for external recipients while allowing it for internal recipients.

upvoted 1 times

✉️👤 jt2214 4 weeks ago

D. the policy rule actions.

You need to adjust the actions taken by the DLP policy when it detects sensitive data. Specifically, you want to allow internal recipients to receive the email while blocking it only for external recipients. This can be achieved by modifying the actions associated with the policy rule. Typically, you would set different actions for internal and external recipients to achieve this. Internal recipients can be allowed to receive the message, while external recipients can be blocked or receive a different notification.

upvoted 4 times

✉️👤 JensV 1 month ago

Should be D the action.  
There you can choose to block everyone or only people outside your organization  
upvoted 2 times

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365 and contains a user named User1.

User emails a product catalog in the PDF format to 300 vendors. Only 200 vendors receive the email message, and User1 is blocked from sending email until the next day.

You need to prevent this issue from reoccurring.

What should you configure?

- A. anti-spam policies
- B. Safe Attachments policies
- C. anti-phishing policies
- D. anti-malware policies

**Correct Answer: A**

 **Paul\_white** 1 week, 6 days ago

GIVEN ANSWER IS CORRECT A - ANTI -SPAM

upvoted 1 times

You have a Microsoft 365 E5 subscription that contains the labels shown in the following table.

Name	Type
Label1	Sensitivity
Label2	Retention

You have the items shown in the following table.

Name	Stored in	Description
File1	Microsoft SharePoint	File document that has Label1 applied
File2	Microsoft Teams channel	File document that has Label2 applied
Mail1	Microsoft Exchange Online	Email message that has Label1 applied
Mail2	Microsoft Exchange Online	Email message that has Label2 applied

Which items can you view in Content explorer?

- A. File1 only
- B. File1 and File2 only
- C. File1 and Mail1 only
- D. File2 and Mail2 only
- E. File1, File2, Mail1, and Mail2

**Correct Answer:** C

 **siulas** Highly Voted 1 month, 1 week ago

**Selected Answer:** E

<https://www.examtopics.com/discussions/microsoft/view/103242-exam-ms-101-topic-3-question-159-discussion/>  
upvoted 5 times

 **Paul\_white** Most Recent 1 week, 6 days ago

Content explorer shows a current snapshot of the items that have a sensitivity label, a retention label or have been classified as a sensitive information type in your organization:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-content-explorer?view=o365-worldwide>  
upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 E5 tenant.

You create a data loss prevention (DLP) policy to prevent users from using Microsoft Teams to share internal documents with external users.

To which two locations should you apply the policy? To answer, select the appropriate locations in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

## Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

ⓘ Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> Off	✉ Exchange email		
<input checked="" type="checkbox"/> Off	🌐 SharePoint sites		
<input checked="" type="checkbox"/> Off	☁ OneDrive accounts		
<input checked="" type="checkbox"/> Off	📠 Teams chat and channel messages		
<input checked="" type="checkbox"/> Off	💻 Devices		
<input checked="" type="checkbox"/> Off	🔐 Microsoft Cloud App Security		
<input checked="" type="checkbox"/> Off	🗄 On-premises repositories		

**Answer Area**

## Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

ⓘ Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

Correct Answer:

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> Off	✉ Exchange email		
<input checked="" type="checkbox"/> Off	🌐 SharePoint sites		
<input checked="" type="checkbox"/> Off	☁ OneDrive accounts		
<input checked="" type="checkbox"/> Off	📠 Teams chat and channel messages		
<input checked="" type="checkbox"/> Off	💻 Devices		
<input checked="" type="checkbox"/> Off	🔐 Microsoft Cloud App Security		
<input checked="" type="checkbox"/> Off	🗄 On-premises repositories		

 **cb0900** 2 weeks, 1 day ago

Answer is correct:

Sharepoint

Onedrive

<https://www.examtopics.com/discussions/microsoft/view/95079-exam-ms-101-topic-3-question-146-discussion/>

Reading the question for the first time I would have said Teams chat and channel messages and Sharepoint. However, the question states 'documents' and according to the link this would require Onedrive and Sharepoint.

<https://learn.microsoft.com/en-us/purview/dlp-microsoft-teams?view=o365-worldwide>

upvoted 4 times

**HOTSPOT**

You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint site named Site1. Site1 contains the files shown in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	5

You create a sensitivity label named Sensitivity1 and an auto-label policy that has the following configurations:

- Name: AutoLabel1
- Label to auto-apply: Sensitivity1
- Choose locations where you want to apply the label: Site1

The Define content that contains sensitive info settings for AutoLabel1 is shown in the following exhibit.

## Define content that contains sensitive info

Choose a category of industry regulations to see the classification groups you can use to classify that information or create a custom group.

The screenshot shows the 'Define content that contains sensitive info' dialog. In the 'Content contains' section, 'Default1' is selected under 'Any of these'. The 'Sensitive info types' section shows a rule for 'IP Address' set to 'High confidence' with an 'Instance count' of '2 to Any'. There are buttons for 'Add', 'Create group', and 'Add condition'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

### Answer Area

Statements	Yes	No
Sensitivity1 is applied to File1.docx.	<input type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File2.txt.	<input type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File3.xlsx.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
Sensitivity1 is applied to File1.docx.	<input type="radio"/>	<input checked="" type="checkbox"/>
Sensitivity1 is applied to File2.txt.	<input type="radio"/>	<input checked="" type="checkbox"/>
Sensitivity1 is applied to File3.xlsx.	<input checked="" type="checkbox"/>	<input type="radio"/>

✉  **DiligentSam** 1 week, 5 days ago

correct

upvoted 1 times

✉  **AlfaExamPro** 2 weeks, 3 days ago

correct

<https://www.examtopics.com/discussions/microsoft/view/56718-exam-ms-101-topic-3-question-95-discussion/>

upvoted 3 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1. Site1 contains the files shown in the following table.

Name	Number of IP addresses in the file
File1	2
File2	3

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Name	Content contains	Policy tip	If there is a match, stop processing	Priority
Rule1	3 or more IP addresses	Tip1	No	0
Rule2	1 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

You apply DLP1 to Site1.

Which policy tip is displayed for each file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

File1:

Tip2 only

Tip3 only

Tip2 and Tip3

File2:

Tip1 only

Tip3 only

Tip1 and Tip2 only

Tip1, Tip2, and Tip3

## Answer Area

File1:

Tip2 only
Tip3 only
Tip2 and Tip3

Correct Answer:

File2:

Tip1 only
Tip3 only
Tip1 and Tip2 only
Tip1, Tip2, and Tip3

✉ **Casticod** Highly Voted 1 month, 1 week ago

Tip 1 is configuring to no Stop The rule, In the second option should be Tip 1 and 2  
upvoted 8 times

✉ **Paul\_white** 1 week, 6 days ago

WHICH MEANS

FILE1: TIP2

FILE2: TIP 1 & 3

upvoted 1 times

✉ **Paul\_white** 1 week, 5 days ago

SORRY FOR THE TYPO

FILE1: TIP2

FILE2: TIP1 & 2

upvoted 1 times

✉ **Paul\_white** Most Recent 1 week, 5 days ago

It's possible for content to match several rules in a DLP policy, but only the policy tip from the most restrictive, highest-priority rule will be shown. For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips?view=o365-worldwide>

upvoted 1 times

✉ **Paul\_white** 1 week, 6 days ago

FILE1: TIP2 ONLY

FILE2: TIP 2 & 3

upvoted 1 times

✉ **cb0900** 2 weeks, 1 day ago

Similar question:

<https://www.examtopics.com/discussions/microsoft/view/82220-exam-ms-500-topic-3-question-32-discussion/>

upvoted 2 times

✉ **ExamCheater1993** 3 weeks, 4 days ago

Anwser is correct.

upvoted 2 times

**Overview -**

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

**Existing Environment -****Active Directory Environment -**

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

**Network Infrastructure -**

Each office has a high-speed connection to the Internet.

Each office contains two domain controllers. All domain controllers are configured as DNS servers.

The public zone for fabrikam.com is managed by an external DNS server.

All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.

All shared company documents are stored on a Microsoft SharePoint Server farm.

**Requirements -****Planned Changes -**

Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.

Fabrikam plans to implement two pilot projects:

- Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
- Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.

Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.

**Technical Requirements -**

Fabrikam identifies the following technical requirements:

- All users must be able to exchange email messages successfully during Project1 by using their current email address.

- Users must be able to authenticate to cloud services if Active Directory becomes unavailable.
- A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.
- Microsoft 365 Apps for enterprise applications must be installed from a network share only.
- Disruptions to email access must be minimized.

#### Application Requirements -

Fabrikam identifies the following application requirements:

- An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
- The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

#### Security Requirements -

Fabrikam identifies the following security requirements:

- After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
- The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.
- After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
- The principle of least privilege must be used.

You are evaluating the required processes for Project1.

You need to recommend which DNS record must be created while adding a domain name for the project.

Which DNS record should you recommend?

- A. mail exchanger (MX)
- B. alias (CNAME)
- C. host information (HINFO)
- D. host (AAAA)

**Correct Answer: A**

 **DiligentSam** 1 week, 6 days ago

the mailboxes of 100 users in the sales department will be moved to Microsoft 365

Mailbox = MX Record

upvoted 1 times

 **Greatone1** 2 weeks ago

Given answer is correct for this one

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Teams Administrator role.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: B**

**HOTSPOT****Overview**

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named A. Datum Corporation.

**Environment****On-Premises Environment**

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins, Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

**Cloud Environment**

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure AD Premium P2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

- Password hash synchronization is enabled.
- Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk Administrator
Admin3	Security Administrator
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.

The Azure AD tenant has Security defaults enabled.

## Problem Statements

-  
Litware identifies the following issues:

- Admin1 cannot create conditional access policies.
- Admin4 receives an error when attempting to use SSPR.
- Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

## Requirements

## Planned Changes

-  
Litware plans to implement the following changes:

- Implement Microsoft Intune.
- Implement Microsoft Teams.
- Implement Microsoft Defender for Office 365.
- Ensure that users can install Office 365 apps on their device.
- Convert all the Windows 10 Pro devices to Windows 10 Enterprise ES.
- Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

## Technical Requirements

-  
Litware identifies the following technical requirements:

- Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
- Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
- Litware users must be able to invite A. Datum users to participate in the following activities:
  - Join Microsoft Teams channels.
  - Join Microsoft Teams chats.
  - Access shared files.
- Just in time access to critical administrative roles must be required.
- Microsoft 365 incidents and advisories must be reviewed monthly.
- Office 365 service status notifications must be sent to Admin2.
- The principle of least privilege must be used.

You need to ensure that Admin4 can use SSPR.

Which tool should you use, and which action should you perform? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Action:

- Enable app registrations.
- Enable password writeback.
- Enable password hash synchronization.
- Disable password hash synchronization.

Tool:

- Azure AD Connect
- Synchronization Rules Editor
- Microsoft Entra admin center

## Answer Area

Correct Answer:

Action:

- Enable app registrations.
- Enable password writeback.**
- Enable password hash synchronization.
- Disable password hash synchronization.

Tool:

- Azure AD Connect
- Synchronization Rules Editor**
- Microsoft Entra admin center**

✉️ **Greatone1** 1 week, 3 days ago

<https://www.examtopics.com/discussions/microsoft/view/107026-exam-ms-100-topic-13-question-1-discussion/>  
upvoted 1 times

✉️ **Greatone1** 1 week, 3 days ago

Correct answers are enable password write back and azure ad connect  
upvoted 1 times

✉️ **jakke91** 1 week, 6 days ago

Trick question as I would have normally said AADConnect, but:  
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr-writeback>  
upvoted 1 times

✉️ **spectre786** 1 week, 6 days ago

Could you please comment on all questions from 122 to 236, only when there is no existing comment already ? Thank you for your help.  
upvoted 1 times

**HOTSPOT****Overview**

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named A. Datum Corporation.

**Environment****On-Premises Environment**

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins, Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

**Cloud Environment**

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure AD Premium P2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

- Password hash synchronization is enabled.
- Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk Administrator
Admin3	Security Administrator
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.

The Azure AD tenant has Security defaults enabled.

## Problem Statements

-  
Litware identifies the following issues:

- Admin1 cannot create conditional access policies.
- Admin4 receives an error when attempting to use SSPR.
- Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

## Requirements

## Planned Changes

-  
Litware plans to implement the following changes:

- Implement Microsoft Intune.
- Implement Microsoft Teams.
- Implement Microsoft Defender for Office 365.
- Ensure that users can install Office 365 apps on their device.
- Convert all the Windows 10 Pro devices to Windows 10 Enterprise ES.
- Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

## Technical Requirements

-  
Litware identifies the following technical requirements:

- Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
- Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
- Litware users must be able to invite A. Datum users to participate in the following activities:
  - Join Microsoft Teams channels.
  - Join Microsoft Teams chats.
  - Access shared files.
- Just in time access to critical administrative roles must be required.
- Microsoft 365 incidents and advisories must be reviewed monthly.
- Office 365 service status notifications must be sent to Admin2.
- The principle of least privilege must be used.

You are evaluating the use of multi-factor authentication (MFA).

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.	<input type="radio"/>	<input type="radio"/>
Users must use the Microsoft Authenticator app to complete MFA.	<input type="radio"/>	<input type="radio"/>
After registering, users must use MFA for every sign-in.	<input type="radio"/>	<input type="radio"/>

## Answer Area

Statements	Yes	No
Correct Answer: Users will have 14 days to register for MFA after they sign in for the first time.	<input checked="" type="radio"/>	<input type="radio"/>
Users must use the Microsoft Authenticator app to complete MFA.	<input type="radio"/>	<input checked="" type="radio"/>
After registering, users must use MFA for every sign-in.	<input type="radio"/>	<input checked="" type="radio"/>

✉️  Paul\_white 1 week, 5 days ago

Just noticed that Tenant has Security defaults enabled!

Security defaults:

Requiring all users and admins to register for MFA using the Microsoft Authenticator app.

Challenging users with MFA, mostly when they show up on a new device or app, but more often for critical roles and tasks.

<https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-conditional-access?view=o365-worldwide#security-defaults>

Require all users to register for Azure AD Multi-Factor Authentication

All users in your tenant must register for multifactor authentication (MFA) in the form of the Azure AD Multi-Factor Authentication. Users have 14 days to register for Azure AD Multi-Factor Authentication by using the Microsoft Authenticator app.

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

Answer: YES, YES, NO

upvoted 2 times

✉️  Paul\_white 1 week, 6 days ago

YES, NO, NO

<https://www.examtopics.com/discussions/microsoft/view/83963-exam-ms-100-topic-16-question-1-discussion/>

upvoted 1 times

**Overview -**

Litware, Inc. is a consulting company that has a main office in Montreal and a branch office in Seattle.

Litware collaborates with a third-party company named A. Datum Corporation.

**Environment -****On-Premises Environment -**

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins, Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

**Cloud Environment -**

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure AD Premium P2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

- Password hash synchronization is enabled.
- Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk Administrator
Admin3	Security Administrator
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.

The Azure AD tenant has Security defaults enabled.

**Problem Statements -**

Litware identifies the following issues:

- Admin1 cannot create conditional access policies.
- Admin4 receives an error when attempting to use SSPR.
- Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

Requirements -

Planned Changes -

Litware plans to implement the following changes:

- Implement Microsoft Intune.
- Implement Microsoft Teams.
- Implement Microsoft Defender for Office 365.
- Ensure that users can install Office 365 apps on their device.
- Convert all the Windows 10 Pro devices to Windows 10 Enterprise ES.
- Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

Technical Requirements -

Litware identifies the following technical requirements:

- Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
- Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
- Litware users must be able to invite A. Datum users to participate in the following activities:
  - Join Microsoft Teams channels.
  - Join Microsoft Teams chats.
  - Access shared files.
  - Just in time access to critical administrative roles must be required.
  - Microsoft 365 incidents and advisories must be reviewed monthly.
  - Office 365 service status notifications must be sent to Admin2.
  - The principle of least privilege must be used.

You need to configure just in time access to meet the technical requirements.

What should you use?

- A. entitlement management
- B. Azure AD Privileged Identity Management (PIM)
- C. access reviews
- D. Azure AD Identity Protection

**Correct Answer: B**

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant includes a user named User1.

You enable Azure AD Identity Protection.

You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege.

To which role should you add User1?

- A. Compliance Administrator
- B. Security Administrator
- C. Service Administrator
- D. User Administrator

**Correct Answer: B**

 **DiligentSam** 1 week, 3 days ago

base on this question <https://www.examtopics.com/discussions/microsoft/view/49685-exam-ms-100-topic-3-question-29-discussion/>  
upvoted 1 times

 **Paul\_white** 1 week, 6 days ago

CORRECT B!!!  
upvoted 1 times

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant includes a user named User1.

You enable Azure AD Identity Protection.

You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege.

To which role should you add User1?

- A. Compliance Administrator
- B. Security Reader
- C. Reports Reader
- D. User Administrator

**Correct Answer: B**

 **DiligentSam** 1 week, 3 days ago

<https://www.examtopics.com/discussions/microsoft/view/49685-exam-ms-100-topic-3-question-29-discussion/>  
upvoted 1 times

 **Paul\_white** 1 week, 6 days ago

SECURITY READER IS CORRECT!!!!  
upvoted 1 times

You have a Microsoft 365 E5 subscription.

You need to create a mail-enabled contact.

Which portal should you use?

- A. the Microsoft Teams admin center
- B. the Intune admin center
- C. the Microsoft 365 Defender portal
- D. the Exchange admin center

**Correct Answer:** D

 **Paul\_white** 1 week, 5 days ago

To create a mail-enabled contact in a Microsoft 365 E5 subscription, you should use the \*\*Exchange admin center\*\*<sup>34</sup>. This is where you can manage mail-enabled security groups and add new ones. You can also modify the email address attribute for each user account<sup>5</sup>. Please note that you need to sign in with an admin account to perform these actions<sup>45</sup>.

upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

The subscription has the following two anti-spam policies:

- Name: AntiSpam1
  - Priority: 0
  - Include these users, groups and domains
  - Users: User3
  - Groups: Group1
  - Exclude these users, groups and domains
  - Groups: Group2
  - Message limits
  - Set a daily message limit: 100
  
- Name: AntiSpam2
  - Priority: 1
  - Include these users, groups and domains
  - Users: User1
  - Groups: Group2
  - Exclude these users, groups and domains
  - Users: User3
  - Message limits
  - Set a daily message limit: 50

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	<input type="radio"/>	<input type="radio"/>
User2 can send a maximum of 50 email messages per day.	<input type="radio"/>	<input type="radio"/>
User3 can send a maximum of 100 email messages per day.	<input type="radio"/>	<input type="radio"/>

**Answer Area**

Statements	Yes	No
Correct Answer: User1 can send a maximum of 150 email messages per day.	<input type="radio"/>	<input checked="" type="checkbox"/>
User2 can send a maximum of 50 email messages per day.	<input checked="" type="checkbox"/>	<input type="radio"/>
User3 can send a maximum of 100 email messages per day.	<input type="radio"/>	<input checked="" type="checkbox"/>

✉️  **DiligentSam** 1 week, 2 days ago

I think User 3 match PolicyName:Anti-spam 1  
so the 3rd option is Yes  
upvoted 1 times

✉️  **DiligentSam** 1 week, 2 days ago

i am sorry , policy 1 exclude group2 ,and user3 is a member of group 2  
upvoted 1 times

✉️  **Paul\_white** 1 week, 6 days ago

NO, YES, NO AS VALIDATED BY BING GPT  
upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains a user named User1 and the administrators shown in the following table.

Name	Role
Admin1	Exchange Administrator
Admin2	Security Administrator
Admin3	User Administrator

User1 reports that after sending 1,000 email messages in the morning, the user is blocked from sending additional emails.

You need to identify the following:

- What administrators can unblock User1
- What to configure to allow User1 to send at least 2,000 emails per day without being blocked

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Administrators:

Admin1 only  
Admin2 only  
Admin1 and Admin2 only  
Admin2 and Admin3 only  
Admin1, Admin2, and Admin3

Settings:

Anti-spam  
Anti-phishing  
Anti-malware  
Advanced delivery  
Enhanced filtering

**Answer Area**

Administrators:

Admin1 only  
**Admin2 only**  
Admin1 and Admin2 only  
Admin2 and Admin3 only  
Admin1, Admin2, and Admin3

Correct Answer:

Settings:

**Anti-spam**  
Anti-phishing  
Anti-malware  
Advanced delivery  
Enhanced filtering

  **Greatone1** 1 week, 5 days ago

Answer is Admin 1 & Admin 2 - Anti Spam  
Exchange Admin do have permission to amend and set up Anti Spam policies.

upvoted 1 times

  **Paul\_white** 1 week, 6 days ago

ADMIN 1 & 2, - ANTI SPAM

<https://www.examtopics.com/discussions/microsoft/view/94096-exam-ms-101-topic-2-question-122-discussion/>

upvoted 1 times