

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

**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%)

✉  **osxvkwpfcfxobqjby** Highly Voted 9 months 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 7 times

✉  **AvoKikinha** Most Recent 2 months, 2 weeks ago

**Selected Answer: C**  
The correct answer is C. text (TXT).

When you add a domain name to Microsoft 365, you're asked to create a TXT record in DNS as a proof of domain ownership. This record won't affect anything else in your domain. It's only used to verify that you own the domain. After the domain is verified, you can use it with Microsoft 365 services. So, for Project1, a TXT record should be created. This will allow Microsoft 365 to verify that Fabrikam has control over the fabrikam.com DNS records.

upvoted 2 times

✉  **Charard** 3 months, 2 weeks ago

**Selected Answer: C**  
C is the correct answer. Links below.  
upvoted 1 times

✉  **AvoKikinha** 5 months, 2 weeks ago

The DNS record you should recommend is text (TXT). This type of record is typically used for domain ownership verification when setting up services like Microsoft 365. The TXT record will contain a generated code that Microsoft 365 services will check to confirm that the domain is owned by the person attempting to set up the service. So, the correct answer is C. text (TXT).

upvoted 3 times

✉  **mikl** 8 months 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** 8 months, 3 weeks ago

**Selected Answer: C**  
Its the first Step, C 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 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 (91%)	9%
---------	----

✉ **osxvkwpfcfxobqjby** Highly Voted 9 months 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 failback 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 15 times

✉ **PMR24875** 8 months ago

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

upvoted 1 times

✉ **PMR24875** 8 months ago

Never mind, didn't read well enough

upvoted 1 times

✉ **Charard** Most Recent 3 months, 2 weeks ago

**Selected Answer: C**

C is the correct answer as explanations below.

upvoted 2 times

✉ **Saj\_316** 5 months ago

**Selected Answer: C**

Hash Sync and SSO

upvoted 1 times

✉ **AvoKikinha** 5 months, 2 weeks ago

The authentication strategy you should implement for the pilot projects is password hash synchronization and seamless SSO. This approach will ensure that users can authenticate to cloud services even if Active Directory becomes unavailable, as required by the technical requirements. It also allows users to be signed in to on-premises and cloud-based applications automatically, as required by the security requirements. So, the correct answer is C. password hash synchronization and seamless SSO.

upvoted 1 times

✉ **TP447** 5 months, 2 weeks ago

PHS only is the right answer for me. SSO isn't needed until afterwards. I choose D

upvoted 2 times

✉ **rfree** 6 months, 2 weeks ago

**Selected Answer: A**

Should be A, as the question clearly states "during Project1 and Project2." During and not After the projects. After migration SSO is needed, but during only Pass Hash is needed.

upvoted 2 times

✉ **letters1234** 8 months, 1 week ago

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

upvoted 1 times

✉ **Greatone1** 8 months, 2 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 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.

Which role should you assign to User1?

- B. Security Reader
- C. Security Administrator
- D. Records Management

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉ **osxvkwpfcfxobqjby** Highly Voted 9 months ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/purview/microsoft-365-compliance-center-permissions>  
upvoted 7 times

✉ **Nilz76** Highly Voted 7 months 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 5 times

✉ **Kaybee2022** Most Recent 1 month, 3 weeks ago

Least privilege should be security administrator because it is stating that User1 should be able to review only.  
Answer C

<https://learn.microsoft.com/en-us/purview/compliance-portal-permissions>  
upvoted 1 times

✉ **Charard** 3 months, 2 weeks ago

**Selected Answer: B**

Security reader is the correct answer.  
upvoted 1 times

✉ **AvoKikinha** 5 months, 2 weeks ago

The role you should assign to User1 is Security Reader. This role in Microsoft 365 compliance center would allow User1 to view all DLP reports from the Microsoft Purview compliance portal, as required by the technical requirements. So, the correct answer is B. Security Reader.  
upvoted 2 times

✉ **Nocho** 6 months ago

B. Security Reader is the correct answer:  
Microsoft Documentation:  
Security Reader - View and investigate active threats to your Microsoft 365 users, devices, and content,  
upvoted 2 times

✉ **dede321** 6 months ago

To allow User1 to view all Data Loss Prevention (DLP) reports from the Microsoft Purview compliance portal, you should assign the Security Administrator role. The Security Administrator role in Microsoft 365 is responsible for configuring and managing security-related settings, including DLP policies and reports.

So, the correct answer is:

C. Security Administrator  
upvoted 1 times

✉ **imlearningstuffagain** 6 months, 3 weeks 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

**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

Last Sync

店铺: 学习小店66  
Enabled

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

osxvkwpcfxobqjby Highly Voted 9 months 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 25 times

□  **Charard** Most Recent 3 months, 2 weeks ago

Explanations below, but answer given is correct.

upvoted 2 times

□  **Jonnaz** 4 months, 2 weeks ago

Question 1:

Answer: both on-premises and cloud-based

Explanation: The principle of least privilege is about giving users only the access they need to perform their jobs. Since Fabrikam is moving to Microsoft 365, users will need to access both on-premises and cloud-based applications<sup>1</sup>. Implementing Azure AD Connect with single sign-on (SSO) allows users to access resources across both environments seamlessly.

Question 2:

Answer: only cloud-based

Explanation: If Active Directory becomes unavailable, users would not be able to authenticate against on-premises resources<sup>2</sup>. However, with the implementation of Azure AD Connect and cloud authentication methods like password hash synchronization and seamless SSO, users can still authenticate to cloud services and access cloud-based resources. This ensures business continuity during outages.

These answers align with the technical requirements of ensuring email exchange and authentication to cloud services during Project<sup>1</sup>, as well as minimizing disruptions to email access.

upvoted 2 times

□  **Moazzamfarooqiii** 2 months, 2 weeks ago

i dont think thats correct

upvoted 1 times

□  **aleper85** 4 months ago

I'm sorry, but I don't agree with you on question 1. If you look at the Azure AD Connect configuration on the screenshot, SSO has not been activated, it's "Disabled" state. The question clearly states "using SSO". So, for me its just on-premise only.

upvoted 2 times

□  **668cffd** 4 months ago

Seamless SSO ist not enabled, but that's not the question, so SSO is possible

upvoted 2 times

□  **Perycles** 3 months, 3 weeks ago

you're wrong : "Users CAN Access By sing SSO..." not "Users COULD access by using SSO.." so in the current state of Enrea ID Connect, it's not the case : Answer B is "cloud Only".

upvoted 1 times

□  **Perycles** 3 months, 3 weeks ago

WTF???? Seamless SSO is disabled >>> SSO will NOT Works.

upvoted 2 times

□  **CBZ57** 6 months, 4 weeks ago

1. Hash Password ENabled so you can access to both

2. cloud only

upvoted 2 times

□  **CheMetto** 6 months, 3 weeks 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** 6 months, 3 weeks 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 2 times

□  **gomezmax** 8 months, 1 week 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 9 months 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 18 times

✉ **Greatone1** Highly Voted 8 months, 2 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 5 times

✉ **samet5** Most Recent 4 days, 10 hours ago

**Selected Answer: C**

C is correct

upvoted 1 times

✉ **HelloItsSam** 1 month, 1 week ago

**Selected Answer: C**

Answer is C

upvoted 1 times

✉ **Charard** 3 months, 2 weeks ago

**Selected Answer: C**

C is the correct answer. Explanations given below.

upvoted 1 times

✉ **AvoKikinha** 5 months, 2 weeks ago

**Selected Answer: C**

You should use the Licenses blade in the Microsoft Entra admin center. This tool allows you to view all the users who are licensed for Office 365 through a group membership, along with the name of the group used to assign the license. So, the correct answer is C. the Licenses blade in the Microsoft Entra admin center. Please note that you need to have the necessary permissions to access this information.  
upvoted 2 times

✉ **NrdAlert** 6 months ago

**Selected Answer: C**

From the M365 admin center billing->licenses->product sub page: "Manage group-based licenses in the Microsoft Entra admin center."  
upvoted 1 times

✉ **Clinton** 6 months ago

You can also view and manage this in 365 Admin Center (D).

Billing-->Licenses-->Select Product-->Groups

upvoted 2 times

✉ **NrdAlert** 6 months ago

Text from the top of this very spot... Manage and view licenses and apps for your users. Manage group-based licenses in the Microsoft Entra admin center.

upvoted 1 times

曰 **Nocho** 6 months ago

**Selected Answer: C**

Correct answer is C.

upvoted 1 times

曰 **larteyotoo** 6 months, 3 weeks ago

C is Correct

upvoted 1 times

曰 **Nilz76** 7 months 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

曰 **sherifhamed** 7 months, 1 week 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

曰 **ATHOOS** 8 months, 1 week ago

**Selected Answer: C**

Correct Answer is C

upvoted 2 times

曰 **gomezmax** 8 months, 2 weeks ago

D is wrong Answer, the Answer should be Is C

upvoted 3 times

曰 **Dtriminio** 8 months, 4 weeks 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

- eq "Guest"
- in "Guest"
- ne "Guest"
- notmatch "Member"

) and (user.department

- contains "Support"
- in "Support"
- match "Support"
- startsWith "Sup"

## Answer Area

Correct Answer: (user.userType ) and (user.department

- eq "Guest"
- in "Guest"
- ne "Guest"
- notmatch "Member"

) and (user.department

- contains "Support"
- in "Support"
- match "Support"
- startsWith "Sup"

④  **Percyles** Highly Voted 9 months ago

Correct answers

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

Be carrefull : Case Sensitive

upvoted 13 times

④  **Blixa** 5 months, 1 week ago

Nope, not case sensitive

upvoted 1 times

④  **Jslei** Most Recent 7 months, 3 weeks ago

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

upvoted 2 times

④  **imlearningstuffagain** 6 months, 3 weeks 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 2 times

④  **gomezmax** 7 months, 3 weeks ago

Correct

upvoted 2 times

④  **vinch** 8 months ago

Good answer is -eq -match

upvoted 1 times

④  **imlearningstuffagain** 6 months, 2 weeks ago

Nope, 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 3 times

④  **nenge** 8 months, 1 week 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 2 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

**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 9 months 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 16 times

👤 **examcrammer** Most Recent 1 week, 1 day ago

This is correct and a good question. See <https://learn.microsoft.com/en-us/microsoft-365/enterprise/add-several-users-at-the-same-time?view=o365-worldwide#:~:text=Expand%20table-,User%20data%20column%20label,-Maximum%20character%20length>  
upvoted 1 times

👤 **Amir1909** 3 months ago

Correct  
upvoted 1 times

👤 **Blixa** 5 months, 1 week ago

Correct, but bad question since there are 4 required parameters in usercreatetemplate.csv:  
[displayName] Required,User name [userPrincipalName] Required,Initial password [passwordProfile] Required,Block sign in (Yes/No)  
[accountEnabled] Required  
upvoted 2 times

👤 **gomezmax** 7 months, 3 weeks 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, ~~店铺：学习小店66~~ 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%)

✉  **Percles** Highly Voted 9 months 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 25 times

✉  **letters1234** Highly Voted 8 months, 1 week ago

**Selected Answer: C**

All users and the two deparments, three groups  
upvoted 7 times

✉  **bleedinging** Most Recent 6 months, 2 weeks ago

**Selected Answer: C**

All, Research, and Marketing. 3 groups.  
upvoted 4 times

店铺：学习小店66

店铺：学习小店66

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

店铺：学习小店66

### Active issues

Issue title	Affected service	Issue type

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%)

✉️  **letters1234**  8 months, 1 week 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 9 times

✉️  **CharlesS76**  3 weeks, 6 days ago

**Selected Answer: C**

I tested in my lab and message center reader can only see these two options under Health:

Message Center, Software Updates. So the answer cannot be A. The answer is C.

upvoted 1 times

✉️  **Moazzamfarooqiiii** 2 months, 2 weeks ago

Option A is correct

The "Message Center Reader" role provides users with the ability to view messages and advisories related to the service health in the Microsoft 365 Message Center. This includes information about service issues, updates, and other important messages that might impact the service. Assigning the Message Center Reader role to User1 will grant them the necessary permissions to access and review advisories in the Message Center, allowing them to investigate service health issues.

upvoted 1 times

✉️  **Nilz76** 7 months 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 4 times

✉️  **rfree** 8 months, 1 week 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** 8 months, 1 week 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** 8 months, 1 week ago

Message center it's not the same of service health

upvoted 2 times

✉️  **Casticod** 8 months, 3 weeks ago

**Selected Answer: C**

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

upvoted 3 times

✉️  **Venusaur** 8 months, 3 weeks 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

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

**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 -

店铺：学习小店66

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"/>

店铺：学习小店66

**Answer Area**

**Statements**

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

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

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

<input checked="" type="radio"/> Yes	<input type="radio"/> No
<input type="radio"/> Yes	<input checked="" type="radio"/> No
<input checked="" type="radio"/> Yes	<input type="radio"/> No

Correct Answer:

  8 months, 3 weeks ago

Yes, Yes, Yes ??

upvoted 29 times

  6 months, 2 weeks ago

Yes No Yes

Eligible assignments require the member of the role to perform an action to use the role. Actions might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.

upvoted 12 times

□ **FireBeast** Most Recent 1 month ago

Y,Y,Y, because if activate it, he is be able to Manage Exchange online

upvoted 1 times

□ **Davito** 2 months, 1 week ago

Question 2 is no because of Known Issues with role-assignable groups:

"If an administrator role is assigned to a role-assignable group instead of individual users, members of the group will not be able to access Rules Organization, or Public Folders in the new Exchange admin center. The workaround is to assign the role directly to users instead of the group." Thus Admin2 will not be able to fully manage Exchange Online.

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept#known-issues>

upvoted 3 times

□ **solderboy** 4 months ago

Answer: YNY

The type of the assignment

- Eligible assignments require the member of the role to perform an action to use the role. Actions might include activation, or requesting approval from designated approvers.
- Active assignments don't require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role.

The duration of the assignment, using start and end dates or permanent. For eligible assignments, the members can activate or requesting approval during the start and end dates. For active assignments, the members can use the assign role during this period of time.

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure>

upvoted 6 times

□ **TP447** 5 months, 2 weeks ago

YNY for me - N only because User 2 would need to activate the role they are eligible for first (that is an important detail). It is an ambiguous question though..

upvoted 8 times

□ **GLLimaBR** 2 months, 2 weeks ago

I agree. There is ambiguity and it left me in doubt, as there is nothing to suggest that eligibility is relevant to the issue. Being eligible or active within the proposed time window and scope of functions, all answers are "Yes", from my point of view.

upvoted 4 times

□ **mikl** 2 weeks, 5 days ago

I could not agree more - this is a totally stupid question. Yes he can - but he needs to activate, now a days most administrative roles should also be PIM enabled, that does not mean I can't do a certain task.

upvoted 1 times

□ **CheMetto** 6 months, 3 weeks ago

Yes no Yes. The second is no. It's elegible, 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 3 times

□ **Darekms0** 6 months, 3 weeks ago

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

upvoted 1 times

□ **imlearningstuffagain** 6 months, 2 weeks ago

You cannot be more spot on, if the line would read "on june 20 Admin2 cn PARTIALLY manage exchange" it would be a Yes.

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

upvoted 1 times

□ **Nilz76** 7 months 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 7 times

amurp35 7 months, 3 weeks 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 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 3 times

mpetlk 7 months, 3 weeks 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 password.

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 4 times

vercracked\_007 7 months, 3 weeks ago

YNY

Statement 2 doesn't say that admin activates his role

upvoted 2 times

AMDf 8 months ago

Yes

?? - It depends

Yes

upvoted 2 times

Tedd\_TS 8 months, 3 weeks ago

Yes, Yes, Yes i think too

upvoted 3 times

Venusaur 8 months, 3 weeks 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 9 months 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

gbartumeu 8 months, 3 weeks ago

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

upvoted 9 times

cb0900 8 months, 2 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

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 (74%)

D (26%)

✉ gbartumeu Highly Voted 7 months, 3 weeks 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 39 times

✉ Xbmc66 4 months, 3 weeks ago

But user1 is listed if you look into the graph and user 1 is a security administrator.

If nothing is listed, then GA will receive a mail.. so the correct answer is only User1  
upvoted 2 times

✉ Xbmc66 4 months, 3 weeks ago

User 1 Only is the only correct answer  
upvoted 1 times

✉ Xbmc66 4 months, 3 weeks ago

Please moderator remove my previous messages, it is wrong! Correct answer is User 2 only :)  
upvoted 3 times

✉ ae88d96 Highly Voted 8 months, 1 week 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 13 times

✉️ **Ody** 5 months, 2 weeks ago

The question says "will be", but your explanation says "may be". Since there is no global privacy contact, Global Admins "will be" notified. The Technical Contact, may be contacted if warranted.

3. Add your privacy info for your users:

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.

upvoted 2 times

✉️ **WORKTRAIN** 7 months 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 2 times

✉️ **JeSuisCertif** Most Recent 2 weeks, 6 days ago

<https://learn.microsoft.com/en-us/entra/fundamentals/properties-area>

upvoted 1 times

✉️ **ismaelo** 3 weeks, 1 day ago

The correct answer is "User 2 only", since the technical contact is for technical support and the privacy contact is in case of a data breach related to Microsoft Entra services. So they will contact the global administrators, User 2  
<https://learn.microsoft.com/en-us/entra/fundamentals/properties-area#:~:text=Esta%20persona%20tambi%C3%A9n,con%20Microsoft%20365>

upvoted 1 times

✉️ **DONPHYLO** 1 month ago

Utilisateurs 1 et 2 uniquement vu que l'énoncé de la question demande quels sont les utilisateurs et non pas quel utilisateur. Donc il est question du pluriel

upvoted 1 times

✉️ **JManuel** 1 month, 1 week ago

**Selected Answer: D**

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

upvoted 1 times

✉️ **JManuel** 1 month, 1 week ago

Correction, actually, B. there is no "Privacy contact".

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

"Providing customers with an ability to specify a dedicated privacy contact who will be notified in the event of a breach. Customers can specify this contact using the Privacy reader role settings for Message Center."

"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, which can be done in the Microsoft 365 admin center. In the event of personal data breach, resources assigned the Message Center Privacy reader role will be able to access the Message center to see relevant privacy notifications and, depending on their Message center preferences, may receive a related email."

upvoted 1 times

✉️ **KerrAvon** 2 months, 1 week ago

**Selected Answer: B**

Reference: <https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-azure-dynamics#customer-notification> This States "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" The key words are MAY BE. The question states WILL BE so in the absence of the privacy contact the GA will be notified.

upvoted 1 times

✉️ **spektrum1988** 3 months, 1 week ago

I believe B:

<https://learn.microsoft.com/en-us/entra/fundamentals/properties-area>

Technical contact. Type the email address for the person to contact for technical support within your organization.  
--> has nothing to do with the data breach

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

✉️ **Charard** 3 months, 2 weeks ago

**Selected Answer: B**

User2 only. There isn't a privacy contact listed, so MS will contact the GA.  
upvoted 3 times

✉️ **Hasa** 3 months, 3 weeks ago

In Microsoft 365, the Global Administrator is the default contact for security and privacy-related matters, including data breaches. If your tenant doesn't have a designated Global Privacy Contact, Microsoft will contact the Global Administrator in the event of a data breach.  
upvoted 1 times

✉️ **Jeeva1jev** 3 months, 4 weeks ago

**Selected Answer: D**

D option is right answer as Global Administrator and Technical contact will be notified  
upvoted 1 times

✉️ **neken123** 4 months ago

**Selected Answer: B**

Microsoft 365 is committed to notifying customers within 72 hours of breach declaration. The customer's tenant administrator will be notified. Tenant admin will be the GA not security admin.  
upvoted 2 times

✉️ **Zelda78** 4 months, 2 weeks ago

Answer to me is: B User2 Only

<https://learn.microsoft.com/en-us/entra/fundamentals/properties-area#add-your-privacy-info-on-azure-ad>

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.

upvoted 1 times

✉️ **Testtest123** 4 months, 3 weeks ago

In the event of a data breach, Microsoft typically contacts the primary point of contact listed in the service agreement or account details. This contact could be the global administrator, a technical person, or another designated individual depending on how the organization's account is set up with Microsoft.

upvoted 1 times

✉️ **benpatto** 5 months ago

Whenever its mentioning a 'data breach' type issue, the technical contact becomes void unless specified specifically. The technical contact is for day to day support with Microsoft. In this case, global admins are contacted as they hold the most control over the tenant and are the highest possible administrator position.

upvoted 1 times

✉️ **TP447** 5 months, 3 weeks ago

1 or more are notified by MS and that includes Global Admin and Technical contacts.

D is the answer for me.

upvoted 1 times

✉️ **bleedinging** 6 months, 2 weeks ago

**Selected Answer: B**

Since Global Privacy contact is blank it leaves the Global Admins only as Microsoft's contact.  
Technical Contact is who the users will use.

upvoted 2 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.

店铺：学习小店66

**Correct Answer: D**

*Community vote distribution*

D (100%)

✉️  **Greatone1** Highly Voted 8 months, 2 weeks ago

**Selected Answer: D**

Given answer is correct

upvoted 9 times

✉️  **AndrewsF** Most Recent 2 months, 3 weeks ago

In my opinion, the correct answer is D.

You don't need to rename a ".local" domain, you can just create an alternate login suffix for the routable domain and purchase the external domain. So D is the only answer that makes the most sense to me.

upvoted 1 times

✉️  **Nilz76** 7 months 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 4 times

✉️  **CheMetto** 6 months, 3 weeks 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

✉️  **Nocho** 6 months ago

It does not matter that they use a ".local" domain name.

When you configure your Microsoft tenant you need to provide your custom domain name.

When syncing users you either provide proxy address details corresponding to your custom domain name or you currently have an exchange server with the SMTP attributes. What your local AD domain is, doesn't matter.

upvoted 3 times

店铺：学习小店66

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**: 学习小店66  
Community vote distribution  
C (100%)

店铺: 学习小店66

✉  osxvkwpfcfxobqjby Highly Voted 9 months 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 16 times

✉  sherifhamed Highly Voted 7 months, 1 week 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 5 times

✉  Amir1909 Most Recent 3 months ago

C is correct

upvoted 1 times

✉  Kmkz83510 4 months, 3 weeks ago

Technically, option A could also work if it's a security-enabled M365 group, but the best answer would be C.

upvoted 3 times

✉  Nilz76 7 months 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 3 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** 店铺：学习小店66  
Community vote distribution

A (90%)

10%

店铺：学习小店66

✉  **Nilz76** Highly Voted  7 months 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 11 times

✉  **anonavia** Highly Voted  8 months, 2 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 5 times

✉  **SecAz0365** Most Recent  3 months, 2 weeks ago

**Selected Answer: C**

So if Auditing is enabled by default, why shouldn't you then choose for C?

<https://learn.microsoft.com/en-us/purview/insider-risk-management-policies>

Insider risk management policies determine which users are in-scope and which types of risk indicators are configured for alerts. You can quickly create a security policy that applies to all users in your organization or define individual users or groups for management in a policy.

upvoted 2 times

✉  **SecAz0365** 3 months, 2 weeks ago

So if Auditing is enabled by default, why shouldn't you then choose for C?

<https://learn.microsoft.com/en-us/purview/insider-risk-management-policies>

Insider risk management policies determine which users are in-scope and which types of risk indicators are configured for alerts. You can quickly create a security policy that applies to all users in your organization or define individual users or groups for management in a policy.

upvoted 1 times

✉  **benpatto** 5 months ago

**Selected Answer: A**

Gotta be A. The others don't really matter in this situation. Anything alert related would have an alert policy setup specifically, so auditing is the only reliable option. Power of deduction is a great thing xD

upvoted 2 times

✉  **osxzkwpfcfxobqjby** 9 months 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 2 times

✉  **GLLimaBR** 2 months, 2 weeks ago

Hello.

I believe the answer below will help you with this question:

"Audit logging is turned on by default for Microsoft 365 organizations. However, when setting up a new Microsoft 365 organization, you should verify the auditing status for your organization. For instructions, see the Verify the auditing status for your organization section in this article."

<https://learn.microsoft.com/en-us/purview/audit-log-enable-disable>

upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

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 (78%)

B (22%)

店铺：学习小店66

✉  **Nilz76** Highly Voted 7 months 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 13 times

✉  **sherifhamed** Highly Voted 7 months, 1 week 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 7 times

✉  **Omta** Most Recent 1 month, 1 week ago

**Selected Answer: D**

the point is data storage location configured during the onboarding process so we need to offboard device first then do onboarding again  
upvoted 1 times

✉  **neken123** 4 months ago

**Selected Answer: B**

Only if you are changing the tenant of the MS Defender for Endpoint, you would need to offboard the devices in the first tenant, otherwise offboarding not required just a restart.

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/announcing-a-streamlined-device-connectivity-experience-for/ba-p/3956236>

upvoted 4 times

✉  **pantcm** 8 months, 1 week ago

D is the correct answer

upvoted 1 times

✉  **gomezmax** 8 months, 2 weeks ago

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

upvoted 1 times

✉  **Greatone1** 8 months, 2 weeks ago

D is the correct answer from MS 101

upvoted 3 times

✉  **Dtriminio** 8 months, 4 weeks ago

**Selected Answer: D**

i will go with D  
upvoted 2 times

✉ **alecrobertburns** 8 months, 4 weeks 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 3 times

✉ **alecrobertburns** 8 months, 4 weeks 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** 9 months 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 3 times

店铺：学习小店66

✉ **osxzvkwpfcfxobqjby** 9 months 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 4 times

店铺：学习小店66

店铺：学习小店66

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%)

✉️  **Dtriminio** Highly Voted 8 months, 4 weeks 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 11 times

✉️  **sherifhamed** Highly Voted 7 months, 1 week ago

**Selected Answer: D**

In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & collaboration > Review > Restricted entities  
upvoted 6 times

✉️  **Tomtom11** Most Recent 2 months, 4 weeks ago

From the Book

To remove a user from the Restricted Entities page, perform the following steps:

1. In the Microsoft 365 Defender portal, navigate to Email & Collaboration and select Review > Restricted Entities.
2. On the Restricted Entities page, select the user to unblock by selecting the checkbox for the entity and then selecting the Unblock action that appears on the page.
3. In the Unblock User flyout menu, verify that the account isn't compromised and

upvoted 2 times

✉️  **Amir1909** 3 months ago

D is correct

upvoted 1 times

✉️  **Charard** 3 months, 2 weeks 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 2 times

✉️  **benpatto** 5 months ago

**Selected Answer: D**

With this specifically, think of where Anti-spam policies are setup. This is normally where you set a daily limit / hourly limit on emails. Once you've got that, most of these questions will always point to the same place.  
upvoted 2 times

✉️  **SandyBridge** 7 months, 2 weeks 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 3 times

✉ **Ruhansen** 7 months, 2 weeks ago

D is correct  
upvoted 1 times

✉ **RAG** 8 months, 4 weeks 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 4 times

Question #17 店铺: 学习小店66

Topic 1

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**  7 months 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 8 times

✉ **Charard**  3 months, 2 weeks ago

**Selected Answer: D**

See Nilz explanation, correct answer.

upvoted 2 times

✉ **Ruhansen** 7 months, 2 weeks ago

D - and assigned to different groups  
upvoted 1 times

✉ **Greatone1** 8 months, 2 weeks 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.

User2 can collect an investigation package from Device2.

User3 can isolate Device1.

**Answer Area**

**Statements**

User1 can run an antivirus scan on Device2.

User2 can collect an investigation package from Device2.

User3 can isolate Device1.

Correct Answer:

Nilz76 Highly Voted 7 months 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 21 times

✉  **sigvast** 5 months, 3 weeks ago

Correct. Collect an investigation package require at least "Alerts Investigation" permission.

upvoted 1 times

✉  **Greatone1**  8 months, 2 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 6 times

✉  **Charard**  3 months, 2 weeks ago

Given answer is correct.

upvoted 1 times

✉  **m2L** 4 months, 2 weeks ago

1) No: Even if alerts Investigation allows users to run a scan as explained in the link below, Device2 is not in user1's Scope. Otherwise, he cannot run a scan on Device 2. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/user-roles?view=o365-worldwide>

2) No

N)Yes

upvoted 2 times

✉  **mhmyz** 8 months, 1 week 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 3 times

✉  **hogehogehoge** 8 months, 1 week ago

Box3: No?

Because Defferent Group In User and Device.

upvoted 1 times

✉  **rinzler1** 8 months, 1 week ago

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

upvoted 9 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:

Alert  
 Threat  
 Compliance

Role:

Quarantine Administrator  
 Security Administrator  
 Organization Management  
 Communication Compliance Administrators

**Answer Area**

Policy type:

Alert  
 Threat  
 Compliance

Correct Answer:

Role:

Quarantine Administrator  
 Security Administrator  
 Organization Management  
 Communication Compliance Administrators

osxzvkwpcfxobqjby Highly Voted 9 months 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 33 times

sigvast 5 months, 3 weeks ago

The correct answer is :

- Alert
- Organization Management

"To create alert policies, you have to be assigned the Manage Alerts role or the Organization Configuration role in the compliance portal or the Defender portal."

<https://learn.microsoft.com/en-us/purview/alert-policies?redirectSourcePath=%252farticle%252f8927b8b9-c5bc-45a8-a9f9-96c732e58264#how-alert-policies-work>

Manage Alerts role is included in the following role groups :

- Compliance Administrator
- Compliance Data Administrator
- Organization Management
- Security Administrator
- Security Operator

Organization Configuration role is included in the following role groups :

- Compliance Administrator
- Compliance Data Administrator
- Organization Management

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

Security Administrator and Organization Management are correct answers but following the principle of least privilege, the correct role group is Organization Management.

upvoted 4 times

✉️ **sigvast** 5 months, 3 weeks ago

My bad, Security Administrator is the correct answer because Organization Management give more permissions ...

upvoted 9 times

店铺：学习小店66

✉️ **letters1234** Highly Voted 8 months, 1 week 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

✉️ **9326359** Most Recent 18 hours, 53 minutes ago

-Alert

-Security administrator

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-by-task>

upvoted 1 times

✉️ **neken123** 4 months ago

we just need the role to create the policy, so organization management role would be least privileged role

upvoted 1 times

✉️ **Jonnaz** 4 months, 2 weeks ago

I think it should be Threat instead of Alert and here's why:

An Alert policy in Microsoft 365 is typically used to track and respond to activity alerts, such as user and admin activities, malware threats, or data loss incidents. While you can create an alert policy to notify administrators when certain activities occur, it's not specifically designed to handle malware detections in email messages1.

On the other hand, a Threat policy (specifically, an anti-malware policy) in Microsoft 365 is designed to configure the settings that determine how malware detections are handled, including settings for notifications when a user receives an email that contains malware.

Therefore, while an Alert policy could potentially be used to achieve similar results, a Threat policy is the more appropriate and direct solution for this specific requirement.

upvoted 1 times

✉️ **m2L** 5 months ago

sigvast you are right the given answer is correct

upvoted 1 times

✉️ **TonyManero** 5 months, 4 weeks ago

Alert and Security Admin.

Please update the answers.

upvoted 5 times

店铺：学习小店66

✉️ **lolern123** 6 months ago

Correct me if im wrong, but people here saying that the Organization Management is not a role in purview and only exchange. Look at this bit.  
<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide>

Can someone break this down? To me it looks like that Organization Management is enough and that security administrator will give a lot of unnecessary access in this case.

For now sticking with the answer provided

- Alert
- Organization Management

upvoted 1 times

✉️ **Clinson** 6 months ago

Nevermind, the communication compliance administrator doesn't have permission to create alert policies.

upvoted 1 times

✉️ **Clinson** 6 months ago

Yep, but per your same link communication compliance administrator can create policies, and has less privileges than Org Management  
upvoted 2 times

✉️ **Alecks** 6 months, 1 week ago

- Alert
- Communication Compliance Administrators

Because "Communication Compliance Administrators" is the principle of least privilege

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide#:~:text=Administrators%20of%20communication%20compliance%20that%20can%20create/edit%20policies%20and%20define%20global%20settings>

upvoted 1 times

✉️ **sergioandreslq** 6 months, 3 weeks 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** 7 months ago

CORRECT!!!

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

upvoted 1 times

✉️ **MarkusSan** 6 months, 4 weeks ago

not correct, by link provided ;)

upvoted 2 times

✉️ **Nilz76** 7 months 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 3 times

✉️ **MondherBB** 7 months, 2 weeks 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** 7 months, 3 weeks ago

Alert and Security Admin

Organisation Management is not a Purview role indeed.

upvoted 2 times

✉️ **Blixa** 5 months ago

But it is:

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

Still think Security Administrator (the purview role - not Entra Id role) is the right answer

upvoted 1 times

✉️ **Casticod** 8 months, 1 week 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** 8 months, 2 weeks ago

Correct, Alert and Organization Management.

upvoted 2 times

✉️ **Greatone1** 8 months, 2 weeks ago

Should be Alert and Security Administrator

upvoted 5 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

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 8 months, 3 weeks 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 18 times

Tomtom11 Most Recent 1 month, 2 weeks ago

**Selected Answer: D**

Configuration analyzer in the Microsoft Defender portal provides a central location to find and fix security policies where the settings are less secure than the Standard protection and Strict protection profile settings in preset security policies.

<https://learn.microsoft.com/en-ie/microsoft-365/security/office-365-security/configuration-analyzer-for-security-policies?view=o365-worldwide>

upvoted 1 times

Amir1909 3 months ago

D is correct

upvoted 1 times

TonyManero 5 months, 4 weeks ago

**Selected Answer: D**

agree with D. Please update the solution.

upvoted 3 times

Nilz76 7 months 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 3 times

ae88d96 8 months, 1 week 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 3 times

曰 **gomezmax** 8 months, 1 week ago

It should be D  
upvoted 1 times

曰 **Greatone1** 8 months, 2 weeks ago

**Selected Answer: D**  
Correct answer is D  
upvoted 1 times

曰 **Takanami** 8 months, 2 weeks ago

Configuration Analyzer is correct, direct link:  
<https://security.microsoft.com/configurationAnalyzer>  
upvoted 1 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

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%)

✉️ **Dtriminio** Highly Voted 8 months, 4 weeks 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 10 times

✉️ **RAG** Highly Voted 8 months, 4 weeks 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 6 times

✉️ **letters1234** Most Recent 8 months, 1 week 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 4 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:

店铺: 学习小店66

- Credential harvest
- Link to malware
- Malware attachment

店铺: 学习小店66

Training experience:

- Identity Theft
- Mass Market Phishing
- Web Phishing

Correct Answer:

**Answer Area**

Social engineering technique:

- Credential harvest
- Link to malware
- Malware attachment

Training experience:

- Identity Theft
- Mass Market Phishing
- Web Phishing

✉  **imlearningstuffagain** Highly Voted 6 months, 3 weeks 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 12 times

✉  **Amir1909** Most Recent 3 months ago

Answer is correct  
upvoted 2 times

✉  **krzysztofbr** 5 months ago

answers are correct  
Credential Harvest  
Mass Market Phishing  
upvoted 1 times

✉  **Nilz76** 7 months 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

□ **imlearningstuffagain** 6 months, 2 weeks ago

this is the announcement for the public preview and almost 3 years old.

upvoted 1 times

□ **faeem** 7 months, 1 week 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 4 times

□ **letters1234** 8 months, 1 week 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** 9 months 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** 8 months, 4 weeks 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 7 times

店铺：学习小店66

店铺：学习小店66

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 (91%)	9%
---------	----

✉ **Nilz76** Highly Voted 7 months 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 8 times

✉ **andrewtb** Most Recent 8 months 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 3 times

✉ **mhmyz** 8 months 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 2 times

✉ **Greatone1** 8 months, 2 weeks ago

**Selected Answer: D**

D is the correct answer

upvoted 2 times

✉ **moshkoshbgosh** 8 months, 3 weeks 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... "店铺: 学习小店66"

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** 8 months, 4 weeks 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

👤 NrdAlert 6 months ago

That's malicious web traffic focused. These are malicious files.

upvoted 2 times

👤 alecrobertburns 8 months, 4 weeks 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 8 months, 4 weeks 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

👤 osxzvkwpfcfxobqjby 9 months ago

Selected Answer: B

Safe attachments is only for mail so the answer is B

店铺：学习小店66

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

upvoted 1 times

👤 cgmaxmax 6 months, 1 week ago

Safe Attachments - Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.

upvoted 4 times

店铺：学习小店66

店铺：学习小店66

## 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)	Not applicable

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

店铺: 学习小店66  
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].

**Correct Answer:**

✉ **Nalle** 8 months, 4 weeks 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 59 times

✉ **Sesbri** 3 months, 2 weeks ago

I agree, it is group 3 and group 1 only. For reference see: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide>  
upvoted 2 times

✉ **RVerzijl** 7 months, 2 weeks ago

Group 3 only  
Group 1 only  
upvoted 10 times

✉ **RVerzijl** 7 months, 2 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 2 times

✉ **Wojer** 2 weeks, 4 days ago

test it on my env. and it was group 3 and after adding tag group 1 only  
upvoted 1 times

✉ **cpaljchc4** 3 months, 4 weeks ago

Can anyone explain what is the point of group 4 as all computers Win 10 will be in group 3 due to rank priority?  
upvoted 1 times

✉ **darcone23** 4 months, 2 weeks ago

You can promote or demote the rank of a device group so that it's given higher or lower priority during matching. 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. You can also edit and delete groups.  
upvoted 1 times

✉ **MayTheForceBeWithYou** 5 months, 1 week ago

Can anyone explain why its not group 4 for the first answer since it has the domain and OS?  
upvoted 1 times

✉ **sh123df** 4 months, 2 weeks ago

Because it is due to Rank. Upper rank in list have priority. If that matches so that will be set.  
upvoted 1 times

✉ **cpaljchc4** 3 months, 4 weeks ago

Can you explain what is the point of group 4 if all computers Win 10 will be in group 3 due to rank priority?  
upvoted 1 times

✉ **Festus365** 5 months, 3 weeks ago

Group 3 and Group 4 only  
Group 1 and Group 2 only for Tag Demo  
upvoted 1 times

✉ **NrdAlert** 6 months ago

Indeed the provided answer is quite wrong. As everyone else stated: Group 3, Group 1  
Why else have a ranked order if there's no single matching with precedence?  
upvoted 1 times

✉ **jt2214** 8 months ago

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

upvoted 1 times

曰  **Greatone1** 8 months, 2 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

曰  **Casticod** 8 months, 3 weeks ago

Group 3 only

Group 1 Only

<https://www.examtopics.com/discussions/microsoft/view/48754-exam-ms-101-topic-2-question-15-discussion/>

upvoted 4 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

**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

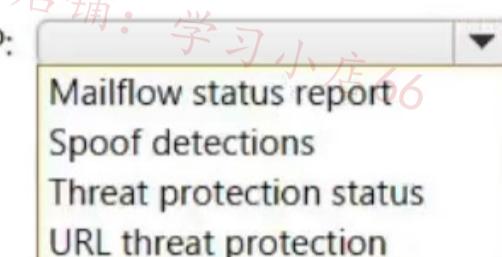
Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

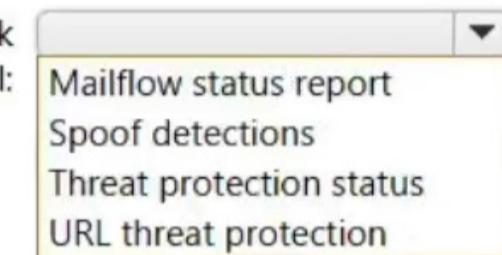
**Answer Area**

店铺：学习小店66

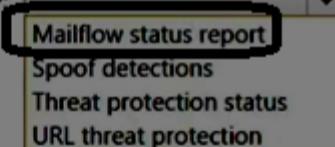
To identify the number of emails quarantined by ZAP:



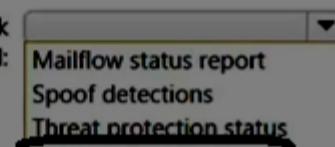
To identify the number of times users clicked a malicious link in an email:

**Answer Area**

To identify the number of emails quarantined by ZAP:

**Correct Answer:**

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



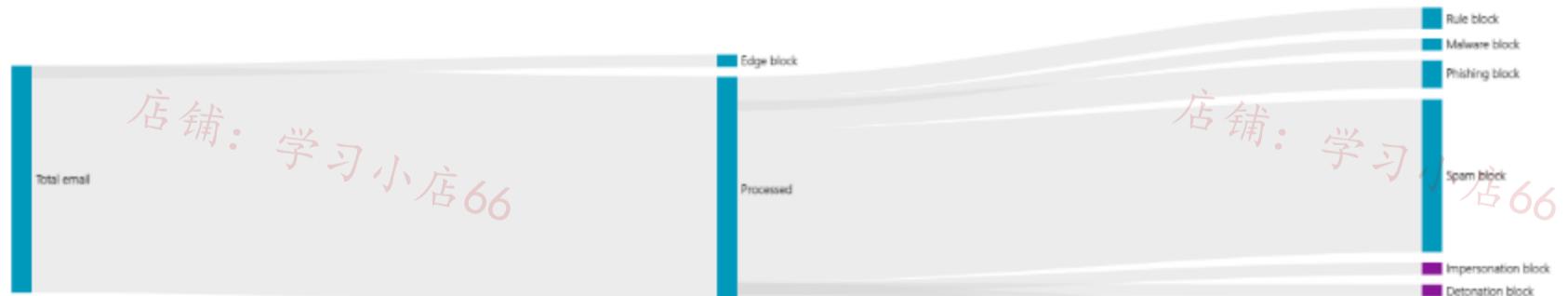
Reports > Mailflow status report

**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.



EOP Defender for Office 365

Show trends Export Refresh

30 items Filter

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	263,604	0	22,755	4,338	26,877	12	157,458	5	22,159
9/20/2021	1,007,087	0	69,528	20,599	117,619	60	733,155	41	66,085

Greatone1 Highly Voted 8 months, 2 weeks ago

Mailflow Status Report

2) URL Protection

upvoted 10 times

✉ **osxvkwpfcfxobjby** Highly Voted 9 months 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 5 times

✉ **Motanel** Most Recent 3 weeks, 5 days ago

Here it says that Threat Protection status should be first.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-defender-for-office-365?view=o365-worldwide&source=docs>

upvoted 1 times

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%)

✉ **Shloeb** Highly Voted 7 months, 2 weeks ago

What kind of questions are these? How does this help in getting certified? Microsoft has lost their mind  
upvoted 16 times

✉ **NrdAlert** 6 months ago

I keep thinking this. Such obscure specific trivia for such a massive platform. Guess that prevents too many people from passing anyway.  
upvoted 3 times

✉ **GenPatton** Highly Voted 7 months, 2 weeks 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 12 times

✉ **Blixa** Most Recent 5 months ago

It also seems to depend on what you have licensed.. looking in my trial tenant I only see "Defender for Cloud Apps" but looking in my production tenant I can filter it on "Defender for Cloud"

upvoted 2 times

✉ **GLLimaBR** 2 weeks, 6 days ago

I see it that way too. The term "Defender for Cloud" leads people to make a mistake in understanding.  
upvoted 1 times

✉ **gomezmax** 7 months, 2 weeks ago

C. Azure Arc  
Right Answer  
upvoted 1 times

✉ **Casticod** 7 months, 3 weeks ago

Real Question in exam  
upvoted 4 times

✉ **cb0900** 8 months, 2 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 3 times

✉ **Greatone1** 8 months, 2 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 3 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 (92%)

5%

✉ certma2023 Highly Voted 8 months, 3 weeks 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 25 times

✉ GLLimaBR 2 weeks, 6 days ago

I agree. I just disagree with this option:

"Modify the User logon name for each user account".

In fact, we change the "User logon name" domain. From my point of view, this option implies that the login name will be changed, but in reality, it is the domain.

upvoted 1 times

✉ WORKTRAIN 6 months, 1 week ago

I agree. The question should be changed to "Which three actions you should do first?".

upvoted 4 times

✉ Casticod Highly Voted 7 months, 3 weeks ago

Real Question in exam

upvoted 5 times

✉ Cryptosuri 1 week, 5 days ago

Then in the real exam are you supposed to put exam topics's answer or the "real" answer ? (real question too ^^)

upvoted 1 times

✉ Scotte2023 Most Recent 6 days, 23 hours ago

**Selected Answer:** ABE

I'm going to say A.B, E as the question mentions preparation for PTA, this article helped me decide on this outcome.

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta-quick-start>

upvoted 1 times

✉ GLLimaBR 2 weeks, 4 days ago

I am under the impression that this question should refer to Microsoft Entra Cloud Sync and not Microsoft Entra Connect (previously called "Azure AD Connect").

I also noticed that the "Modify user logon name for each user account" option is incorrect.

In fact, we changed the "User Login Name". However, this option tricks us into thinking that the login name needs to be changed, but in reality it is the domain that needs to be changed.

upvoted 1 times

✉ **Motanel** 3 weeks, 5 days ago

**Selected Answer: ACE**

A and E is definitely correct at least.

B is not correct because you configure this in Entra ID

Prior to enabling Pass-through Authentication through Microsoft Entra Connect with Step 2, download the latest release of the PTA agent from the Microsoft Entra admin center. You need to ensure that your agent is versions 1.5.1742.0. or later. To verify your agent see Upgrade authentication agents

After downloading the latest release of the agent, proceed with the below instructions to configure Pass-Through Authentication through Microsoft Entra Connect.

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta-quick-start>

upvoted 1 times

✉ **Motanel** 3 weeks, 5 days ago

Prior to enabling Pass-through Authentication through Microsoft Entra Connect with Step 2, download the latest release of the PTA agent from the Microsoft Entra admin center. You need to ensure that your agent is versions 1.5.1742.0. or later. To verify your agent see Upgrade authentication agents

A and E is definitely correct at least.

B is not correct because you configure this in Entra ID

After downloading the latest release of the agent, proceed with the below instructions to configure Pass-Through Authentication through Microsoft Entra Connect.

upvoted 1 times

✉ **Sesbri** 3 months, 2 weeks ago

I think the shown answers are correct as in MS exam language I think they will focus on what is to do to be ready for PTA:

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta-quick-start>

upvoted 1 times

✉ **Sesbri** 3 months, 2 weeks ago

For me the answer shown is correct. We're not talking about user preparation we're talking about infrastructural requirements. For reference see here: <https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta-quick-start>

upvoted 1 times

✉ **cpaljchc4** 3 months, 4 weeks ago

**Selected Answer: CEF**

<https://www.examtopics.com/discussions/microsoft/view/52600-exam-ms-100-topic-4-question-9-discussion/>

upvoted 2 times

✉ **Xbmc66** 4 months, 1 week ago

**Selected Answer: CEF**

it is absolutely not B

BECAUSE:

configuring authentication is something what you should do in Entra ID Connect

upvoted 2 times

✉ **TonyManero** 4 months, 2 weeks ago

**Selected Answer: ABE**

Here the prerequisite for PTA:

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta-quick-start>

upvoted 1 times

you're wrong : the question is : "You need to PREPARE your environment..." so CEF are correct.

upvoted 1 times

✉ **Perycles** 3 months, 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 3 times

✉ **ggdevices** 7 months, 2 weeks 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

✉ **mccheesey** 8 months, 2 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 course, real world application vs. test questions are always different I suppose. :)

upvoted 2 times

✉ **amurp35** 7 months, 3 weeks ago

You enable PTA when configuring AD Connect. In order to configure ADConnect, you must have the UPNs matching the domain in AzureAD.  
upvoted 2 times

✉️  **NrdAlert** 6 months ago

Going to say, PTA means you need a routable domain for the UPN in AD on-prem. It wouldn't pass through with a tenant domain.  
upvoted 1 times

✉️  **Casticod** 8 months, 3 weeks ago

**Selected Answer: CEF**

CDF I don't Dude  
upvoted 2 times

✉️  **Casticod** 8 months, 3 weeks ago

CEF, sorry  
upvoted 1 times

✉️  **osxzvkwpfcfxobjby** 9 months 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 3 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**

店铺: 学习小店66

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

**Correct Answer:**

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

✉  **osxvkwpfcfxobqjby** Highly Voted 9 months ago

- Notification to Microsoft Authenticator app
- 14 days

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/security-defaults#authentication-methods>  
upvoted 13 times

✉  **sherifhamed** Highly Voted 7 months, 1 week 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 6 times

✉  **northgaterebel** 6 months, 2 weeks ago

Hold on now. All 3 of these methods are listed in the answer area. We can only pick one? The best one? Smh  
upvoted 1 times

✉  **nils241** 4 months ago

This is the standard behavior when security defaults are activated.

<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#require-all-users-to-register-for-microsoft-entra-multifactor-authentication>  
upvoted 1 times

曰  **benpatto** Most Recent 5 months, 1 week ago

MS auth app is the DEFAULT Microsoft want us to use. You have the ability to setup SMS, email, voice call etc but the AUTHENTICATOR APP is MS' recommendation and automatically defaulted in every tenant unless specified otherwise.

upvoted 1 times

曰  **Alecks** 6 months, 1 week ago

- MS Auth App  
- 14 Days  
is the default  
upvoted 3 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 (81%) Other

✉️ **Haso** Highly Voted 8 months, 3 weeks 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 19 times

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

**Selected Answer: D**

The correct answer is D. Group1, User1 and User2.

Azure AD Connect synchronizes all Active Directory objects that meet the following criteria:

Object type: Azure AD Connect synchronizes user and group objects only.

\*\*Sync scope:\*\* Azure AD Connect only syncs objects that are in the configured sync scope.

Sync filter: Azure AD Connect only syncs objects that meet the configured sync filters.

In the scenario described, there are no sync filters or sync scope configured. Therefore, Azure AD Connect will synchronize all user and group objects in the contoso.com domain.

Details:

Group1: It is a global security group, which is a type of object synchronized by Azure AD Connect.

User1: It is an enabled user account, which is an object type synchronized by Azure AD Connect.

User2: It is a disabled user account. Azure AD Connect syncs disabled user accounts by default.

Therefore, all three objects will be synchronized with Azure AD.

upvoted 2 times

✉️ **benpatto** 5 months ago

All will sync, the question has NO context whatsoever. If it mentioned filtering at all, this question would change. In my tenant, we have 2x OUs, one for shared mailbox retaining and one for fully disabled users. Remove one and keep the other to prevent sync errors

upvoted 1 times

✉️ **benpatto** 5 months, 1 week ago

**Selected Answer: D**

All will sync, you can specify in AD Connect what you don't want to sync. In this case, nothing was mentioned so all will automatically sync  
upvoted 2 times

✉️ **Festus365** 5 months, 3 weeks ago

Only Group1 and User1 will sync to Azure AD in this scenario.

upvoted 1 times

✉️ **Ruhansen** 7 months, 2 weeks 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** 7 months, 3 weeks ago

Real Question in exam

upvoted 2 times

□ **Tisi** 8 months 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** 8 months, 2 weeks ago

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

upvoted 2 times

□ **Mr4D97** 8 months, 3 weeks ago

**Selected Answer: D**  
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 3 times

□ **Casticod** 8 months, 3 weeks 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** 8 months, 3 weeks 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** 8 months, 3 weeks 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 4 times

□ **certma2023** 8 months, 3 weeks ago

You're right. Group1 is definitely 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** 8 months, 3 weeks 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** 8 months, 3 weeks 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** 8 months, 3 weeks 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

✉️  **NrdAlert** 6 months ago

Resource and shared mailboxes are attached to disabled user accounts, so that makes sense.

upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

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 (87%)	13%
---------	-----

✉️  certma2023 Highly Voted 8 months, 3 weeks 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 20 times

✉️  golijat 5 months, 3 weeks ago

Your approach is indeed a clever one and it seems like it could work. However, there might be a potential issue with the first rule.

In your first rule, you're targeting all users and all locations except a custom trusted location (Public IP Ranges of the company), and you're granting access with MFA + Compliant device. This rule might conflict with the third rule where you're blocking all users from signing in from outside the United States and Canada.

The issue arises because the first rule could potentially allow users to sign in from outside the United States and Canada if they're using a compliant device and MFA, which contradicts the third rule that aims to block all sign-ins from outside these two countries.

Therefore, it's safer to separate these into two different rules to avoid any potential conflicts or overlaps. This way, you can ensure that each rule is enforced correctly without any unintended consequences. Hence, a total of 5 rules would be needed to meet all the requirements.

Please note that the actual configuration might vary based on the specific settings and conditions in your environment. It's always a good idea to test the policies in a controlled environment before deploying them in a production environment.

upvoted 1 times

✉️  newark123 4 months, 2 weeks ago

It wont work like that . You could create a 100 policies that allow access and 1 rule that blocks access and if the one rule that blocks trigger access will be blocked . Having a rule that lets you in will not allow you to log in from a blocked rule .

upvoted 2 times

✉️  Moazzamfarooqiiii Most Recent 2 months, 2 weeks ago

Chat GPT is saying C = 5

upvoted 4 times

✉️  Amir1909 3 months ago

B is correct

upvoted 1 times

✉️ 🚩 **Xbmc66** 4 months, 1 week ago

Selected Answer: A

3.....

1 CA with: MFA and compliant device sign-in and block US and Canada

2 CA with blocking Android and IOS for only R&D

3 App1 access for finance department

upvoted 3 times

✉️ 🚩 **Master\_Tx** 8 months 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 2 times

✉️ 🚩 **nsotis28** 8 months, 1 week ago

answer is correct:

B

upvoted 2 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

**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**

店铺: 学习小店66

Tool:

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

店铺: 学习小店66

Required group membership:

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

**Answer Area**

Tool:

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

Correct Answer:

Required group membership:

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

osxvkwpcfxobqjby Highly Voted 9 months 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 28 times

Casticod Highly Voted 8 months, 3 weeks 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 6 times

Tomtom11 Most Recent 2 months, 4 weeks ago

Regular" users who have accounts in an Active Directory domain are, by default, able to read much of what is stored in the directory, but are able to change only a very limited set of data in the directory.

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory>

upvoted 1 times

✉ **Amir1909** 3 months ago

- IdFix
- Domain Users

upvoted 1 times

✉ **azagroth** 4 months, 2 weeks ago

IdFix & Domain Users - any authenticated user can use the tool to view but not to edit

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. If you want to apply changes to the directory, the authenticated user needs read/write permission to the desired objects.

upvoted 1 times

✉ **Tidi** 4 months, 3 weeks ago

Iare confuser  
upvoted 2 times

✉ **benpattro** 5 months, 1 week ago

It can be domain users as they're considered authenticated users, which is the MINIMUM requirement to run the tool

upvoted 1 times

✉ **Tibo49100** 5 months, 3 weeks ago

It says "identify" not "fix" the potentials issues so i'll go with "IdFix & Domain Users"

upvoted 1 times

✉ **vercracked\_007** 7 months, 3 weeks ago

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

upvoted 3 times

✉ **rfree** 8 months 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

## 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 type="radio"/>

**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 checked="" 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 checked="" 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"/>

**Correct Answer:**

When User1 connects to App1 from a device that has an IP address of 131.107.50.10, User1 must use MFA.  
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.  
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.

Haso Highly Voted 8 months, 3 weeks 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 19 times

365cm 5 months ago

I don't think its marked as a trusted location, as its in a different subnet than the subnets listed as trusted.

upvoted 1 times

lali11 4 months ago

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-mfasettings>

upvoted 1 times

osxvkwpcfxobqjby Highly Voted 9 months 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 7 times

sergioandresiq 6 months, 3 weeks 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 6 times

certma2023 8 months, 3 weeks 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 12 times

lali11 4 months ago

Believe the given answer is correct, first you need to remove IP from trusted IP and add to trusted location otherwise it will bypass mfa prompt:

<https://dirteam.com/sander/2020/07/07/todo-move-from-mfa-trusted-ips-to-conditional-access-named-locations/>

upvoted 2 times

Scotte2023 Most Recent 4 days, 19 hours ago

Trusted locations

Locations such as your organization's public network ranges can be marked as trusted. This marking is used by features in several ways.

Conditional Access policies can include or exclude these locations.

Sign-ins from trusted named locations improve the accuracy of Microsoft Entra ID Protection's risk calculation, lowering a user's sign-in risk when they authenticate from a location marked as trusted.

Locations marked as trusted can't be deleted. Remove the trusted designation before attempting to delete.

Trusted IPs

The trusted IPs feature of Microsoft Entra multifactor authentication also bypasses MFA prompts for users who sign in from a defined IP address range. You can set trusted IP ranges for your on-premises environments. When users are in one of these locations, there's no Microsoft Entra multifactor authentication prompt. The trusted IPs feature requires Microsoft Entra ID P1 edition.

upvoted 1 times

Wuhao 1 week, 5 days ago

The trusted IPs feature of Microsoft Entra multifactor authentication bypasses multifactor authentication prompts for users who sign in from a defined IP address range. You can set trusted IP ranges for your on-premises environments. When users are in one of these locations, there's no Microsoft Entra multifactor authentication prompt. The trusted IPs feature requires Microsoft Entra ID P1 edition.

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-mfasettings#trusted-ips>

upvoted 1 times

Tomtom11 1 month, 2 weeks ago

MFA Enabled vs Enforced

Microsoft Azure Active Directory uses various terms to show the status of multi-factor authentication (MFA) for each user. These user states are shown in the Azure portal and all start out as disabled.

MFA Enabled: The user has been enrolled in MFA but has not completed the registration process. They will be prompted to complete the registration process the next time they sign in.

MFA Enforced: The user has been enrolled and has completed the MFA registration process. Users are automatically switched from enabled to enforced when they register for Azure AD MFA.

MFA Disabled: This is the default state for a new user that has not been enrolled in MFA.

upvoted 2 times

Vaerox 3 months, 1 week ago

I also believe it's YY:

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/location-condition#configure-mfa-trusted-ips>

I believe it only skips MFA if you configure "Skip multifactor authentication for requests from federated users on my intranet" as an option for a Conditional Access policy.

upvoted 1 times

mabew316 4 months, 2 weeks ago

itexamslab.com

Given answer is correct  
upvoted 1 times

- **Navin\_83** 4 months, 2 weeks ago  
It should be YYY because the policy is set Include All trusted location, not exclude any trusted location. Which means its YYY.  
upvoted 1 times
- **benpatto** 5 months, 1 week ago  
Agree with Y Y N (This is marked as a trusted location so MFA can be skipped)  
upvoted 2 times
- **365cm** 5 months, 1 week ago  
Y  
Y  
N  
Trusted IPs you can set it to where it bypasses MFA.  
upvoted 2 times
- **TP447** 5 months, 3 weeks ago  
If the CA policy is scoped to Trusted Locations then by definition, an Untrusted location would get access to APP1 fine where as ALL trusted locations would be challenged for MFA.  
CA would still prompt for MFA to grant access even if the legacy MFA settings have trusted IPs (unless the Trusted IPs were EXCLUDED from the policy which they are not).  
I think this should be Y/Y/Y here on this basis personally.  
upvoted 2 times
- **northgaterebel** 6 months, 2 weeks ago  
NYN? User1 MFA is disabled. I have seen questions like this on SC-300 and the consensus was that since the user can't use MFA they will be denied and that's different from using MFA to grant access. Roll the dice.  
upvoted 4 times
- **Iccen** 3 months, 2 weeks ago  
Correct me if I'm wrong please! But question is he must used? Not Can he use it?  
upvoted 1 times
- **NrdAlert** 5 months, 4 weeks ago  
But the question is whether the statement is true. Down to the last point of the first statement... MFA is required. I think answer is still technically yes this is a true statement as policies don't make exceptions for people that are not enrolled in MFA.  
upvoted 1 times
- **daye** 5 months, 2 weeks ago  
The Q is about if the user 1 MUST use MFA. And the answer is Yes because it's forced by the Conditional Access and he / she have to use it. Next topic is about the current MFA user status, that user will be asked to register / active it since the MFA is a requirement. This is the difference.  
upvoted 1 times

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** Highly Voted 7 months, 1 week 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 6 times

✉ **Amir1909** Most Recent 3 months ago

Correct

upvoted 1 times

✉ **SBGM** 3 months ago

**Selected Answer: A**

Given answer is correct

upvoted 1 times

✉ **GLL** 8 months, 1 week ago

**Selected Answer: A**

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

upvoted 3 times

✉ **TheMCT** 3 months, 2 weeks ago

Conditional Access is found in the Microsoft Entra admin center under Properties > Conditional Access. (Not protection)

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:

店铺：学习小店66

- 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

To enable self-remediation, select:

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

**Correct Answer:**

✉️  **RAG**  8 months, 4 weeks ago

Looks correct - <https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa>  
upvoted 10 times

✉️  **certma2023** 8 months, 3 weeks 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 applies an action on an 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 requires an Azure AD P2 license).

Therefore the second one should be correct too, assuming that the question about configuring a rule that applies a specific action to a compromised account (MS also says "leaked credentials" in some documentation).

upvoted 4 times

✉️  **NrdAlert** 5 months, 4 weeks ago

Thanks for sharing new way!

upvoted 1 times

✉️  **amurp35** 7 months, 3 weeks 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** 8 months, 2 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 2 times

□ **Tomtom11** [Most Recent] 1 month, 2 weeks ago

<https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks>

upvoted 1 times

□ **Tomtom11** 1 month, 2 weeks ago

Multifactor authentication registration policy

Makes sure users are registered for Microsoft Entra multifactor authentication. If a sign-in risk policy prompts for MFA, the user must already be registered for Microsoft Entra multifactor authentication.

User risk policy

Identifies and automates response to user accounts that might have compromised credentials. Can prompt the user to create a new password.

upvoted 1 times

□ **benpatto** 5 months, 1 week ago

Surely second means SSPR? As far as I'm aware, you require 2FA for this right? So realistically MFA and Password change are both viable options but I guess pw change is needed 1st<sup>66</sup>

upvoted 1 times

□ **365cm** 5 months, 1 week ago

Yes, answer is correct. "user-risk policy" User risk is related to the probability that a given identity or account is compromised. It can be triggered by various factors such as leaked credentials

upvoted 1 times

□ **daye** 5 months, 2 weeks ago

Correct

<https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-policies#user-risk-based-conditional-access-policy>

upvoted 2 times

□ **Tatinho** 6 months ago

@60ed5c2 - Totally agree with you. Have you already taken the exam? If you have, do you think the questions from here are in fact useful on the real exam?

upvoted 1 times

□ **60ed5c2** 6 months, 1 week ago

I know the answer is correct. I am looking at the user risk policy setting that says "allow access" with a check box for require password change. And my vent means nothing - but I have to say it. How stupid is it that if a user's credentials are compromised and shared on the dark web you think requiring a password change is a good idea? Couldn't the person that has the credentials execute the password change and still have access because they know what they changed the password to? Wouldn't it make more sense to require multi factor authentication? More sense in a practical sense - not in a what do I have to answer in order to pass the exam sense. I hate these exams.

upvoted 4 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

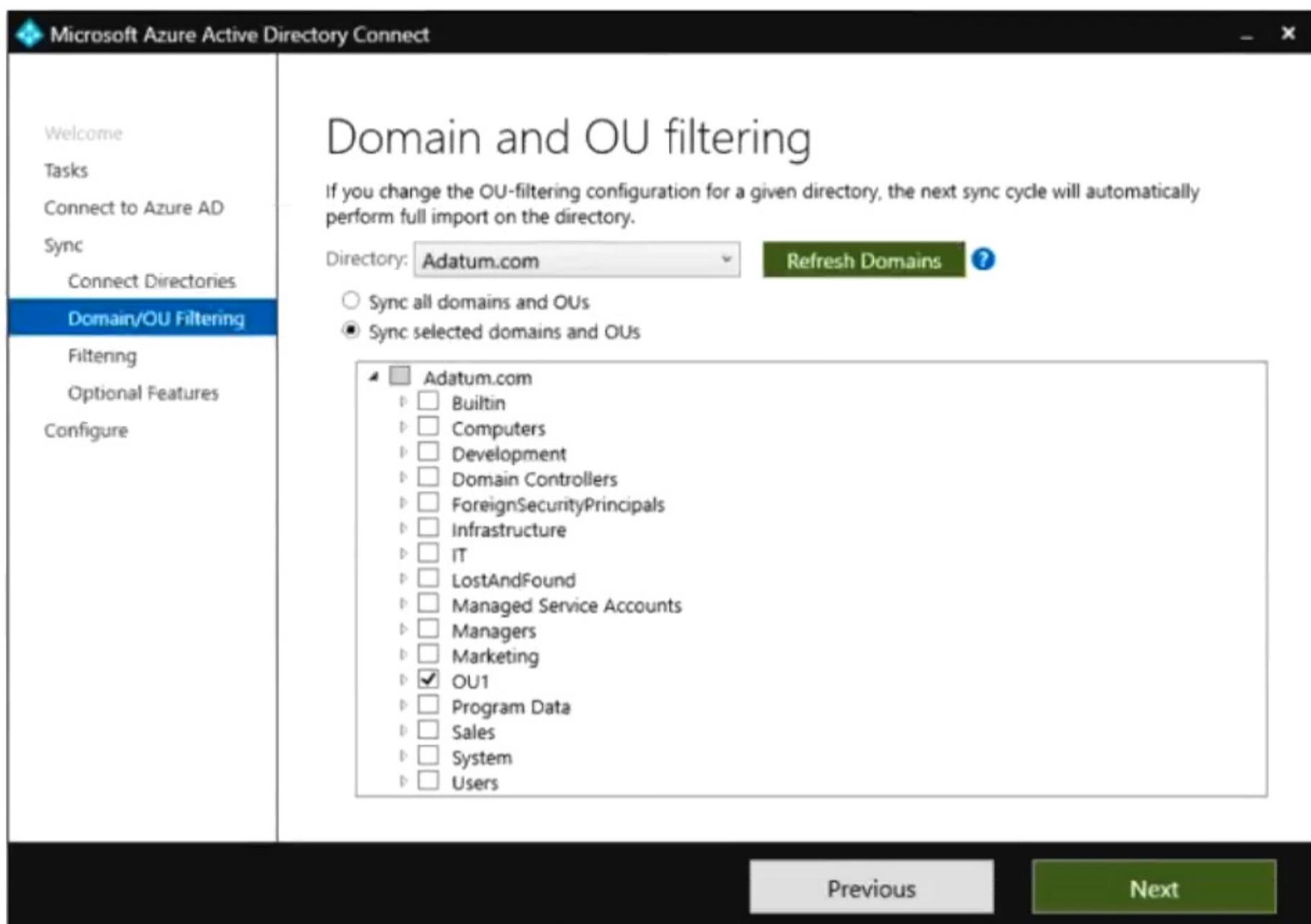
The domain contains the groups shown in the following table.

Name	Member of	In OU
Group1	None	Sales
Group2	Group1	OU1

店铺：学习小店66

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.

店铺：学习小店66

店铺：学习小店66

**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**

店铺：学习小店66

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**

User1 syncs to Azure AD.  
Correct Answer:  
  **User2 syncs to Azure AD.**  
  **Group2 syncs to Azure AD.**

**Yes** **No**

店铺：学习小店66

**Casticod** Highly Voted 8 months, 3 weeks 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 25 times

**WORKTRAIN** 6 months, 1 week ago

You are right.

There is some confusion in the general discussion. Let me explain this a bit different.

OU1 contains user1, user2 and group2: in basic these are 'ready to sync'.

But later in the wizard. Group-based filtering is used. Read it like this: from everything 'ready to sync' only the members of this group-based filter will actually be synced.

The group-based filter contains group1. But group1 is not 'ready to sync'. Zero objects apply on the group-based filter. No objects are synced

upvoted 5 times

✉  **mhmyz**  7 months, 4 weeks 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 7 times

✉  **Tomtom11**  1 month, 2 weeks ago

<https://azurecloudai.blog/2019/10/20/field-notes-azure-active-directory-connect-domain-ou-and-group-filtering/>

upvoted 1 times

店铺：学习小店66

✉  **Tomtom11** 1 month, 2 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-configure-filtering#group-based-filtering>

upvoted 1 times

✉  **Vaerox** 3 months, 1 week ago

It's Y N Y.

View 'Group1' as if it is a Security Group which just happens to be part of the Sales OU. Microsoft is trying to trick you here into believing your devices should be a member of the Sales OU. They are in fact member of OU1, therefore they will sync (except for the second statement).

upvoted 1 times

✉  **TP447** 5 months, 3 weeks ago

This is a botched config. OU1 is in scope but the filter targets Sales OU. Nothing will sync unless it is a member of the Sales OU.

None of User1, User2 or Group2 are in the Sales OU and therefore wont sync. N/N/N is the correct answer here but the configuration is ridiculous

upvoted 1 times

✉  **NrdAlert** 5 months, 4 weeks ago

It is No No No. "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/entra/identity/hybrid/connect/how-to-connect-sync-configure-filtering#group-based-filtering>

upvoted 1 times

✉  **MondherBB** 7 months, 1 week 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 4 times

✉  **vercracked\_007** 7 months, 3 weeks 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

店铺：学习小店66

✉  **EEMS700** 7 months, 2 weeks 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** 8 months, 1 week 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 include 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** 8 months, 2 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** 8 months, 2 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** 8 months, 3 weeks ago

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

so all answers NO

upvoted 4 times

✉  **Mr4D97** 8 months, 3 weeks 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

✉  **osxvkwpfcfxobjby** 9 months 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' switch is turned on. Under 'Target', the 'Select groups' option is selected, and 'Group1' is listed. The 'Authentication mode' dropdown is set to 'Any'.

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 checked="" 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 checked="" type="radio"/> |
| User3 can use passwordless authentication without further action.                                                           | <input type="radio"/>            | <input checked="" type="radio"/> |

The screenshot shows the 'Correct Answer' section with the same three statements and their corresponding 'Yes' and 'No' radio buttons. The 'Yes' radio button is selected for both User1 and User3, while the 'No' radio button is selected for User2.

certma2023 [Highly Voted] 8 months, 3 weeks 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 14 times

GLLimaBR 2 weeks, 4 days ago

And there is one more aggravating factor: The authentication mode selected for group1 is "Any". It's not "passwordless". In other words, as User1 is already configured with MFA in PUSH mode, according to the MFA policy that has the "any" authentication mode, this indicates that nothing will change for User1, that is, it will continue to use password and push.

upvoted 1 times

gomezmax [Highly Voted] 8 months, 1 week ago

Yes Correct YNN

upvoted 5 times

Question #37

Topic 1

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%)

✉️  **Wazery** 2 months ago

**Selected Answer: A**

To meet the requirements, you should choose option A: a data loss prevention (DLP) policy.

The Data Loss Prevention (DLP) policy in Microsoft 365 enables you to identify, monitor, and protect sensitive data. You can configure rules to search for personally identifiable information (PII) in documents stored in Microsoft Teams and SharePoint. You can also generate custom reports to notify about shared documents that contain personal information

upvoted 1 times

✉️  **cb0900** 6 months, 3 weeks 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 4 times

✉️  **KT\_Paradise75** 7 months, 3 weeks ago

The only answer here is A

upvoted 4 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%)

✉ **RAG** Highly Voted 8 months, 4 weeks ago

**Selected Answer: E**

This is the correct see <https://learn.microsoft.com/en-gb/purview/sensitivity-labels>  
upvoted 6 times

✉ **Dtriminio** Highly Voted 8 months, 4 weeks ago

**Selected Answer: E**

<https://learn.microsoft.com/en-us/purview/sensitivity-labels-teams-groups-sites>  
upvoted 6 times

✉ **Amir1909** Most Recent 3 months ago

Correct

upvoted 1 times

✉ **Hasa** 3 months, 2 weeks ago

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 Microsoft Entra ID.  
<https://learn.microsoft.com/en-us/purview/sensitivity-labels>  
upvoted 4 times

✉ **ankitata28** 3 months, 3 weeks ago

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 Microsoft Entra ID.

[https://learn.microsoft.com/en-us/purview/sensitivity-labels#:~:text=Choose%20which%20users%20and%20groups%20see%20the%20labels.%20Labels%20can%20be%20published%20to%20any%20specific%20user%20or%20email%20enabled%20security%20group%2C%20distribution%20group%2C%20or%20Microsoft%20365%20group%20which%20can%20have%20dynamic%20membership\)%20in%20Microsoft%20Entra%20ID.](https://learn.microsoft.com/en-us/purview/sensitivity-labels#:~:text=Choose%20which%20users%20and%20groups%20see%20the%20labels.%20Labels%20can%20be%20published%20to%20any%20specific%20user%20or%20email%20enabled%20security%20group%2C%20distribution%20group%2C%20or%20Microsoft%20365%20group%20which%20can%20have%20dynamic%20membership)%20in%20Microsoft%20Entra%20ID.)  
upvoted 1 times

✉ **omnomsnom** 4 months, 1 week ago

Sensitivity labels cannot be assigned to distribution groups, tho?

upvoted 5 times

✉ **ankitata28** 3 months, 3 weeks ago

It can be,

[https://learn.microsoft.com/en-us/purview/sensitivity-labels#:~:text=Choose%20which%20users%20and%20groups%20see%20the%20labels.%20Labels%20can%20be%20published%20to%20any%20specific%20user%20or%20email%20enabled%20security%20group%2C%20distribution%20group%2C%20or%20Microsoft%20365%20group%20\(which%20can%20have%20dynamic%20membership\)%20in%20Microsoft%20Entra%20ID.](https://learn.microsoft.com/en-us/purview/sensitivity-labels#:~:text=Choose%20which%20users%20and%20groups%20see%20the%20labels.%20Labels%20can%20be%20published%20to%20any%20specific%20user%20or%20email%20enabled%20security%20group%2C%20distribution%20group%2C%20or%20Microsoft%20365%20group%20(which%20can%20have%20dynamic%20membership)%20in%20Microsoft%20Entra%20ID.)  
upvoted 1 times

✉ **gomezmax** 6 months, 2 weeks ago

D. Group1 and Group2 only

upvoted 1 times

≡  **Martham** 6 months, 3 weeks ago

Given Answer is correct

upvoted 2 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

**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**

店铺：学习小店66

**Answer Area**

Correct Answer:

店铺：学习小店66

 **AMDF**  8 months ago

Correct:

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

upvoted 9 times

 **Dtriminio**  8 months, 4 weeks 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 5 times

 **Shloeb**  4 months ago

Incorrect.

First option is Data Loss Prevention and the second option is correct. It should be Settings as mentioned below.  
<https://learn.microsoft.com/en-us/purview/dlp-create-deploy-policy?view=o365-worldwide>

Information Protection mainly deals with the Sensitivity labels and Publishing, but while creating DLP policies you can choose the encrypt content.

upvoted 2 times

 **JazzyStahh** 3 weeks, 3 days ago

Incorrect. DLP is when you know what data you're looking for. Auto labelling is done from Information protection, you can specify the sites and OneDrive locations to apply a specific label that'll encrypt the documents.

upvoted 1 times

店铺：学习小店66

店铺：学习小店66

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**: 学习小店66

Community vote distribution

A (90%)

10%

店铺：学习小店66

✉️ **Alecks** Highly Voted 6 months, 1 week ago

**Selected Answer: A**

In DLP Policy creation is "Sensitive info types" the only available option. So A is correct.

<https://imgur.com/a/zEqXoBA>

upvoted 11 times

✉️ **moshkoshbgosh** Highly Voted 8 months, 3 weeks 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 Message 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 5 times

✉️ **certma2023** 8 months, 3 weeks 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 2 times

✉️ **Sayulis** Most Recent 4 months, 2 weeks ago

You can add Sensitive info types or Trainable classifiers

upvoted 2 times

✉️ **Armins** 6 months ago

A 100% confirmed with my honor.

upvoted 3 times

✉️ **sherifhamed** 7 months, 1 week 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. 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.

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

upvoted 4 times

✉️ **sergioandresiq** 6 months, 3 weeks 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 2 times

✉️ **AMDF** 8 months ago

**Selected Answer: A**

Vote for A

upvoted 1 times

✉️ **SheryID** 8 months, 1 week 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 4 times

✉ **gomezmax** 8 months, 2 weeks ago

Should be A

upvoted 1 times

✉ **Greatone1** 8 months, 2 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** 8 months, 3 weeks 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 Message 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

店铺: 学习小店66

✉ **moshkoshbgosh** 8 months, 3 weeks ago

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

upvoted 1 times

✉ **Dtriminio** 8 months, 4 weeks ago

**Selected Answer: D**

A+D are correct

upvoted 2 times

✉ **osxzvkwpfcfxobqjby** 9 months 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

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

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?

店铺：学习小店66

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

**Correct Answer: C**

*Community vote distribution*

C (84%)      B (16%)

✉️  **moshkoshbgosh** Highly Voted 8 months, 3 weeks 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 33 times

✉️  **ATHOOS** 5 months, 2 weeks ago

Tested and Approved ! well done  
upvoted 2 times

✉️  **Witnz** 3 months, 1 week ago

not specified  
upvoted 1 times

✉️  **NrdAlert** Most Recent 5 months, 4 weeks ago

**Selected Answer: C**

They don't specify to exclude private chats, so you need 3.

upvoted 2 times

✉️  **jay209328032038** 6 months, 3 weeks 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 3 times

✉️  **smiff** 7 months, 2 weeks ago

**Selected Answer: B**

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

upvoted 1 times

✉️  **mhmyz** 7 months, 3 weeks 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 2 times

□ **Nandokun01** 8 months, 2 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** 8 months, 2 weeks ago

**Selected Answer: C**

3 is the correct answer from previous test  
upvoted 1 times

□ **nublit** 8 months, 3 weeks 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** 8 months, 3 weeks 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

□ **osxvkwpcfxobqjby** 9 months 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 8 months, 3 weeks 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 49 times

✉ **cpaljchc4** 4 months, 2 weeks ago

Why is Deleted 7 years after they were created correct?

How about the delete after retention period? If my retention period is 30 days?

It is not going to be deleted after 7 years isn't it?

Sorry, I'm not native English speaker.

But Retained not more than 7 years from they created sounds more logically right, no?

if retention period = 30days, Retained < 7years = files created > 7 years will be deleted and (retention period = 30days) < (retained file < 7 years) also been fulfilled isn't it?

upvoted 2 times

✉  **nordbymikael** 1 month, 1 week ago

There is no retention period specified in the policy. There is a separate setting called "retain for x amount of time and then delete".

upvoted 1 times

✉  **gomezmax**  8 months, 1 week 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 9 times

✉  **hagosc**  2 weeks, 5 days ago

I think the first is correct but the second should be Some data will be deleted immediately

upvoted 1 times

✉  **Armins** 6 months ago

Deleted 7 years after they were created

and

Some data will be deleted immediately

upvoted 7 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

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 (83%)

BE (17%)

✉️  Hard1k Highly Voted 8 months, 1 week 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 16 times

✉️  hagosm Most Recent 2 weeks, 5 days ago

The correct answers are A and E.

upvoted 1 times

✉️  GLLimaBR 2 months, 1 week ago

I understand that it is more of an ambiguous issue, because a document fingerprint is generated based on samples and after creation, it will be made available as "a sensitive info type", and can be used in DLP policies.

upvoted 1 times

✉️  sherifhamed 7 months, 1 week 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 2 times

✉️  Casticod 8 months 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 8 months 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** 8 months, 2 weeks ago

"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 3 times

✉️ 🤙 **gomezmax** 8 months, 2 weeks ago

Agree Should be, BE

upvoted 1 times

✉️ 🤙 **Greatone1** 8 months, 2 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** 8 months, 2 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

店铺：学习小店66

店铺：学习小店66

**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. i

Block only people outside your organization. i

店铺：学习小店66

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:

A dropdown menu labeled "User1:" containing five numbered options: 1, 2, 3, 4, and 5. The menu has a standard Windows-style border and a downward-pointing arrow in the top right corner.

User2:

A dropdown menu labeled "User2:" containing five numbered options: 1, 2, 3, 4, and 5. A red watermark reading "店铺: 学习小店66" is overlaid across the entire menu. The menu has a standard Windows-style border and a downward-pointing arrow in the top right corner.

### Answer Area

User1:

A dropdown menu labeled "User1:" containing five numbered options: 1, 2, 3, 4, and 5. The option "5" is highlighted with a black square selection box.

Correct Answer:

User2:

A dropdown menu labeled "User2:" containing five numbered options: 1, 2, 3, 4, and 5. The option "2" is highlighted with a black square selection box.

✉ **mhmyz** 7 months, 2 weeks 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, PPT, PPS, PPSX, PPT, PPTM, PPTX, XLC, XLS, XLSB, XLSM, XLSX, XLT

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

upvoted 7 times

店铺: 学习小店66

✉ **hogehogehoge** 8 months, 2 weeks ago

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

upvoted 3 times

✉ **osxzvkwpfcfxobqjby** 9 months 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

✉ **Nandokun01** 8 months, 2 weeks ago

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

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.

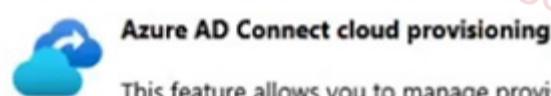
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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



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 Highly Voted 7 months, 2 weeks ago

B.No

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

upvoted 7 times

✉ Greatone1 Highly Voted 8 months, 2 weeks ago

Selected Answer: B

Should be no

upvoted 6 times

✉ NrdAlt Most Recent 5 months, 4 weeks ago

Its funny how when you get an obviously easy question(fabrikam.com upn is not contoso.com), you question what you are missing, what's the gotcha.

upvoted 5 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 (69%)

B (31%)

曰 **Greatone1** 8 months, 2 weeks ago

**Selected Answer: A**

Correct answer is A

upvoted 8 times

曰 **TonyManero** 1 week, 4 days ago

**Selected Answer: A**

The domain fabrikam.com isn't synchronized at all (as I see in the picture..), so the only way to logon is to use contoso.com. It seems clear.  
upvoted 1 times

曰 **Vukosir** 2 months, 1 week ago

Answer is A

The on-premises Active Directory domain is named contoso.com. You can enable users to sign on using a different UPN (different domain), by adding the domain to Microsoft 365 as a custom domain. Alternatively, you can configure the user account to use the existing domain (contoso.com).

upvoted 1 times

曰 **AAlmani** 3 months ago

**Selected Answer: B**

The requirement as follow:

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.

Correct answer is: B. user2 should authenticate as user2@fabrikam.com

upvoted 3 times

✉ **RJTW070** 3 months, 2 weeks ago

**Selected Answer: B**

No, the solution does not meet the goal. The UPN suffix for User2 should be set to @fabrikam.com, not @contoso.com. The UPN suffix is used to authenticate a user in Azure AD, so it must match the domain name of the user's email address. By setting the UPN suffix to @contoso.com, User2 will not be able to authenticate to Azure AD using their email address user2@fabrikam.com. Instead, you should set the UPN suffix for User2 to @fabrikam.com, and then instruct User2 to sign in as user2@fabrikam.com. This will allow User2 to authenticate to Azure AD and access the resources they need.

upvoted 1 times

✉ **bipsta** 3 months ago

The way I am reading it, I don't believe fabrikam.com is being synced at all!

upvoted 4 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

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

A (67%)

B (33%)

Greatone1 Highly Voted 8 months, 2 weeks ago

Selected Answer: A

the answer is A.

upvoted 13 times

sherifhamed Highly Voted 7 months, 1 week 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 6 times

AAlmani Most Recent 3 months ago

Selected Answer: A

Correct answer is A

upvoted 2 times

□  **RJTW070** 3 months, 2 weeks ago

**Selected Answer: A**

Yes, the solution meets the goal. By adding fabrikam.com as a custom domain in the Microsoft Entra admin center, you can ensure that User2 can authenticate to Azure AD using their email address user2@fabrikam.com. This is because the UPN suffix is used to authenticate a user in Azure AD so it must match the domain name of the user's email address. By adding fabrikam.com as a custom domain, you can ensure that User2 can authenticate to Azure AD using their email address user2@fabrikam.com. You can then instruct User2 to sign in as user2@fabrikam.com to access the resources they need

upvoted 3 times

□  **jbuexamtopics** 6 months ago

**Selected Answer: B**

Didnt mentioned that it was verified.

upvoted 2 times

□  **Constyle** 6 months, 2 weeks ago

Answer is A

upvoted 1 times

□  **jbuexamtopics** 6 months, 3 weeks ago

**Selected Answer: B**

Very tricky, I'll go for B because it didnt mentioned that fabrikam.com was verified.

upvoted 4 times

□  **Casticod** 8 months ago

**Selected Answer: B**

From the first reading, I think that the local active directory has the UP 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 4 times

□  **letters1234** 8 months 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

□  **NrdAlert** 5 months, 4 weeks ago

It's stated both users exist in the domain which means frabikam.com is a UPN in the contoso.com domain, not a separate forest. The only gotcha is they don't mention the very critical step of verifying the domain. Adding it won't necessarily enable this person to sign-on unless there's an assumption the domain is verified as part of the process of adding it. I'm leaning towards A on this one as I feel that's a safe assumption at the level of detail this scenario provides.

upvoted 4 times

□  **Greatone1** 8 months, 1 week 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 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: 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**  8 months 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 Directory<sup>1</sup>. 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 365<sup>2</sup>. 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 11 times

✉  **RJTW070**  8 months 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 Directory<sup>1</sup>. You can start by understanding the synchronization process and then follow the troubleshooting steps mentioned in the article

upvoted 2 times

✉  **Takanami** 8 months, 2 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 4 times

✉  **Greatone1** 8 months, 2 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**  8 months 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 6 times

店铺：学习小店66

店铺：学习小店66

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

B (80%)

A (20%)

 **Anonymous121011**  5 months, 3 weeks ago

No, this solution does not meet the goal.

Creating a new outbound synchronization rule in the Synchronization Rules Editor will not solve the issue of the 10 user accounts not being synchronized to Azure AD.

Outbound synchronization rules define what happens after Azure AD Connect has combined the data from all connected directories. They don't control which objects are being synchronized to Azure AD.

The issue seems to be with the scope of the objects that are being synchronized. It's possible that the OU containing these 10 users is not included in the synchronization scope.

To solve this issue, you should check the configuration of Azure AD Connect and ensure that the OU containing these 10 users is included in the synchronization scope.

upvoted 9 times

 **sherifhamed**  7 months, 1 week 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 5 times

 **692a0df**  3 months ago

##### Selected Answer: A

I think its A.

Its not related to OU selection/filtering as AAD Connect health says it has synced ALL user accounts BUT these 10 are not appearing in Azure AD. So the accounts are making the initial sync from the OnPrem AD into the Meta zone (AAD Connect).

Rules then apply and if the rule conditions are met - then the sync from the Meta to Azure AD will complete.

So it's feasible that a rule is causing the problem. Why not impact the other accounts. Maybe these accounts are missing specific attrs from their OnPrem AD that the current rule needs to push the sync.

Saying all that... it could potentially be something else. Maybe stale / relic objects in Azure AD that match attrs from these 10 accounts. So its A for me but only a 70% A.

upvoted 1 times

 **Abhishek1610** 3 months, 2 weeks ago

**Selected Answer: B**

From Azure AD Connect, you modify the filtering settings  
upvoted 4 times

✉ **cpaljchc4** 3 months, 3 weeks ago

**Selected Answer: B**

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

✉ **m2L** 4 months, 2 weeks ago

Hello Guys,  
The Answer is no doubt A because making OU Filtering is a way to use Sync Rule Editor.  
<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-fix-default-rules?source=recommendations>  
upvoted 2 times

✉ **Nyamnyam** 5 months ago

**Selected Answer: B**

This is a clear OU filtering question.  
upvoted 2 times

店铺：学习小店66

✉ **benpatto** 5 months, 1 week ago

No, you require OU filtering. This will then allow the OU that has the 10 users to sync to Azure AD  
upvoted 1 times

✉ **daye** 5 months, 3 weeks ago

**Selected Answer: B**

No, It does not meet the goal since you don't have any evidence.

As other guy said, firstly you should review the OU filtering or do some extra troubleshooting to identify the root cause.  
upvoted 2 times

✉ **NrdAlert** 5 months, 4 weeks ago

**Selected Answer: B**

It states everyone is syncing fine except a single OU. That's selecting the OU as part of setting up AADC's scope which is not the same as changing an outbound synchronization rule. To be more specific using IDM language, that scope effects AADC's ability to import/see those accounts before it exports them to Entra/AAD.  
upvoted 2 times

✉ **AlfaExamPro** 6 months, 1 week ago

**Selected Answer: B**

No.

Does not meet the goal.  
upvoted 2 times

✉ **santi32** 7 months, 2 weeks 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 4 times

店铺：学习小店66

✉ **RJTW070** 8 months ago

**Selected Answer: A**

Yes, creating a new outbound synchronization rule from the Synchronization Rules Editor could potentially solve the issue. 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. 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

✉ **imlearningstuffagain** 6 months, 2 weeks ago

The rules editor is not the same as the AD Connect configuration. If sync is running OK for all others, there can be a filtering issue, but that is not changed in the rules editor. You can compare this to renaming the domain if your AAD domain is not the same, sure it will work. However a suffix will do the trick and is much easier.

upvoted 1 times

✉️ **letters1234** 8 months, 1 week 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

✉️ **imlearningstuffagain** 6 months, 2 weeks ago

The rules editor is not the same as the ad configuration.  
upvoted 1 times

✉️ **Greatone1** 8 months, 2 weeks ago

**Selected Answer: A**

Correct answer should be yes  
upvoted 2 times

✉️ **osxzvkwpfcfxobqjby** 9 months 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**

店铺: 学习小店  
Teams daily active users:

- Microsoft Secure Score
- Adoption Score
- Service health
- Usage reports

店铺: 学习小店66

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

曰  **Casticod** Highly Voted 8 months, 3 weeks 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 7 times

曰  **Amir1909** Most Recent 3 months ago

Correct

upvoted 1 times

曰  **daye** 5 months, 3 weeks ago

It's correct, easy one.

upvoted 1 times

曰  **gomezmax** 8 months, 1 week ago

Correct

upvoted 4 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

## 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****Answer Area**

Billing Administrator

Group1:  Role

Global Administrator

Group2:  Role

Helpdesk Administrator

License Administrator

Service Support Administrator

User Administrator

**Answer Area**

Correct Answer:

Group1: Billing Administrator

Group2: User Administrator

曰  **daye** 5 months, 3 weeks ago

correct

upvoted 2 times

店铺：学习小店66

曰  **amurp35** 7 months, 2 weeks agocorrect <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference?view=o365-worldwide#billing-administrator>  
upvoted 3 times曰  **Casticod** 8 months, 3 weeks agoCorrect: <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 (80%)

A (20%)

✉ **nsotis28** Highly Voted 8 months, 1 week 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 11 times

✉ **TheMCT** 3 months ago

Correct Answer: C

This domain can't be removed after it's added. Make sure the spelling is correct before you add the domain, as you can only have 5 total onmicrosoft.com domains.

upvoted 1 times

✉ **Amir1909** Most Recent 3 months ago

Correct

upvoted 1 times

✉ **TonyManero** 4 months, 2 weeks ago

**Selected Answer: C**

In Microsoft documentation is specified max 5 onmicrosoft.com

upvoted 2 times

✉ **Alecks** 6 months, 1 week ago

**Selected Answer: C**

C is correct: "You are limited a total of five onmicrosoft.com domains in your Microsoft 365 environment. Once they are added, they cannot be removed."

<https://learn.microsoft.com/en-us/microsoft-365/admin/setup/add-or-replace-your-onmicrosoftcom-domain?view=o365-worldwide>  
upvoted 4 times

✉ **sherifhamed** 7 months, 1 week ago

**Selected Answer: C**

The correct answer is C. 5.

According to the first web search result<sup>1</sup>, 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** 7 months, 1 week ago

**Selected Answer: C**

Only 5 onmicrosoft domains are possible

upvoted 2 times

✉ **martin\_salan07** 7 months, 1 week 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** 7 months, 2 weeks 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** 8 months, 2 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** 8 months, 2 weeks 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** 8 months, 3 weeks 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 [Highly Voted] 7 months, 3 weeks 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 11 times

Be41223 7 months, 3 weeks 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 30 times

✉️ **JensV** 7 months, 2 weeks ago

<https://learn.microsoft.com/en-us/azure/active-directory/roles/privileged-roles-permissions?tabs=admin-center#who-can-reset-passwords>  
upvoted 6 times

✉️ **Exam2us** 2 months ago

I think this is not correct. Review this link for more information - <https://learn.microsoft.com/en-us/azure/active-directory/roles/privileged-roles-permissions?tabs=admin-center#who-can-reset-passwords>

upvoted 1 times

✉️ **benpatto** 5 months ago

I'd like to agree but this is why there are global admins. There's always at least one global administrator in a tenant which has the ability to do anything it needs to - no bars held. So I think N, Y, N  
upvoted 1 times

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

Correct answer: Y,Y,Y

If we read this document <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/privileged-roles-permissions?tabs=admin-center#who-can-reset-passwords>, we can see how the password manager can change even that of the global administrator  
upvoted 1 times

✉️ **Amir1909** 3 months ago

Correct

upvoted 1 times

✉️ **SBGM** 3 months ago

Link provided by JensV:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/privileged-roles-permissions?tabs=admin-center#who-can-reset-passwords>

"For example, a Password Administrator can reset the password for Directory Readers, Guest Inviter, Password Administrator, and users with no administrator role. If a user is assigned any other role, the Password Administrator cannot reset their password."

upvoted 1 times

✉️ **m2L** 4 months, 2 weeks ago

Agree with Be41223

upvoted 1 times

✉️ **spg1** 5 months, 2 weeks ago

NO, YES, NO

All explanation is here

"Password admin - Assign the Password admin role to a user who needs to reset passwords for non-administrators and Password Administrators"

<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

✉️ **Festus365** 5 months, 3 weeks ago

I personally chose the answers: YYY!!

upvoted 3 times

✉️ **Rylz** 6 months ago

there is a problem here with user 1

you cant assign role for two AUs - tried it right now and it did not work

upvoted 1 times

✉️ **imlearningstuffagain** 6 months, 2 weeks ago

NYN

User1 can reset password for User3 -> NO, password admin cannot reset passwords for User Admin. Check check <https://learn.microsoft.com/en-us/azure/active-directory/roles/privileged-roles-permissions?tabs=admin-center#who-can-reset-passwords>

User2 can Update display name of User 1 -> YES, he is User Admin on AU1 and User 1 is member of AU1, A useradmin can update Most user properties including admin. <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#user-administrator>

User1 can reset password for User2 -> NO, password admin cannot reset passwords for User Admin. Check check <https://learn.microsoft.com/en-us/azure/active-directory/roles/privileged-roles-permissions?tabs=admin-center#who-can-reset-passwords>

upvoted 2 times

nsotis28 8 months, 1 week ago

provided answer is correct  
upvoted 1 times

Greatone1 8 months, 2 weeks ago

I think this one is correct as an Admin cannot reset another Admins password  
upvoted 4 times

Question #55

Topic 1

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?

店铺：学习小店66

- 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%)

Greatone1 Highly Voted 8 months, 2 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 5 times

Motanel Most Recent 3 weeks, 5 days ago

Azure AD Powershell will be deprecated, so get\_MgUser needs to be used.  
upvoted 1 times

sherifhamed 7 months, 1 week 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 3 times

mhmyz 7 months, 2 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 2 times

店铺：学习小店66

**HOTSPOT -**

Your company has a Microsoft 365 E5 subscription.

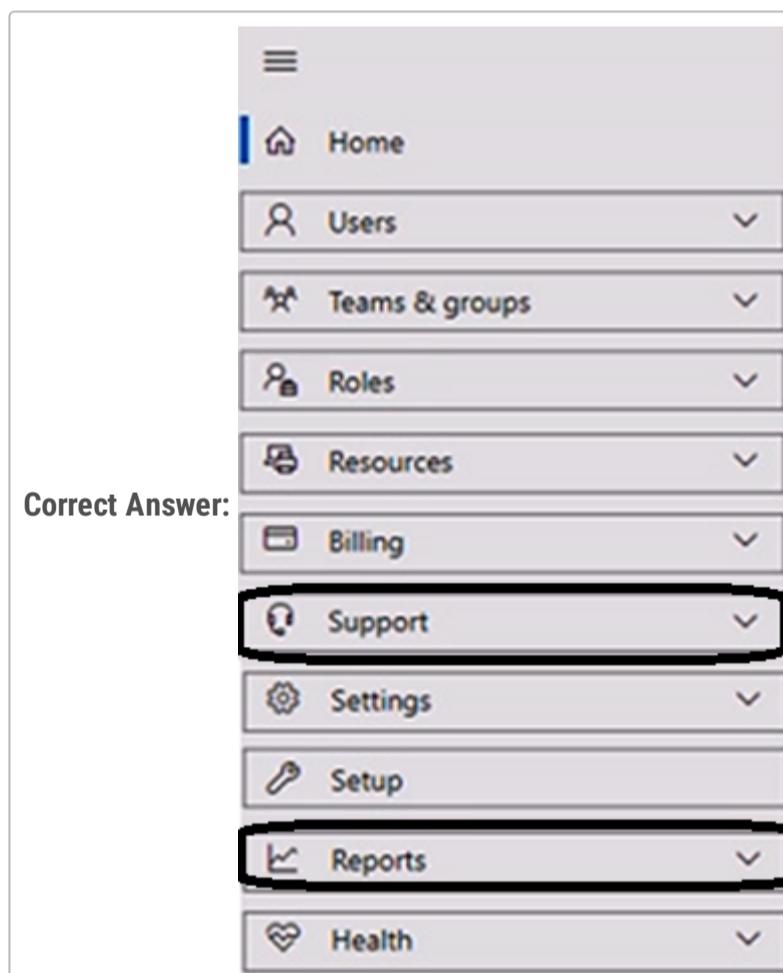
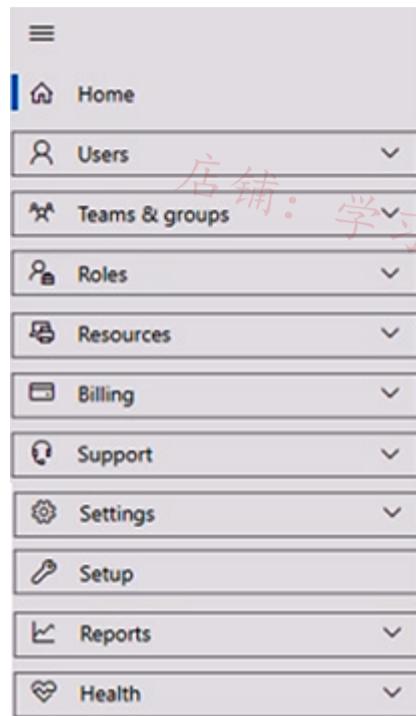
You need to perform the following tasks:

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.



Amir1909 3 months ago

Correct

upvoted 1 times

daye 5 months, 3 weeks ago

correct

upvoted 3 times

gomezmax 8 months, 2 weeks ago

IT is Reports then Adoption Score

upvoted 4 times

Casticod 8 months, 2 weeks ago

Correct.

Support to open case a MS

Report to access to the adoption Score

upvoted 4 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

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%)

✉️  **sherifhamed**  7 months, 1 week 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 22 times

✉️  **shaffer** 2 months, 1 week ago

Thank you, I was so confused  
upvoted 1 times

✉️  **Martham** 6 months, 3 weeks ago

Thanks alot  
upvoted 1 times

✉️  **Mustardonk**  8 months, 3 weeks ago

Wrong picture?  
upvoted 5 times

✉️  **kayci**  3 weeks, 5 days ago

Correct Answer: E

As a user administrator, user5 can manage regular user accounts, which includes resetting passwords and managing user attributes. However, the user administrator role does not grant permissions to delete users. Deleting users typically requires global administrator or equivalent privileges.

Therefore, user5 cannot delete user2 and user4, as they lack the necessary permissions.

upvoted 1 times

✉️  **nordbymikael** 1 month, 1 week ago

**Selected Answer: AE**

Correct

upvoted 3 times

✉️  **TheMCT** 3 months ago

Correct Picture:

User1, Exchange Administrator  
User2, User Administrator  
User3, Global Administrator  
User4, None

You add another user named User5 to the User Administrator role.

You need to identify which two management tasks User5 can perform

Correct Answer: A, E  
upvoted 2 times

✉  **sergioandreslq** 6 months, 2 weeks ago

Tested in Lab, the correct answers are: A-E  
A. Delete User2 and User4 only.  
E. Reset the password of User2 and User4 only.

Wrong: user admin can't:

C. Reset the password of any user in Azure AD. there are some admin users that this role can't reset password  
D. Delete User1, User2, and User4 only. I tried to delete the exchange administrator and I got error  
F.Delete any user in Azure AD. I tried to delete the GA and I got error, this role can only delete non-admin users and other User Admins.  
upvoted 3 times

✉  **sherifhamed** 7 months, 1 week ago

!!!!!! Wrong picture !!!!!!!  
upvoted 1 times

✉  **Tisi** 7 months, 2 weeks ago

Wrong picture  
upvoted 3 times

✉  **Master\_Tx** 7 months, 4 weeks ago

This doesnt match what's on the exam. There is a second image that should go with this.  
upvoted 2 times

✉  **Casticod** 8 months, 2 weeks ago

**Selected Answer: AE**  
A and E are correct.  
upvoted 2 times

✉  **f7d3be6** 8 months, 2 weeks ago

<https://www.examtopics.com/discussions/microsoft/view/98896-exam-ms-100-topic-3-question-21-discussion/>  
upvoted 3 times

✉  **Vaati** 8 months, 3 weeks 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.

**Group1**  
Private group • 1 owner • 1 member

General Members Settings Microsoft Teams

**General settings**

Allow external senders to email this group  Private  Public

Send copies of group conversations and events to group members

Hide from my organization's global address list

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:	<input type="checkbox"/> Add User1 to the subscription as an active user. <input type="checkbox"/> For Group1, change the Privacy setting to Public. <input type="checkbox"/> For Group1, select Allow external senders to email this group. <input type="checkbox"/> Invite User1 to collaborate with your organization as a guest.
Portal:	<input type="checkbox"/> The Microsoft Entra admin center <input type="checkbox"/> The Exchange admin center <input type="checkbox"/> The Microsoft 365 admin center <input type="checkbox"/> The Microsoft Purview compliance portal

**Answer Area**

Action:	<input type="checkbox"/> Add User1 to the subscription as an active user. <input type="checkbox"/> For Group1, change the Privacy setting to Public. <input type="checkbox"/> For Group1, select Allow external senders to email this group. <input checked="" type="checkbox"/> Invite User1 to collaborate with your organization as a guest.
Portal:	<input checked="" type="checkbox"/> The Microsoft Entra admin center <input type="checkbox"/> The Exchange admin center <input type="checkbox"/> The Microsoft 365 admin center <input type="checkbox"/> The Microsoft Purview compliance portal

✉ **GLLimaBR** 2 months, 1 week ago

Both answers are correct.

There is no need to change the group privacy just to include one external user (and probably not even if there were multiple external users).

Be careful with the mental trap that the image can provoke: This is not the portal where we make the group settings, but rather the only portal where we can invite external users. The only portal where we can create guest users is on the Microsoft Entra Portal.

upvoted 3 times

□  **Casticod** 8 months, 1 week 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

□  **Master\_Tx** 7 months, 4 weeks 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

□  **GLL** 7 months, 3 weeks 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 6 times

□  **TonyManero** 5 months, 3 weeks ago

True, you will be redirected to Entra...

upvoted 1 times

□  **hogehogehoge** 8 months, 2 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 2 times

□  **hogehogehoge** 8 months, 1 week ago

Sorry. This answer is correct. Because Group type is not necessary to change.

upvoted 1 times

□  **Greatone1** 8 months, 2 weeks ago

Given answer is correct

<https://www.examtopics.com/discussions/microsoft/view/94423-exam-ms-100-topic-3-question-94-discussion/>

upvoted 3 times

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)

店铺：学习小店66

**Correct Answer: D**

*Community vote distribution*

D (100%)

✉️  **RJTW070** Highly Voted 8 months ago

**Selected Answer: D**

Pim should be right  
upvoted 5 times

✉️  **Amir1909** Most Recent 3 months ago

Correct  
upvoted 1 times

✉️  **daye** 5 months, 3 weeks ago

**Selected Answer: D**

Correct, PIM  
upvoted 3 times

店铺：学习小店66

店铺：学习小店66

**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

Retention period:

24 hours  
 7 days  
 14 days  
30 days  
 90 days

✉  **KerrAvon** 2 months, 1 week ago

Correct since its MS365 only. If it were a hybrid (on-prem AD) you can recover the others from the AD recycle bin.

upvoted 1 times

✉  **imlearningstuffagain** 6 months, 3 weeks 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** 7 months, 1 week 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** 7 months, 2 weeks 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 4 times

□  **Greatone1** 8 months, 1 week ago

Letters already provided the answer only Microsoft 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** 8 months, 1 week 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 3 times

□  **Greatone1** 8 months, 1 week ago

Should be group 3 and 30 days  
店铺: 学习小店66

upvoted 3 times

□  **DiligentSam** 8 months, 2 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** 7 months, 2 weeks ago

ChatGPT and other tools will quite often give you the wrong answers because it "sounds right" to their algorithms.

upvoted 4 times

□  **Greatone1** 8 months, 2 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

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

**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 24 times

□ **omnomsnom** 3 months, 2 weeks ago

Sorry, but you have misinterpreted the documentation. The 'activation maximum duration' setting is how long the role is active for after activation (with or without approval), it has nothing to do with how long an activation request can sit there waiting for approval. Also, note that the user must already have the role assigned as eligible for them to activate the role to start with. Best wishes.  
upvoted 2 times

□ **Shloeb** 7 months, 1 week ago

Correct. Others are misunderstanding this. 8 hours is meant for the activation request not the actual assignment.  
upvoted 5 times

□ **amurp35** 7 months, 2 weeks 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 4 times

□ **santi32** Highly Voted 7 months, 2 weeks 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 9 times

□ **Vaerox** 3 months, 2 weeks ago

Agreed!  
upvoted 1 times

□ **DONPHYLO** Most Recent 4 weeks ago

Ici le point marquant c'est qu'il n'y a pas d'approbation vu qu'il est administrateur global, ainsi lorsque l'utilisateur active la mission il a 15 jours pour travailler avant que son activation ne s'expire après 15 jours pour que le l'utilisateur fasse une nouvelle demande d'activation et il est à note qu'il a 3 mois d'éligibilité c'est à dire 3 mois pour exploiter le rôle d'administrateur global après ceci il perdra ce privilège.

Réponses :

- 1) 15 jours
  - 2) 3 mois
- upvoted 1 times

□ **Amir1909** 3 months ago

Correct  
upvoted 1 times

□ **m2L** 4 months, 2 weeks ago

Hello Guys, according to the link below, 8 hours is just the required time for the admin to activate the role if a user requests it.  
For example: if User1 requests an admin role.  
the PIM admin has 8 hours to activate the role for User1. 8 hours after the requests of User1 if the admin doesn't activate the role for him, the request will expire and User1 has to request again.  
But if the admin activates the role for User1 within 8 hours, User1 will have 15 days to do his job. After 15 days he will lose the role.  
<https://learn.microsoft.com/fr-fr/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings>  
upvoted 3 times

□ **Nyamnyam** 5 months ago

Correct answers are:

A user that is assigned the Global Admin role \*as active\*: will lose the role after 15 days  
You can make a Global Admin role available to \*activation requests\*: for up to eight hours.

People often misunderstand the difference between Activation section and Assignment section.

Keyword—"activation" is always the process of elevation from eligibility to active assignment, and is regulated via "Activation maximum duration"  
Keyword—"active" is always the "permanent active assignment", and is regulated by "Expire active assignment after"

upvoted 3 times

□ **daye** 5 months, 3 weeks ago

TBH, I think the config is wrong, a PIM profile can be eligible or active but not both, so I don't know why we can see both options.

In that case is eligible, so the role, once is active manually, will be active for 8 hours, afterwards, he/she will lose the rol (question A).

This kind of activation will be available for 3 months (question B)

upvoted 1 times

□ **daye** 5 months, 3 weeks ago

Nevermind, I confused user assignment with role settings. It would be A) 15 days and B) 3 months  
upvoted 2 times

□ **northgaterebel** 6 months, 1 week ago

Atrocious wording. Depending on how you interpret "lose" 3 options in 1st answer can be valid:  
will lose the role after 8 hours  
can reactivate the role every 8 hours  
will lose the role after 15 days  
2nd answer is correct: 3 months  
upvoted 1 times

□ **CheMetto** 6 months, 1 week ago

I think this should be the correct lecture:  
You can activate the role or extend it anytime you want, you don't need to wait the 8 hours, so the correct answer for the first one is after 15 days role will disappear.  
upvoted 1 times

□ **spectre786** 8 months, 1 week ago

First one : will lose the role after 8 hours AND can reactivate every 8 hours  
Right ?  
upvoted 2 times

□ **Casticod** 8 months, 1 week 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 4 times

□ **nsotis28** 8 months, 1 week ago

first is correct - will lose the role after 8 hours  
second is questionable -- why not 15 days ?  
upvoted 4 times

□ **cb0900** 8 months, 1 week 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

□ **CheMetto** 6 months, 1 week ago

Nope! It said "you can make the role GA available to activation request <- this is an eligible role! 3 months  
upvoted 1 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'

$disabledPlans = $E3.ServicePlans | Where ServicePlanName -in
("MICROSOFTBOOKINGS") | select -ExcludeProperty ServicePlanID

$licenseOptions = @(
{
    SkuId = $E3.SkuId
    DisabledPlans = $disabledPlans
}
)

Set-AzureADUser -UserId User1@contoso.com -AddLicenses $licenseOptions -RemoveLicenses @()

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'

$disabledPlans = $E3.ServicePlans | Where ServicePlanName -in
("MICROSOFTBOOKINGS") | select -ExcludeProperty ServicePlanID

$licenseOptions = @(
{
    SkuId = $E3.SkuId
    DisabledPlans = $disabledPlans
}
)

Set-AzureADUser -UserId User1@contoso.com -AddLicenses $licenseOptions -RemoveLicenses @()

Set-MgUserLicense
Set-MSOLUser
```

**Correct Answer:**

 **Ruhansen** Highly Voted 7 months, 2 weeks ago

Correct - All Graph commands

upvoted 5 times

 **Amir1909** Most Recent 3 months ago

Correct

upvoted 1 times

 **929826d** 8 months, 2 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 4 times

Question #63

Topic 1

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**

*Community vote distribution*

A (100%)

✉  **nordbymikael** 1 month, 1 week ago

**Selected Answer: A**

PIM is correct because you can make eligible assignments that expire after a certain amount of time  
upvoted 2 times

✉  **benpatto** 5 months, 1 week ago

**Selected Answer: A**

Correct  
upvoted 4 times

✉  **BossLG** 6 months, 1 week ago

Azure AD Privileged Identity Management (PIM) is correct Ref Question #61 <https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings?source=recommendations>  
upvoted 3 times

✉  **Paul\_white** 7 months ago

GIVEN ASNWERS IS CIRRECT!!!  
upvoted 4 times

✉  **BRico6969** 2 months, 3 weeks ago

Calm down Paul  
upvoted 4 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 (70%)

AB (30%)

✉  **sherifhamed** Highly Voted 7 months, 1 week 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 14 times

✉  **daye** 5 months, 3 weeks ago

Agree, A will only show issues not news. I just check it.

upvoted 3 times

✉  **Hard1k** Highly Voted 8 months 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 application 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 6 times

✉  **Shloeb** 7 months, 1 week 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

✉  **ubiquituz** Most Recent 3 months, 1 week ago

B&D

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/admin/manage/message-center.md>

upvoted 1 times

✉  **ubiquituz** 3 months, 1 week ago

IT IS NOT service health...service health is for....You can view the health of your Microsoft services, including Office on the web, Microsoft Teams, Exchange Online, and Microsoft Dynamics 365 on the Service health page in the Microsoft 365 admin center.

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

upvoted 1 times

✉  **saya\_222** 7 months, 1 week ago

A&B is correct.

<https://www.examtopics.com/exams/microsoft/ms-100/view/7/>

upvoted 1 times

✉  **saya\_222** 7 months, 1 week ago

Topic2 #19

upvoted 1 times

 **sherifhamed** 7 months, 1 week 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 3 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

You have a Microsoft 365 subscription that contains the domains shown in the following exhibit.

## Domains

[+ Add domain](#) [Buy domain](#) [Refresh](#)

Domain name ↑	Status	<a href="#">Choose columns</a>
<input type="checkbox"/> Sub1.contoso221018.onmicrosoft.com (D...)	<span style="color: orange;">⚠ Possible service issues</span>	店铺: 学习小店66
<input type="checkbox"/> contoso.com	<span style="color: blue;">ℹ Incomplete setup</span>	
<input type="checkbox"/> contoso221018.onmicrosoft.com	<span style="color: green;">✓ Healthy</span>	
<input type="checkbox"/> Sub2.contoso221018.onmicrosoft.com	<span style="color: blue;">ℹ Incomplete setup</span>	

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**

*Community vote distribution*

D (90%) 10%

 **amurp35** Highly Voted 7 months, 2 weeks 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 23 times

 **Vaerox** 3 months, 2 weeks ago

Agreed. Just added my own domain to a test tenant but then did not add the verification TXT record to the hosting provider. Status of the domain in Microsoft 365 is "Incomplete setup".

I was NOT able to add a new user with that domain.

upvoted 1 times

 **m43s** 3 months, 2 weeks ago

I agree too

upvoted 1 times

 **krzysztofbr** 5 months ago

agree.

upvoted 3 times

 **nsotis28** Highly Voted 8 months, 2 weeks ago

Domains with status "Incomplete setup" can not be used

upvoted 7 times

 **Eckay9** Most Recent 1 week, 1 day ago

**Selected Answer: B**

If you go by the picture, the answer is B. This is because contoso.com and sub2.contoso221018.onmicrosoft.com have an incomplete setup. If you go by the logic, it's a complete nonsense since sub2 has already been verified via the main domain.

upvoted 1 times

□ **momowagdy** 3 weeks, 5 days ago

Hello guys, the correct answer is D. I tested 4 domains with the three status and the three of them are functioning without errors.

upvoted 1 times

□ **CharlesS76** 4 weeks, 1 day ago

After reading through everyone's responses I was so confused I setup the question in my 365 lab environment. I was able to use a healthy domain and its subdomain with incomplete setup, and its 2nd subdomain with Possible service issues to create a new user. I could not use an unverified root domain. So the correct answer (lab tested 4/7/24) is C.

upvoted 1 times

□ **TheMCT** 3 months ago

contoso.com and sub2.contoso221018.onmicrosoft.com domains are in incomplete setup status. As such, you cannot use the domains yet; you cannot create users that contain the contoso.com and sub2.contoso221018.onmicrosoft.com domains.

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

upvoted 1 times

□ **mickey88** 4 months, 1 week ago

The Answer is B, Do you guys see Sub.contoso221018.onmicrosoft.com this domain listed in the domain list. It is only Sub1 and Sub2 only.

C. only contoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com

upvoted 1 times

□ **m2L** 4 months, 2 weeks ago

Hello Guys,

Incomplete domains cannot be used to create users. otherwise, a domain with a service health issue is already verified and can be used when creating a user

I Test it.

Regards.

upvoted 2 times

□ **passy951** 5 months ago

**Selected Answer: D**

You can assign all of them, but can't use it.

upvoted 4 times

□ **passy951** 5 months ago

Isn't it a bit confusing? You can assign all Domains to a User, but you can't use it to receive mails for example.

upvoted 1 times

□ **Testtest123** 4 months, 3 weeks ago

Correct, so the answer here is that you can use all the domains to create an user account!

upvoted 1 times

□ **benpatto** 5 months ago

Healthy & possible service issues CAN be used for the following reason: If a domain is either healthy or stating errors, it means the domain has been submitted as a custom domain and VERIFIED (THIS IS THE IMPORTANT PART).

Incomplete setup means the domain has not been verified which means it cannot be used.

upvoted 1 times

□ **Clinson** 5 months, 1 week ago

**Selected Answer: D**

I've created accounts with domains that were in the incomplete setup status and domains with service issues, so I believe it is D.

upvoted 5 times

□ **TP447** 5 months, 3 weeks ago

Contoso.com can be used also (anyone suggesting B is the answer, one of the options for B is a sub domain of Contoso.com and has the same status so that can't be right!).

I believe the answer to be D (All of them) - tested in a lab and Incomplete Status sub domain still allowed me to assign the domain to a user. Answer is D.

upvoted 3 times

□ **Snakad** 6 months ago

Please ignore my comment I got wrong and B is correct

upvoted 1 times

□ **Snakad** 6 months ago

Microsoft Azure / M365

Domain name:

1) Sub1.contoso221018.onmicrosoft.com | Status Possible service issues

2) contoso.com | Incomplete setup

3) contoso221018.onmicrosoft.com | Healthy

4) Sub2.contoso221018.onmicrosoft.com | Incomplete setup

Which domain name suffixes can you use when you create users?  
Only response choice

ChatGPT:

You can use the following domain name suffix when you create users:  
contoso221018.onmicrosoft.com

Why not Sub1.contoso221018.onmicrosoft.com too?

ChatGPT:

I apologize for any confusion. You can indeed use "Sub1.contoso221018.onmicrosoft.com" as a domain name suffix when creating users, as long as it's available and there are no service issues. So, the correct response would be:

Sub1.contoso221018.onmicrosoft.com  
contoso221018.onmicrosoft.com

upvoted 2 times

曰 **daye** 5 months, 3 weeks ago  
my chatgpt said me C haha

"The correct answer is C. Only contoso221018.onmicrosoft.com, Sub1.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com are the domains that are included in your Microsoft 365 subscription."

Afterwards it explains that the issues can be fixed but you can still create users.

he domain Sub1.contoso221018.onmicrosoft.com is a possible service issue because it is a subdomain that you have created under your default domain contoso221018.onmicrosoft.com. However, there might be some problems with the DNS configuration or the service health c

this subdomain

upvoted 1 times

曰 **Shuihe** 6 months ago

contoso221018.onmicrosoft.com, Sub1.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com . Because contoso221018.onmicrosoft.com has already been verified, sub1 and sub2 are sub-domains of contoso221018.onmicrosoft.com, all three domain are able to use.

upvoted 3 times

曰 **gomezmax** 6 months, 3 weeks ago

B is correct

upvoted 1 times

店铺：学习小店66

店铺：学习小店66

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 (75%)

E (25%)

✉ **certma2023** Highly Voted 8 months, 3 weeks 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 18 times

✉ **Clinson** 5 months, 1 week ago

Additionall in my customer's E5 tenant When I add a policy, the only scope available is Exchange. I suspect that will change moving forward bu  
as of today's date it is only Exchange.

upvoted 1 times

✉ **Greatone1** Highly Voted 8 months, 2 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 5 times

✉ **Scotte2023** Most Recent 6 days, 22 hours ago

**Selected Answer: A**

Also, Enabling privileged access management for Exchange Online in Microsoft 365 allows your organization to operate with zero standing privileges and provide a layer of defense against standing administrative access vulnerabilities.

<https://learn.microsoft.com/en-us/purview/privileged-access-management-solution-overview>  
upvoted 1 times

✉ **Scotte2023** 6 days, 22 hours ago

**Selected Answer: A**

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 1 times

✉ **Exam2us** 2 months ago

Looks like A is the correct answer. Rest M365 products support is not finalized - Privileged access management will be available in other Office 365 workloads soon. Visit the Microsoft 365 Roadmap for more details.

upvoted 1 times

✉ **eufdf12342** 3 months, 2 weeks ago

Answer A, only Exchange appears on scope during policy creation.

upvoted 1 times

Charard 3 months, 2 weeks ago

**Selected Answer: A**

EoL only.

upvoted 2 times

NrdAlert 5 months, 3 weeks ago

**Selected Answer: A**

PAM is not the same as Purview as whole which is what others are linking to when answering E. I cannot find anything that confirms PAM is available on anything other than EXO at this time. Every mention of PAM only has example with Azure AD and EXO. No other M365 services seem to be supported.

upvoted 4 times

dlast 6 months ago

**Selected Answer: E**

<https://learn.microsoft.com/en-us/purview/purview#microsoft-purview-risk-and-compliance-solutions>

upvoted 1 times

poesklap 6 months, 1 week ago

**Selected Answer: E**

Microsoft Purview is primarily designed to manage and control privileged access to resources within Azure Active Directory (Azure AD) and Microsoft 365 services. The workloads in Microsoft 365 that support privileged access management typically include:

E. Microsoft Teams, Exchange Online, and SharePoint Online

upvoted 1 times

dennis123 6 months, 2 weeks ago

**Selected Answer: E**

Answer E:

Microsoft Purview includes risk and compliance solutions that support services included in Microsoft 365. These services include Microsoft Teams, SharePoint, OneDrive, Exchange, and others. These compliance and risk solutions help your organization to:

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

upvoted 3 times

sherifhamed 7 months, 1 week 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 workload. 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 7 months, 2 weeks ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/purview/privileged-access-management>

upvoted 5 times

sherifhamed 7 months, 1 week 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 7 months, 1 week 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 3 times

jbuexamtopics 7 months, 1 week ago

Sorry this is for Access Support. But still, can you show us where it's mentioned on the link?

upvoted 1 times

spektrum1988 3 months, 1 week ago

I'm pretty sure they mean "when will privileged access management support..."

upvoted 1 times

PhoenixMan 7 months, 3 weeks 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** 8 months ago

**Selected Answer: E**

I agree E

upvoted 1 times

□  **DiligentSam** 8 months, 2 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

□  **amurp35** 7 months, 2 weeks ago

Exactly: <https://learn.microsoft.com/en-us/purview/privileged-access-management> meaning PAM is not supported outside of Exchange Online.

upvoted 1 times

□  **SandyBridge** 7 months, 2 weeks ago

If you are going to use ChatGPT, do us all a favor and do not spread misinformation.

upvoted 8 times

□  **mrac** 8 months, 3 weeks 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 8 months, 3 weeks 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 34 times

daye 5 months, 3 weeks ago

Exactly!

Release Preferences and User 1

upvoted 4 times

nsotis28 Highly Voted 8 months, 2 weeks ago

release preferences  
user1

upvoted 15 times

□ **Casticod** 8 months, 1 week ago

Me too

<https://learn.microsoft.com/en-us/microsoft-365/admin/manage/release-options-in-office-365?view=o365-worldwide>

upvoted 6 times

□ **haimrevolution** Most Recent 3 months, 1 week ago

The answer is definitely wrong why would a global admin not have the ability

upvoted 1 times

□ **Festus365** 5 months ago

Can user2 service support administrator modify the setting?

upvoted 1 times

□ **imlearningstuffagain** 6 months, 3 weeks 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

**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:

A screenshot of a dropdown menu with the following options: Anti-spam, Anti-Phishing, Safe Attachments, and Safe Links. The menu has a standard Windows-style border and a downward-pointing arrow in the top right corner.

Impersonation and spoofing attacks in email messages:

A second screenshot of a dropdown menu with the same four policy options: Anti-spam, Anti-Phishing, Safe Attachments, and Safe Links. This menu is also styled like the first one.

**Answer Area**

Opening files in SharePoint that contain malicious content:

A screenshot of a dropdown menu for SharePoint malicious content. The option 'Safe Attachments' is highlighted with a black rectangular box around it. The other options are 'Anti-spam', 'Anti-Phishing', and 'Safe Links'. The menu has a standard Windows-style border and a downward-pointing arrow.

**Correct Answer:**

Impersonation and spoofing attacks in email messages:

A second screenshot of a dropdown menu for email spoofing attacks. The option 'Anti-Phishing' is highlighted with a black rectangular box around it. The other options are 'Anti-spam', 'Safe Attachments', and 'Safe Links'. The menu has a standard Windows-style border and a downward-pointing arrow.

✉️ **PhoenixMan** 5 months, 2 weeks ago

in today exam  
upvoted 4 times

✉️ **gomezmax** 8 months ago

Correct  
upvoted 2 times

✉️ **Greatone1** 8 months, 2 weeks ago

Yes correct  
safe attachments  
anti-phishing  
upvoted 3 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 小店66	Active	-	Threat management	2	店铺: 学习小店66 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

✉  **saya\_222**  7 months, 1 week 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 18 times

✉  **sergioandresiq** 6 months, 2 weeks ago

Yes, I tested just to confirm, you can roll-back a resolved alert to Dismissed, Investigating, or Active  
upvoted 1 times

✉  **Romke\_en\_Tomke** 7 months ago

You can post direct url: <https://www.examtopics.com/discussions/microsoft/view/94571-exam-ms-101-topic-3-question-140-discussion/>  
upvoted 2 times

✉  **m2L**  4 months, 2 weeks ago

Please guys can you test a gain?  
On my side I tested with 2 different Alerts, but after changing their state to "resolved". I wouldn't be able to roll back to DISMISS or

## INVESTIGATING.

So I confirm that the given answers are correct.  
upvoted 3 times

✉ **faeem** 7 months, 1 week 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 4 times

✉ **sergioandreslq** 6 months, 2 weeks ago

Yes, I tested just to confirm, you can roll-back a resolved alert to Dismissed, Investigating, or Active  
upvoted 2 times

✉ **amurp35** 7 months, 2 weeks 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 3 times

✉ **daye** 5 months, 3 weeks ago

This Alert is from Purview not from Security Admin, so the actions are different.

I just test it, and you can rollback it. In my case, I didn't have any explicit button but changing the comments, I was able to change the status as well.

<https://learn.microsoft.com/en-us/purview/compliance-manager-alert-policies>

upvoted 2 times

✉ **AMDF** 8 months ago

Alert1 correct  
Alert5 should be "not change status"

For resolved issue there is no option to change status

upvoted 2 times

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 Highly Voted 8 months ago

**Selected Answer:** BE

Correct answers

upvoted 6 times

✉  sigvast Most Recent 5 months, 3 weeks ago

Correct.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1-2?view=o365-worldwide>

Defender P2 required for advanced hunting and device discovery

Vulnerability add-on required for digital certificate assessment

upvoted 2 times

✉  letters1234 8 months, 1 week 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 8 months, 2 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 4 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*

D (79%)

C (21%)

✉ **northgaterebel** Highly Voted 6 months, 1 week ago

**Selected Answer: D**

Data from Microsoft Defender for Endpoint is retained for 180 days, visible across the portal. However, in the advanced hunting investigation experience, it's accessible via a query for a period of 30 days. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/data-storage-privacy?view=o365-worldwide#how-long-will-microsoft-store-my-data-what-is-microsofts-data-retention-policy>

upvoted 12 times

✉ **ITCALegends** Highly Voted 5 months, 2 weeks ago

**Selected Answer: D**

It was 90 days but was changed in october to 180 days so make of that what you will  
upvoted 5 times

✉ **examcrammer** Most Recent 2 weeks, 1 day ago

**Selected Answer: C**

C is correct until the exam is updated. After that it is D.  
The English language version of this exam will be updated on April 26, 2024. Review the study guide linked in the "Tip" box for details on upcoming changes. If a localized version of this exam is available, it will be updated approximately eight weeks after this date.  
upvoted 1 times

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

**Selected Answer: D**

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

On the top navigation you can:  
Customize columns to add or remove columns  
Apply filters  
Display the alerts for a particular duration like 1 Day, 3 Days, 1 Week, 30 Days, and 6 Months  
Export the alerts list to excel  
Manage Alerts  
upvoted 2 times

✉ **Amir1909** 3 months ago

C is correct  
upvoted 1 times

✉ **AncaMada112233** 5 months, 3 weeks ago

"Alerts are displayed in the portal for 90 days, even if the resource related to the alert was deleted during that time. This is because the alert might indicate a potential breach to your organization that needs to be further investigated." - from: <https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview>  
upvoted 3 times

✉ **HeirrBourne** 5 months, 3 weeks ago

its correct  
<https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview>  
upvoted 1 times

✉ **daye** 5 months, 3 weeks ago

**Selected Answer: D**

I just tested and you can filter it for 6 months, also it's explained here:

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue?view=o365-worldwide>  
upvoted 4 times

✉️ **dlast** 6 months ago

**Selected Answer: C**

The retention period is asked for alert data. This should be 90 days ( 3months) see <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data-retention?view=o365-worldwide#defender-for-office-365-plan-1>  
Given answer is correct

upvoted 1 times

✉️ **daye** 5 months, 3 weeks ago

No, it's not, this link talks about defender for office but the question is talking about Defender portal. I just tested and you can filter it for 6 months

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue?view=o365-worldwide>  
upvoted 3 times

✉️ **sergioandreslq** 6 months, 2 weeks ago

I went to defender portal--> blade alerts --> time period and I can go back 6 months.  
my answer is D: 6 months  
upvoted 3 times

店铺：学习小店66

✉️ **sergioandreslq** 5 months, 3 weeks ago

I re-confirm in defender portal that action center is 6 months.  
Defender-->Actions&Submitions-->Action Center--> History tab--> Select the time to see and export.

the issue with this question is that Microsoft upgrade the service from 3 months to 6 months few months ago and exist the risk that this answer is now updated to 6 months,

so, it is a risk either to choose 3 months or 6 months because we don't know if this is updated or not.

upvoted 3 times

✉️ **Casticod** 8 months, 1 week ago

**Selected Answer: C**

Correct <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data-retention?view=o365-worldwide>  
upvoted 4 times

✉️ **daye** 5 months, 3 weeks ago

No, it's not, this link talks about defender for office but the question is talking about Defender portal. I just tested and you can filter it for 6 months

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue?view=o365-worldwide>  
upvoted 2 times

店铺：学习小店66

店铺：学习小店66

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 (53%)

A (35%)

12%

✉️ **KairKnows** Highly Voted 5 months ago

Answer should be 1 Day

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-email-security?view=o365-worldwide#export-report-data>  
upvoted 15 times

✉️ **KairKnows** 4 months, 3 weeks ago

This question is also asked in the Microsoft Learn practice test and the correct answer is 1 Day.

upvoted 9 times

✉️ **Kmkz83510** 4 months, 2 weeks ago

Just to add on - there might be confusion because the wording says that 30 days is available. however note the question is about the time range that can be included in the report (ie exported). That is indeed 1 day.

upvoted 3 times

✉️ **cb0900** Highly Voted 8 months 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 5 times

✉️ **LLama33** Most Recent 3 weeks, 1 day ago

just tried for DETAIL DATA EXPORT is 1 day  
here an error message from the console:

For detailed data exports, we only support a time range of one day. Please adjust your time range selection.

upvoted 3 times

✉️ **eks913** 1 month ago

**Selected Answer: A**

MS Training says 1 DAY.

upvoted 2 times

✉️ **HelloItsSam** 1 month, 1 week ago

**Selected Answer: B**

7 days:

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

✉️ **Tuno** 1 month, 2 weeks ago

1 day.

" Select a view to export: Select one of the following values:

Summary: Data from the last 90 days is available. This is the default value.

Details: Data from the last 30 days is available. A date range of one day is supported.'

For the detailed report (Details option), data from the last 30 days is available, but you can only export the report for a date range of one day at a time. This means that while you can access data from the past 30 days, you must select a single day within that range for the detailed export.

upvoted 1 times

✉️ **Craiggg** 2 months, 2 weeks ago

This is a question in the Microsoft question. They have it at one day.

upvoted 1 times

Hasa 2 months, 3 weeks ago

On the report page, select Export.

In the Export conditions flyout that opens, review and configure the following settings:

Select a view to export: Select one of the following values:

Summary: Data from the last 90 days is available. This is the default value.

Details: Data from the last 30 days is available. A date range of one day is supported. <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-email-security?view=o365-worldwide#export-report-data>

upvoted 1 times

Y2 2 months, 3 weeks ago

**Selected Answer: A**

The answer is 1 day, a lot of the questions with disputed answers are answered correctly in the Microsoft practice assessment:

<https://learn.microsoft.com/en-us/credentials/certifications/exams/ms-102/practice/assessment?assessmentId=75&assessment-type=practice>

upvoted 4 times

Y2 2 months, 3 weeks ago

You can export the URL threat protection report from the Microsoft 365 Defender portal by selecting Reports, Email & collaboration, and then URL threat protection. You can export a Summary report of URL threat protection for a long period, but a detailed report (Details option) can be exported only for a single day. If you want to export the report for a longer period, you will get the following error message: "For detailed data exports, we only support a time range of one day. Please adjust your time range selection." The longest time range that can be used in the detailed URL threat protection report is one day.

upvoted 1 times

Amir1909 3 months ago

C is correct

upvoted 1 times

Charard 3 months, 2 weeks ago

**Selected Answer: B**

7 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

nils241 4 months ago

A

Read the question: "What is the longest time RANGE that can be INCLUDED in the REPORT?"

You have access to the data for last 30 Days. Inside a SINGLE report you have a time range of 1 day!

upvoted 1 times

Shuihe 5 months ago

For detailed data exports, only support a time range of one day.

upvoted 1 times

WizerEyez 5 months, 2 weeks ago

I think the answer is 90 days because if you sort the filter, the date range can go back about 3 months.

upvoted 2 times

maltns 2 months, 3 weeks ago

just tested it and the export starts from 14.11.23 till today = 90 days!

upvoted 1 times

Casticod 8 months, 1 week ago

**Selected Answer: C**

Correct <https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-users?view=o365-worldwide#timeline>

upvoted 4 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.

**Correct Answer:**

店铺：学习小店66

Add trusted senders and domains
Enable domains to protect
<b>Enable users to protect</b>
Phishing email threshold

Add trusted senders and domains
Enable intelligence for impersonation protection
<b>Enable spoof intelligence</b>

✉  **omnomsnom** 3 months, 2 weeks ago

You should only add a sender to the trusted senders to bypass the user impersonation checks for that person. E.g., if the CEO sends email into the org from his personal email account, or the CEO of the other organisation happens to have the exact same name as another protected user. Mailbox Intelligence uses the users individual patterns of communication to help protect them against impersonation/spoofing, so this is the most relevant feature for the second part of the question in, my opinion. In the real world, ensuring smooth communication should never be at the expense of security, but who knows what Microsoft want us to answer here.

upvoted 1 times

✉  **sergioandreslq** 6 months, 2 weeks ago

the suggested answers are correct:

Enable uses to protect: Add the CEO display name and the email to avoid impersonation.

Add trusted senders and domains: Add the CEO email to the trusted sender list. this will avoid to tag any email from this CEO as phishing if Display name and email match.

upvoted 4 times

✉️ **faeem** 7 months, 1 week 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 2 times

✉️ **amurp35** 7 months, 2 weeks 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 4 times

✉️ **Casticod** 8 months 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 2 times

✉️ **letters1234** 8 months, 1 week 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

曰  **Greatone1** Highly Voted 8 months, 2 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 7 times

曰  **jt2214** Highly Voted 7 months, 1 week ago

I wish they were all this easy.  
upvoted 6 times

曰  **sehlohomoletsane** 6 months ago

No cause same  
upvoted 1 times

曰  **Tomtom11** Most Recent 2 months, 3 weeks ago

You can promote or demote the rank of a device group so that it's given higher or lower priority during matching. A device group with a rank of is the highest ranked group. When a device is matched to more than one group, it's added only to the highest ranked group. You can also edit an delete groups.

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

✉️ 🚩 **Festus365** 5 months, 3 weeks ago

Server1-London = Operating system windows server 2016 appears to be in group 3 not group 2 [Can anyone say something about this]  
upvoted 2 times

✉️ 🚩 **benpatto** 5 months ago

This is because, as part of the filtering, group 2 says 'Has London' in the name. Rankings are what matter on this question, although Server1-London can go in both 2 & 3, the highest rank will always come first.  
upvoted 2 times

✉️ 🚩 **amurp35** 7 months, 2 weeks ago

Yes, answer is correct due to rankings.  
upvoted 4 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

**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**

Anti-malware

Anti-phishing

Anti-spam

Safe Attachments

**Answer Area**

Customize the common attachments filter:

Anti-malware

Enable impersonation protection for sender domains:

Anti-phishing

**Policy Types****Answer Area**

Customize the common attachments filter:

Anti-malware

**Correct Answer:**

Enable impersonation protection for sender domains:

Anti-phishing

Anti-spam

Safe Attachments

 **f7d3be6** Highly Voted 8 months, 2 weeks ago

Correct Antimalware ,anti-phishing <https://answers.microsoft.com/en-us/msoffice/forum/all/impersonation-protection/97b82164-5331-4ee6-97e0-423f17c55399>

upvoted 7 times

 **Amir1909** Most Recent 3 months ago

Correct

upvoted 1 times

 **benpatto** 5 months ago

Correct, common attachments is used when blocking emails from being sent which have attachments to them. Safe attachments (which looks the nicest) checks the attachments in emails etc rather than just blocking them so is slightly different.

upvoted 2 times

 **amurp35** 7 months, 2 weeks ago

Correct

upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

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 (75%)

C (25%)

AMDf Highly Voted 8 months 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 15 times

amurp35 Highly Voted 7 months, 2 weeks 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 5 times

Jillis Most Recent 7 months, 3 weeks ago

**Selected Answer: A**

AMDF is correct

upvoted 3 times

letters1234 8 months, 1 week 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 3 times

mccheesey 8 months, 2 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 3 times

曰 **Greatone1** 8 months, 2 weeks ago

<https://www.examtopics.com/discussions/microsoft/view/49358-exam-ms-101-topic-2-question-27-discussion/>

upvoted 3 times

曰 **Greatone1** 8 months, 2 weeks ago

**Selected Answer: A**

A is correct

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

upvoted 4 times

曰 **Casticod** 8 months, 2 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 3 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** Highly Voted 7 months, 4 weeks 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 12 times

✉  **Amir1909** Most Recent 3 months ago

Correct

upvoted 1 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	Unassigned 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**

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
**Answer Area****Statements**

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

✉️  **Greatone1**  8 months, 2 weeks ago

No - High severity Alert.

No - Doesn't have 'Device' in name.

Yes - Has OS name Andriod and Tag contains 'Inventory'

upvoted 8 times

店铺：学习小店66

✉️  **Motanel**  3 weeks ago

Yes - the severity is set to low, so it will be any alerts from low, medium, high

No

Yes

upvoted 3 times

✉️  **OwerGame** 1 month, 1 week ago

It catches low and above incidents, not specifically low incidents, so it will catch the high severity alert.

Yes

No

Yes

upvoted 2 times

✉️  **amurp35** 7 months, 2 weeks ago

Correct  
upvoted 2 times

✉  **nsotis28** 8 months, 2 weeks ago  
correct answer  
upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

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

The screenshot shows the 'Edit policy' screen for 'Policy1'. At the top, there are 'Edit policy' and 'Delete policy' buttons. A 'Status' toggle switch is set to 'On'. Below this, under 'Name your alert', there is a 'Description' field with 'Add a description' and a 'Severity' field set to 'Medium'. Under 'Category', it says 'Information governance'. In the center, there is a red watermark reading '店铺: 学习小店66'. Below this, the 'Create alert settings' section includes 'Conditions' (Activity is FileChangeActivity), 'Aggregation' (Aggregated), 'Scope' (All users), 'Threshold' (5), and 'Window' (1 hour). Under 'Set your recipients', there is a 'Recipients' field with 'User1@sk220912.outlook.onmicrosoft.com' and a 'Daily notification limit' of 25. To the right of the recipient field is a blue icon with a white question mark and a dark blue icon with a white speech bubble.

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 (70%)

D (30%)

✉ **Jillis** [Highly Voted] 7 months, 3 weeks 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 12 times

✉ **Jahanzeb88** 7 months, 2 weeks ago

so the aggregated threshold is 5, so shouldnt the answer be 5 as well?

upvoted 1 times

✉ **daye** 5 months ago

no, threshold 5 windows 1 hour, it means 5 attempts during 1 hour will generate 1 alert. Therefore, 2 alerts.

upvoted 6 times

✉️ 🚩 **9711d59** 2 months, 4 weeks ago

But we have try every 4 minutes during 1 hour, so we have 3 alerts during 1 hour  
upvoted 3 times

✉️ 🚩 **santi32** Highly Voted 7 months, 2 weeks 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 6 times

✉️ 🚩 **daye** 5 months, 3 weeks ago

exactly, it will create an alert per hour, that's all. 2 alerts -> A  
upvoted 1 times

✉️ 🚩 **ThomasMcThomasface** Most Recent 6 months, 1 week ago

**Selected Answer: A**

Window: 1 hour. So as I read it, there will be a notification once per hour

upvoted 2 times

✉️ 🚩 **sergioandreslq** 6 months, 2 weeks ago

The aggregate interval could be 1 minute or 15 min depending on the Microsoft365 subscription.  
<https://learn.microsoft.com/en-us/purview/alert-policies?view=o365-worldwide#alert-aggregation>

In that case, you will have the first alert at minutes 20, 40, 60, 80, and 120. The total number of alerts will be 5.

My selection will be 5 following the Microsoft article related the aggregate interval which in this case the max is 15 min but each threshold is reached every 20 min. each even will generate a single alert.

upvoted 1 times

✉️ 🚩 **sergioandreslq** 5 months, 3 weeks ago

Sorry for my wrong answer, the window interval is 1 hour, which means that 1 alert will be triggered per hour if threshold 5 is reached in this hour.  
The correct answer is the A.  
upvoted 2 times

✉️ 🚩 **gomezmax** 6 months, 3 weeks ago

I'm Sorry for My Wrong Answer, but it is A  
upvoted 1 times

✉️ 🚩 **Greatone1** 7 months ago

2 is correct answer  
<https://www.examtopics.com/discussions/microsoft/view/94370-exam-ms-101-topic-3-question-150-discussion/>  
upvoted 2 times

✉️ 🚩 **spectre786** 7 months, 4 weeks ago

Anyone got the right answer please?  
upvoted 1 times

✉️ 🚩 **nsotis28** 8 months, 2 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** 7 months, 4 weeks ago

So right answer is A. 2 ?  
upvoted 2 times

✉️ 🚩 **gomezmax** 8 months, 2 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%)

✉  **solderboy**  4 months ago

**Selected Answer: B**

Answer is B

- EDIT: The information in the UPDATE column will be used to modify the attribute value for the selected object.
- COMPLETE: The original value is acceptable and should not be changed despite being identified as being in an error state.

<https://microsoft.github.io/idfix/Step%203%20-%20Query%20and%20fix%20invalid%20attributes/>  
upvoted 5 times

✉  **Greatone1**  8 months, 2 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 3 times

✉  **Casticod** 8 months, 2 weeks ago

**Selected Answer: B**

Correct It is necessary to modify the maximum threshold of modifications in each synchronization.  
upvoted 2 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.)

店铺：学习小店66

**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.

User2 can authenticate to Azure AD by using a username of user2@contoso.com.

User3 can authenticate to Azure AD by using a username of user3@contoso.com.

**Answer Area****Statements**

**Yes**   **No**

User1 can authenticate to Azure AD by using a username of user1@contoso.com.

Correct Answer:

User2 can authenticate to Azure AD by using a username of user2@contoso.com.

User3 can authenticate to Azure AD by using a username of user3@contoso.com.

✉  **Greatone1**  8 months, 2 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 14 times

✉  **OwerGame**  2 months, 1 week ago

Federation is disabled

upvoted 1 times

✉  **Vaerox** 3 months, 2 weeks ago

This question is a typical "it's too good to be true" type of question, if you ask me. Statements and answers are too obvious. I don't think this question will appear on the exam.

upvoted 3 times

✉  **Haso** 4 months, 1 week ago

Question: What would be the answer, if password hash was enabled?

upvoted 2 times

✉  **rfree** 7 months, 1 week 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** 7 months, 1 week ago

Pass-through is enabled so the AD server authenticates the password

upvoted 4 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

certma2023 [Highly Voted] 8 months, 3 weeks 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 supporter. Agent installation on Windows Server Core is not supported.

upvoted 6 times

daye [Most Recent] 5 months, 3 weeks ago

Answer is correct but this agent is only required in ONE on server, that can be a DC or a member server.

However, Microsoft recommends to enable High Availability, that's why it should be install in multiple servers.

Since MS recommends to be installed in 3 servers but is Core servers is not supported, then the answer is correct (server 1 & 2 with the provisioning agent)

upvoted 1 times

letters1234 8 months, 1 week 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

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

**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.



User2 can access Site1 from Device2.



User2 can access Site1 from Device3.

店铺

**Answer Area****Statements****Yes****No**

Correct Answer:

User1 can access Site1 from Device1.



User2 can access Site1 from Device2.



User2 can access Site1 from Device3.

amurp35 Highly Voted 7 months, 2 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 35 times

Paul\_white 7 months ago

MY BROTHER YOU ARE TOO GOOD!!!! EXCELLENT RESPONSE

upvoted 5 times

ghjbhj 7 months, 2 weeks 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 3 times

Motanel 1 week, 5 days ago

But if the filter is not applied, then the default will be applied, which is allow, right?

upvoted 1 times

ThomasMcThomasface 6 months, 1 week ago

This translation is so very useful to me. Thank you so much. We need more people like you

upvoted 2 times

Moazzamfaroqiiii Most Recent 2 months, 1 week ago

All the devices are called Device so there is a filter to exclude device. They all have device name So does that not mean YYY

upvoted 1 times

692a0df 3 months ago

Y/Y/Y for me...

First one: my reading on this - as the device is not registered in Azure AD then the CAP does not apply. Then it's down to the Global settings (Sharepoint Admin -> Policies -> Access Control -> Unmanaged Device) for unmanaged devices (see link) which by default is set to 'Allow full access'.

[https://learn.microsoft.com/en-US/sharepoint/control-access-from-unmanaged-devices?WT.mc\\_id=365AdminCSH\\_spo](https://learn.microsoft.com/en-US/sharepoint/control-access-from-unmanaged-devices?WT.mc_id=365AdminCSH_spo)

upvoted 2 times

SBCM 3 months ago

CA Policy does apply to every user, and because the device is unregistered it is not query'd for its name so the policy does NOT filter him out meaning the device will be blocked.

upvoted 1 times

daye 5 months ago

but... a non Azure AD device cannot be applied by a Conditional Access, therefore it won't validate it, so it won't be blocked. In other words, it's a cloud solution for a non cloud identity device. Am I missing something?

upvoted 1 times

daye 5 months ago

ah ok, I just get the ghjbhj comment. Unregistered device + positive operators = filter not applied = blocked

upvoted 1 times

hoge 8 months, 2 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 7 months, 4 weeks 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

CheMetto 6 months, 1 week ago

it's block, you are right, but CA condition said "Exclude device that starts with Device", so NYY

upvoted 1 times

PhoenixMan 7 months, 3 weeks ago

Yes I think the same, the policy blocks access and the answer should be Y/N/N

upvoted 3 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

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 (85%)	Other
---------	-------

✉️  **letters1234** Highly Voted 8 months, 1 week 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 11 times

✉️  **Shloeb** 7 months 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** 7 months, 2 weeks ago

You are thinking of user-risk, which gets remediated through SSPR.

upvoted 1 times

✉️  **Scotte2023** Most Recent 6 days, 21 hours ago

**Selected Answer: D**

Self-remediation with self-service password reset

If a user has registered for self-service password reset (SSPR), then they can remediate their own user risk by performing a self-service password reset.

<https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-remediate-unblock#self-remediation-with-risk-based-policy>

upvoted 1 times

✉️  **MarcMouelle** 3 weeks, 4 days ago

**Selected Answer: C**

La réponse C est l'idéal et rendu possible avec la sélection du pays/régions. L'utilisateur devra tout simplement partager ses coordonnées GPS à partir de l'application ms authentificateur , ceci est plus efficace et adéquat que de demander à un utilisateur de changer son mot de passe à chaque connexion

upvoted 1 times

✉️  **OwerGame** 2 months, 1 week ago

Excluding the users from the CA, and making separate CA policy for their department would be the easiest way. Although impossible travel alert works taking time and time zones into consideration and wouldn't trigger as often as You think in practice. SSPR is the next most viable option here.

upvoted 1 times

✉️  **Amir1909** 3 months ago

D is correct

upvoted 1 times

✉️ **Blixa** 4 months, 4 weeks ago

Question must be wrong - since it is a sign-in risk they should be able to verify their identity with MFA not getting help changing password.  
upvoted 3 times

✉️ **NrdAlert** 5 months, 3 weeks ago

**Selected Answer: B**

For some reason everyone is thrown off by this question. You actually have two separate groups of users to consider here. One(France) has MFA registered and can be prompted for MFA anytime they need to remediate. The other is simply a marketing group. Imagine all these traveling users having to reset their password to remediate after every high risk sign-in. That is certainly not the result we want. They really need MFA and modifying the MFA policy can have them all register.

upvoted 1 times

✉️ **NrdAlert** 5 months, 3 weeks ago

Reread and I'm wrong. :-( It says all users are in france and they all have MFA. My bad.

The only high risk event that would trigger that can't be remediated by MFA is a compromised account or password leak if using Identity Protection. D - SSPR is where it's at.

upvoted 1 times

✉️ **poesklap** 6 months, 1 week ago

**Selected Answer: D**

If a user has registered for self-service password reset (SSPR), then they can remediate their own user risk by performing a self-service password reset.

<https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-remediate-unblock>

upvoted 2 times

✉️ **CheMetto** 6 months, 1 week ago

B guys. Try to create a risky sign-in policy. You can allow but the only option available is "Require MFA". SSPR is used for risky users policy, not sign-in  
upvoted 1 times

✉️ **CheMetto** 6 months, 1 week ago

ops... sorry,. All users are in france, so modifying MFA doesn't make any sense... yes, go with D

upvoted 1 times

✉️ **sergioandreslq** 6 months, 2 weeks ago

For me, the correct answer will be B.  
the admins need to update the MFA registration policy to include the countries where the rep will travel.  
This will allow the user if he is detected as Sign-in risk to auto-remediate the issue.

the SSPR will apply for User-risk which in this case is not the requested.

Auto-remediation for Sign-in risk is MFA

Auto-remediation for User risk is SSPR.

named locations: I can list the countries to allow the connection of the representant, but, the user will be excluded for MFA which is not good.

Exclude group doesn't apply, I won't remove MFA for the user authentication, more when he is traveling and I need to open the registration from others countries.

upvoted 1 times

✉️ **santi32** 7 months, 2 weeks 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 3 times

✉️ **amurp35** 7 months, 2 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** 7 months, 2 weeks 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** 8 months, 1 week ago

The Answer Is C

upvoted 1 times

✉  **DiligentSam** 8 months, 1 week 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** 7 months, 2 weeks ago

Why do people supply 'answers' from ChatGPT? It makes things up, literally.

upvoted 1 times

✉  **amurp35** 7 months, 2 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.  
~~店铺：学习小店66~~

upvoted 1 times

✉  **Ranger\_DanMT** 8 months, 1 week 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** 8 months, 1 week ago

Pretty sure the answer to this would be B?

upvoted 1 times

店铺：学习小店66

店铺：学习小店66

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 (67%)

C (33%)

✉️  **CharlesS76** 4 weeks, 1 day ago

**Selected Answer: D**

UPN is the ONLY attribute used for account login (not email or aliases). The answer is D - change the UPN to match the email address that the user wants to log in with.

upvoted 1 times

✉️  **nordbymikael** 1 month, 1 week ago

**Selected Answer: D**

The UPN is the username you use to sign in. To sign in with other credentials than your UPN, you have to change the UPN.

upvoted 1 times

✉️  **Amir1909** 3 months ago

D is correct

upvoted 1 times

✉️  **benpatto** 5 months ago

Realistically the answer is tell the user to stop being awkward and sign in with the UPN HOWEVER, its Microsoft, so change the UPN is the best option.

upvoted 4 times

✉️  **2dwarf** 5 months, 1 week ago

**Selected Answer: D**

D is right

upvoted 1 times

✉️  **TP447** 5 months, 3 weeks ago

Unsure on the confusion here. UPN is the ONLY attribute used for account login (not email or aliases). The answer is D - change the UPN to match the email address that the user wants to log in with.

upvoted 3 times

✉️  **jt2214** 6 months, 3 weeks ago

**Selected Answer: D**

I agree with Milad

upvoted 1 times

✉️  **MZeeshanTayyab** 6 months, 4 weeks ago

**Selected Answer: D**

D is right

upvoted 2 times

✉  **Paul\_white** 7 months ago

ANSWER IS D

upvoted 3 times

✉  **darcone23** 7 months 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 3 times

✉  **Milad666** 7 months 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 8 times

✉  **spectre786** 7 months, 4 weeks ago

I think it's D. Modify the UPN

upvoted 2 times

店铺：学习小店66

店铺：学习小店66

**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 Azure AD Connect interface. On the left, a 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), 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 (which is checked), Program Data, System, and Users. At the bottom are 'Previous' and 'Next' 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** *店铺：学习小店66*  
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	CN=Group2,OU=OU2,DC=fabrikam,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
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 type="radio"/>	<input type="radio"/>

✉  **Greatone1**  8 months, 2 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 8 times

✉  **Tomtom11**  1 month, 1 week ago

<https://azurecloudai.blog/2019/10/20/field-notes-azure-active-directory-connect-domain-ou-and-group-filtering/>

upvoted 1 times

✉  **Festus365** 3 months ago

{Group2 and User3 belong to OU2 initially}. NYY is correct  
upvoted 2 times

✉  **benpatto** 5 months ago

Answers are correct, if a user or group has been assigned directly to an OU, they will sync. If they're only nested within a group that is in that OU, the main user account or group will be hiding away somewhere different in the AD Forest so will not sync.  
upvoted 2 times

✉  **ATHOOS** 5 months, 2 weeks ago

Group2 will not be synchronized...  
NNY  
upvoted 2 times

✉  **amurp35** 7 months, 2 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 3 times

店铺: 学习小店66

✉  **Vaerox** 3 months, 1 week ago

But User2 is a member of Group2 and Group2 is a member of OU2...I'm confused.  
upvoted 2 times

✉  **Bouncy** 3 months ago

User2 has been filtered out by the OU2 filter already, the next filter won't even see this object. Think of it as a 2 stage filter, the second stage can only see what's left over by the first filter.  
upvoted 4 times

✉  **nsotis28** 8 months, 2 weeks ago

Answers are correct  
upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

**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

店铺：学习小店66

店铺：学习小店66

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

店铺：学习小店66

flim322 Highly Voted 8 months 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 12 times

ELQUMS Most Recent 4 months ago

Just stupid question, would be better to just ask how many days you need to register the MFA

upvoted 3 times

□  **spektrum1988** 3 months ago

Now you also have to do math.

upvoted 2 times

□  **passy951** 5 months ago

Answers are correct.

Imagine beeing bad at math during the exam :D

upvoted 3 times

□  **Vaerox** 3 months, 1 week ago

Exactly, because of this...I don't expect the question will be in the exam.

upvoted 2 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

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

店铺：学习小店66

**Correct Answer: D**

*Community vote distribution*

D (86%) 14%

✉️  **spektrum1988** 3 months ago

Answer A works if password writeback is enabled, but they don't mention it.

upvoted 1 times

✉️  **TheMCT** 3 months ago

**Selected Answer: A**

The correct answer is A. password hash synchronization. This is a sign-in method that syncs the hash of users' passwords from your on-premises Active Directory to Azure AD

upvoted 1 times

✉️  **benpatto** 5 months ago

**Selected Answer: D**

Although there is no mention of password writeback which is the main requirement for a hybrid setup, PTA (Pass through authentication) can be used to automatically enable Password writeback and allow for the cloud setup to respect the DCs enforcements. I choose you D!

upvoted 1 times

✉️  **Bouncy** 3 months ago

Correct choice, wrong explanation. A passed through password doesn't need to be written back, it's passed through to the DC already. Write back is a sync feature of AAD Connect but in a PTA scenario, passwords are not synced in the first place.

Also, writeback is not connected to password policy enforcements.

upvoted 2 times

✉️  **letters1234** 8 months, 1 week 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 3 times

✉️  **Casticod** 8 months, 1 week 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** 8 months, 1 week 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 4 times

✉️  **sergioandresiq** 6 months, 2 weeks ago

D: On-premises Active Directory password complexity policies must be enforced.  
this is PTA

upvoted 2 times

  **sergioandreslq** 5 months, 3 weeks ago

The most probably correct answer is D.

PTA is 100% enforced authentication using AD settings.

however, PHS:

When password hash synchronization is enabled, the password complexity policies in your on-premises Active Directory instance override complexity policies in the cloud for synchronized users. You can use all of the valid passwords from your on-premises Active Directory instance to access Microsoft Entra services.

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-password-hash-synchronization#password-complexity-policy>

So, PTA or PHS comply with the requirements:

Inherited from local AD: On-premises Active Directory password complexity policies must be enforced.

PTA and PHS: support password writeback.

both PTA and PHS comply with the requirements, however, I will go with answer D which is the cleanest answer as all the authentication is executed in local AD.

upvoted 3 times

  **Ranger\_DanMT** 8 months, 1 week 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 8 months, 2 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** 8 months, 2 weeks ago

I think A is correct. Because Users must use SSPR in AzureAD.

unvoted 2 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%)

店铺：学习小店66

✉️  **sherifhamed** Highly Voted 7 months, 1 week 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 6 times

✉️  **Moazzamfarooqiiii** Most Recent 2 months, 1 week ago

Chat GPT response

In this scenario, users are regularly being blocked when attempting to access Microsoft 365 via the corporate Virtual Desktop Infrastructure (VDI) solution after enabling a sign-in risk policy in Azure AD Identity Protection. To address this issue, you should consider configuring:

C. a Conditional Access policy exclusion

upvoted 1 times

✉️  **markcasera** 2 months ago

Stop posting CGPT Responses bro!

upvoted 4 times

✉️  **Amir1909** 3 months ago

B is correct

upvoted 1 times

✉️  **Paul\_white** 7 months ago

CORRECT ANSWER SHOULD BE C

upvoted 2 times

✉️  **Paul\_white** 7 months ago

NEVER MIND, ITS B. A TRUSTED LOCATION

upvoted 1 times

✉️  **certma2023** 8 months, 3 weeks 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 3 times

店铺：学习小店66

**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** *店铺：学习小店66*

**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.

*店铺：学习小店66*

If User1 enters the same wrong password 15 times, waits 11 minutes, and then enters the same wrong password again, the user [answer choice].

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

## Answer Area

[Answer choice] will be accepted as a password.



### 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].

vercracked\_007 Highly Voted 7 months, 3 weeks 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 18 times

EM1234 7 months, 1 week 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 3 times

Kmkz83510 4 months, 3 weeks ago

Agree. Given answer for Box 2 is incorrect. At the link provided, there is an explanation which says "If the first sign-in after a lockout period has expired also fails, the account locks out again. If an account locks repeatedly, the lockout duration increases."

upvoted 4 times

Kmkz83510 4 months, 2 weeks ago

Actually, I retract my statement. The given answer is correct because the account would never get locked out in the first place, due to smart lockout. The same password entered 15 times wouldn't trigger it. Box 2 would be wrong if the user entered in enough wrong passwords (not repeating) to get locked out.

upvoted 2 times

letters1234 Highly Voted 8 months, 1 week 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 password within the next 9 minutes to lock the user out.

upvoted 12 times

Kmkz83510 4 months, 3 weeks ago

Check here: <https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout> - see note regarding lockout after the first failed login following a lockout period.

upvoted 3 times

Noble00 5 months ago

You are very right.

upvoted 1 times

GeorgeMar Most Recent 3 weeks, 4 days 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.

upvoted 1 times

Vukosir 2 months, 1 week ago

All 3 passwords must be allowed , Password is different to Password22 and Falcon as well as F@lcon are not the same thing.

upvoted 1 times

TP447 5 months, 3 weeks ago

Key here is "Same wrong password" - entering the same wrong password 15 times would only be seen as 1 threshold on the counter so wouldn't trigger a lockout. Therefore the user could just attempt to sign in again.

Seems like a poorly worded question or a trick.

upvoted 4 times

ExamCheater1993 7 months, 2 weeks ago

Picture is correct. The trap is, that this person 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 6 times

 **TP447** 5 months, 3 weeks ago

Totally agree here.  
upvoted 1 times

 **SandyBridge** 7 months, 1 week 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 2 times

 **TP447** 5 months, 3 weeks ago

Totally agree here.  
upvoted 2 times

 **amurp35** 7 months, 2 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

 **gomezmax** 7 months, 4 weeks ago

1 Box Correct T4il\$pin45dg4  
The 2nd Box is incorrect it should be lockout  
upvoted 1 times

 **nsotis28** 8 months, 1 week ago

Box 1 - only T4il\$pin45dg4  
Box 2 - will be locked  
upvoted 2 times

 **hogehogehoge** 8 months, 2 weeks ago

Box1:Only F@lcon and T4il\$pin45dg4.  
Because "a" is replaced "@", and match this policy.  
upvoted 1 times

 **Romke\_en\_Tomke** 7 months, 2 weeks 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** 8 months, 3 weeks ago

If you fail again after a lockout periode, you are locked again no?  
upvoted 2 times

 **spectre786** 7 months, 4 weeks 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 (67%)

A (33%)

✉  certma2023  8 months, 3 weeks 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 6 times

✉  amurp35 7 months, 2 weeks ago

Correct, except for cloud-only users. Therefore, the correct answer is B.

upvoted 5 times

✉  MarcMouelle  3 weeks, 4 days ago

**Selected Answer: B**

L'utilisateur 1 uniquement. L'authentification directe nécessite que le réseau local soit disponible or le hachage de mot de passe crypté les mots de passe et les stocke dans l' entra id

upvoted 1 times

✉  nordbymikael 1 month, 1 week ago

**Selected Answer: B**

PTA works for synced users only. Cloud-native users always use Entra ID for authentication, even if PTA is enabled.

upvoted 2 times

✉  Tomtom11 2 months, 2 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn>

upvoted 1 times

✉  Tomtom11 2 months, 2 weeks ago

[https://www.reddit.com/r/Office365/comments/zqmfho/passthrough\\_authentication\\_and\\_password\\_hash/](https://www.reddit.com/r/Office365/comments/zqmfho/passthrough_authentication_and_password_hash/)

upvoted 1 times

□ **TP447** 5 months, 3 weeks ago

Initially i thought User1 and User2 but then realised that a change would be needed to switch to PHS. User1 being cloud only wouldnt be impacted so answer is B.

upvoted 2 times

□ **Snakad** 6 months ago

Chat GPT say only User1 because in the event of a connectivity loss between on-premises Active Directory and the internet, User1 will be able to authenticate using Azure AD because they are cloud-native and have the necessary authentication methods enabled. User2 may face authentication issues as they rely on on-premises AD DS for authentication, and User3 is not provisioned in Azure AD, so they won't be able to authenticate through Azure AD.

upvoted 1 times

□ **MoreCertificatesForMe** 7 months 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 2 times

□ **amurp35** 7 months, 2 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 4 times

□ **AMDf** 8 months ago

**Selected Answer: B**

Vote for B

upvoted 3 times

□ **ae88d96** 8 months ago

**Selected Answer: B**

Correct Answer B, Cloud User won't be affected. Tested on my lab.

upvoted 4 times

□ **Carine** 8 months 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** 8 months, 2 weeks ago

it Should be A

upvoted 1 times

□ **Greatone1** 8 months, 2 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 2 times

True, but user1 is a cloud only user, and is not dependent on Pass Through Auth/AD

upvoted 1 times

□ **nsotis28** 8 months, 2 weeks ago

For sure A

certman2023 has shared explanation

upvoted 1 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 (87%)	13%
---------	-----

店铺：学习小店66

✉️  **Casticod** Highly Voted 8 months, 2 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 hour setting configured in on-premise AD.

Other solution it's PIM but not valid in that question

upvoted 11 times

✉️  **nordbymikael** Most Recent 1 month, 1 week ago

**Selected Answer: A**

Use PTA to keep using the existent authentication restrictions. If PTA is enabled with the sync, no additional configuration in the cloud is required

upvoted 1 times

✉️  **TonyManero** 6 months, 1 week ago

PTA is correct:

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn#cloud-authentication-pass-through-authentication>  
"For example, access is denied when an on-premises user's account state is disabled, locked out, or their password expires or the logon attempt falls outside the hours when the user is allowed to sign in."

upvoted 1 times

✉️  **Alscoran** 6 months, 3 weeks 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** 7 months, 2 weeks 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** 6 months, 3 weeks ago

There is no time condition in CA. This isn't correct. Don't trust this answer.

upvoted 2 times

✉️  **ATHOOS** 5 months, 2 weeks ago

Nonsense response ...

upvoted 2 times

✉️  **Perycles** 3 months, 3 weeks ago

just checked all CA , nothing about Hours restrictions for WIndows Login .... you are talking about "Ressources access" not "Windows login .... "  
so PTA is definitively the good answer.

upvoted 1 times

⊕ **DiligentSam** 8 months, 1 week 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** 7 months, 3 weeks 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** 8 months, 2 weeks ago

I was wrong given answer is correct

upvoted 1 times

⊕ **Greatone1** 8 months, 2 weeks ago

I believe answer is b conditional access

upvoted 2 times

店铺：学习小店66

店铺：学习小店66

Question #93

Topic 1

Your network contains three Active Directory forests. There are forest 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**

*Community vote distribution*

A (100%)

⊕ **nordbymikael** 1 month, 1 week ago

**Selected Answer: A**

"Microsoft Entra Connect supports syncing from multiple forests. It supports only one instance of Microsoft Entra Connect syncing to Microsoft Entra ID. In cases where Microsoft Entra ID is already installed in one forest, the existing instance of Microsoft Entra Connect must be updated to sync from the other forest."

<https://learn.microsoft.com/en-us/skypeforbusiness/hybrid/cloud-consolidation-aad-connect>

upvoted 2 times

⊕ **Shuihe** 6 months ago

A

When you have multiple forests, all forests must be reachable by a single Azure AD Connect sync server. The server must be joined to a domain. If necessary to reach all forests, you can place the server in a perimeter network.

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/plan-connect-topologies#multiple-forests-single-azure-ad-tenant>

upvoted 1 times

⊕ **nsotis28** 8 months, 2 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 4 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 (79%)

E (21%)

✉  amurp35  7 months, 2 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 8 times

✉  gbartumeu  7 months, 3 weeks 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 5 times

✉  KerrAvon  2 months, 2 weeks ago

**Selected Answer: D**

After 1 year the file would be deleted if not modified. Since it was modified the retention period takes precedence. However it is still flagged for deletion so once the retention period is up it will then be deleted.

upvoted 2 times

✉  Amir1909 2 months, 4 weeks ago

E is correct

upvoted 1 times

✉  365cm 5 months ago

E- I believe because as others have noted....retention wins over deletion.

upvoted 1 times

365cm 5 months ago

Nvm...Correct Answer is D

upvoted 1 times

Festus365 5 months ago

Answer is A. January 1 2023. The question is concerned exactly will the file be deleted not modified which it will take 1 year retention period and the deletion took place automatically according to the information in the table

upvoted 1 times

Festus365 3 months, 3 weeks ago

Answer is correct D! January 31, 2024

upvoted 2 times

Alscoran 6 months, 3 weeks ago

**Selected Answer: D**

Gbartumeu provides the perfect example. Just look at his article and do a find for "suspended". Second hit.

upvoted 4 times

ZZNZ 7 months ago

**Selected Answer: E**

E is correct answer: Retention wins over deletion

upvoted 1 times

BlindSentry 7 months 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 4 times

DiligentSam 6 months, 4 weeks 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 2 times

Blagojche 7 months, 1 week 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 2 times

smiff 7 months, 1 week 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 3 times

vercracked\_007 7 months, 3 weeks 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 8 months, 1 week 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 policies change, it would not be deleted.

upvoted 2 times

✉  **hogehogehoge** 8 months, 2 weeks ago

**Selected Answer: D**

I think D is correct. Please check this URL. <https://learn.microsoft.com/en-us/purview/retention?tabs=table-overriden>

upvoted 4 times

✉  **Vaati** 8 months, 3 weeks ago

Could someone explain? im thinking E

upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

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 (89%)

5%

✉️  **amurp35** Highly Voted 7 months, 2 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 15 times

✉️  **sergioandreslq** 6 months, 2 weeks ago

This is correct, I tested. the key of this question is to which kind of resource you can scope the sensitivity label.

it is totally different to use a sensitivity label to PROTECT an MS365 group.

the key of this question is to which kind of resource we can scope users for the sensitivity label.

upvoted 1 times

✉️  **9711d59** Most Recent 3 months, 1 week ago

**Selected Answer: D**

This is good answer. I have tested it

upvoted 2 times

✉️  **cpaljhc4** 4 months, 1 week ago

What label policies can do

After you create your sensitivity labels, you need to publish them to make them available to people and services in your organization. The sensitivity labels can then be applied to Office documents and emails, and other items that support sensitivity labels.

Unlike retention labels, which are published to locations such as all Exchange mailboxes, sensitivity labels are published to users or groups. Apps that support sensitivity labels can then display them to those users and groups as applied labels, or as labels that they can apply.

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 Microsoft Entra ID."

Double checked and quoted this.

<https://learn.microsoft.com/en-us/purview/sensitivity-labels#what-label-policies-can-do>

upvoted 1 times

✉️  **Dannith** 5 months ago

**Selected Answer: A**

A lot of people in this thread seem to think otherwise, but according to <https://learn.microsoft.com/en-us/entra/identity/users/groups-assign-sensitivity-labels>, Sensitivity labels can only be applied to M365 groups. See the troubleshooting section...

"The sensitivity label option is only displayed for groups when all of the following conditions are met...

6. The group is a Microsoft 365 group.

upvoted 1 times

✉ **mhmyz** 7 months, 2 weeks 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

✉ **sergioandreslq** 6 months, 2 weeks ago

No, Regular security groups can be selected when you try to define the scope of the label policy.

Microsoft 365 Groups, SharePoint sites, Distribution Groups, and Mail-enabled Security Groups

upvoted 1 times

✉ **RJTW070** 7 months, 3 weeks 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<sup>1</sup>. 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<sup>1</sup>.

upvoted 2 times

✉ **rfree** 7 months, 3 weeks 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** 8 months, 1 week 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 3 times

✉ **gomezmax** 8 months, 1 week ago

(A) it is Correct only applied into the Email

upvoted 1 times

✉ **sergioandreslq** 6 months, 2 weeks ago

Nop, A will be the answer if you are planning to protect a MS365 group, but this question is to which kind of resource you can choose when you are defining the scope of the label policy.

the correct answer is D, I tested in my label policy.

upvoted 1 times

✉ **gomezmax** 8 months, 1 week ago

Correct

upvoted 1 times

✉ **Greatone1** 8 months, 2 weeks ago

Correct answer is D

upvoted 1 times

✉ **certma2023** 8 months, 3 weeks 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."<sup>66</sup>

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

upvoted 2 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

Correct Answer:

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

hoge hogehoge Highly Voted 8 months, 2 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 40 times

f09257a Most Recent 2 months, 2 weeks ago

Rule 1 for both, when multiple rules matches, the rule with the higher priority is enabled.

upvoted 1 times

9711d59 3 months, 1 week ago

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:

Rule 1: only notifies users

Rule 2: notifies users, restricts access, and allows user overrides

Rule 3: notifies users, restricts access, and doesn't allow user overrides

Rule 4: restricts access

upvoted 2 times

KairKnows 5 months ago

Hoge is correct.

"Only the policy tip from the highest priority, most restrictive 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."

upvoted 2 times

NrdAlert 5 months, 3 weeks ago

Tips follow rules applied and are not cumulative as that would be confusing. DLP rules are applied as one with most restrictive actions over priority unless the policies are the same in terms of restrictions. File 1 : Rule 2 only, File 2 : Rule 4 only

upvoted 1 times

rfree 6 months, 2 weeks ago

Correction, Rule 2 then Rule 4 as each is the Most Restrictive.

upvoted 1 times

rfree 6 months, 2 weeks ago

Confusing, now thinking Rule 2, then Rule 3.

It's possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). 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.

<https://learn.microsoft.com/en-us/purview/use-notifications-and-policy-tips>

upvoted 1 times

rfree 7 months, 1 week ago

As its not asking which rules are applied, but which rules are Shown.

upvoted 1 times

rfree 7 months, 1 week 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 7 months, 2 weeks ago

Question #97

Topic 1

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 Highly Voted 8 months, 2 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 8 times

TheMCT Most Recent 3 months ago

**Selected Answer: D**

User Overrides

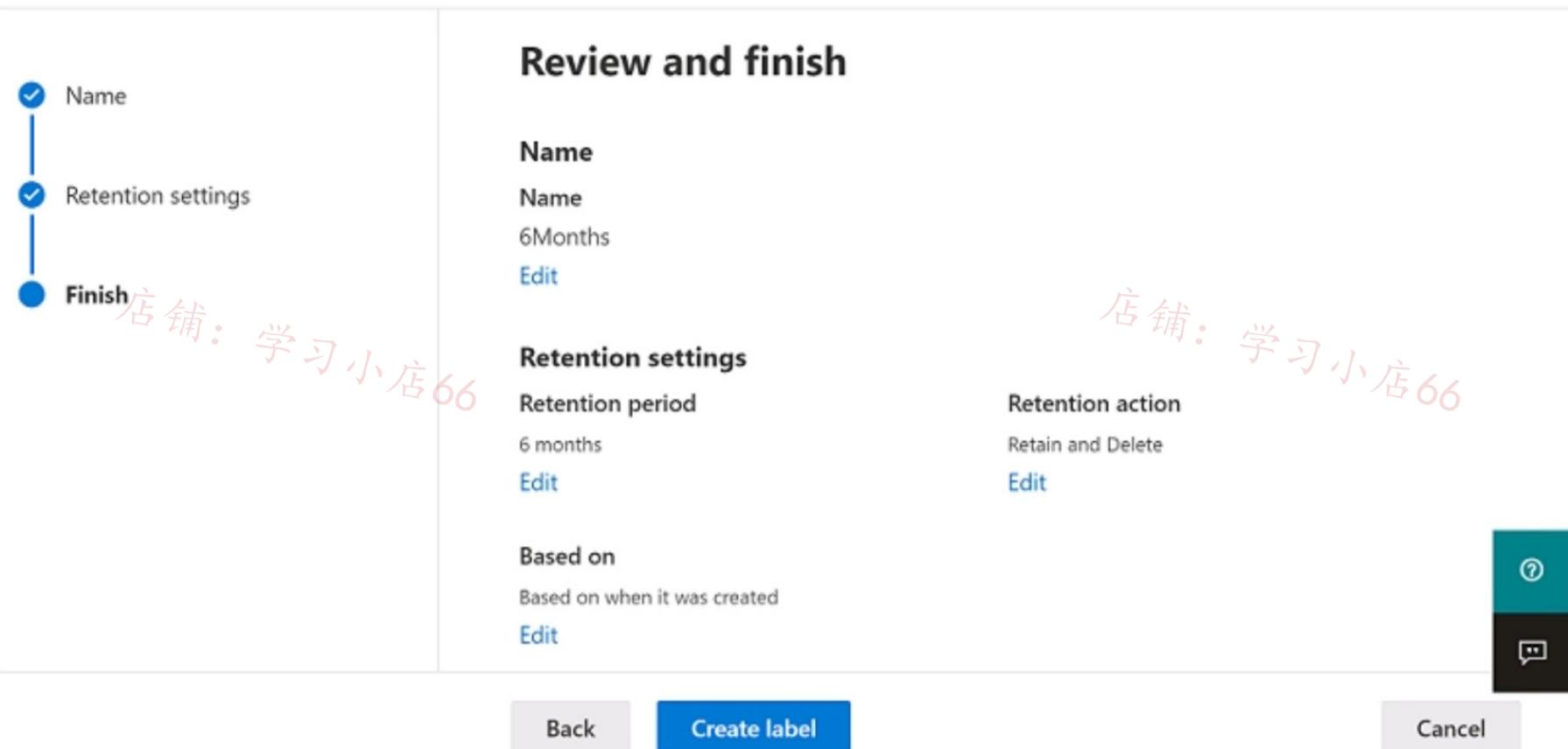
<https://techcommunity.microsoft.com/t5/security-compliance-and-identity/overrides-and-false-positives-in-dlp-policy-end-user-experience/mp/202790>

upvoted 1 times

You have a Microsoft 365 E5 tenant.

You create a retention label named Retention1 as shown in the following exhibit.

## Create retention label



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 Highly Voted 7 months ago

**Selected Answer: A**

wrong image : <https://www.examtopics.com/discussions/microsoft/view/65184-exam-ms-101-topic-3-question-105-discussion/>  
upvoted 9 times

✉️ spectre786 Most Recent 8 months 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 8 months, 1 week 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 4 times

✉️ Greatone1 8 months, 2 weeks ago

**Selected Answer: A**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide>  
upvoted 1 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

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](#)

[+ Create a label](#) [Publish labels](#) [Refresh](#)

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** Highly Voted 7 months, 2 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 11 times

✉  **sergioandresiq** 6 months, 2 weeks ago

100% agreed, I have parent label and sub-labels, I can only apply the sub-labels to the content.  
upvoted 2 times

✉  **letters1234** Highly Voted 8 months, 1 week ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/purview/sensitivity-labels#sublabels-grouping-labels>  
upvoted 5 times

✉  **nordbymikael** Most Recent 1 month, 1 week ago

**Selected Answer: C**

Parent labels cannot be applied if they have child labels  
upvoted 2 times

✉  **Tomtom11** 2 months, 2 weeks ago

Sublabels (grouping labels)

With sublabels, you can group one or more labels below a parent label that a user sees in an Office app. For example, under Confidential, your organization might use several different labels for specific types of that sensitivity. In this example, the parent label Confidential is simply a text label with no protection settings, and because it has sublabels, it can't be applied to content. Instead, users must choose Confidential to view the sublabels, and then they can choose a sublabel to apply to content.

Sublabels are simply a way to present labels to users in logical groups. Sublabels don't inherit any settings from their parent label, except for the label color. When you publish a sublabel for a user, that user can then apply that sublabel to content and containers, but can't apply just the parent label

upvoted 1 times

□  **cyp99** 4 months, 4 weeks ago

**Selected Answer: C**

Agree with amurp35. Parent labels cannot be used by user  
upvoted 2 times

□  **[Removed]** 6 months, 2 weeks ago

The AZ-103 certification exam needs extra attention and knowledge to get through it. But Dumps4azure made it a piece of cake for me! Dumps4azure Study Guide really helped to gain excellent and detailed knowledge of the domain in very short time  
upvoted 1 times

□  **gomezmax** 8 months, 2 weeks ago

Should be C. Label1, Label3, Label4, and Label6 only  
upvoted 3 times

□  **f7d3be6** 8 months, 2 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** 8 months, 2 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 3 times

□  **hogehogehoge** 8 months, 2 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 5 times

店铺：学习小店66

店铺：学习小店66

**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

**Correct Answer:**

Office file types that support the sensitivity labels:

- Microsoft 365 Apps for enterprise and Office for the web only

- .doc only
- .docx only
- .xls only
- .xlsx only
- .doc and .xls
- .docx and .xlsx
- .doc, .docx, .xls, and .xlsx

 **northgaterebel**  6 months, 1 week ago

Office 2016 and Office 2019 only

.doc, .docx, .xls, and .xlsx

upvoted 10 times

 **ShlomiR** 6 months, 1 week ago

<https://learn.microsoft.com/en-us/purview/sensitivity-labels-office-apps#office-file-types-supported>

second answer only docx and xlsx,

upvoted 17 times

daye 5 months ago

exactly, the article explains:

Generally, Office apps that have built-in labeling for Word, Excel, and PowerPoint files support the Open XML format (such as .docx and .xlsx) but not the Microsoft Office 97-2003 format (such as .doc and .xls),

upvoted 3 times

letters1234 Highly Voted 8 months, 1 week 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/b-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 8 times

RJTW070 7 months, 3 weeks 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 Office1. The add-in component that is required for these editions is the Azure Information Protection (AIP) unified labeling client2. However, this add-in is now in maintenance mode and will be retired in April 20242. Therefore, it is recommended to move to built-in labeling for Office apps if possible

upvoted 3 times

RJTW070 7 months, 3 weeks ago

So I will go for Office 2016 and 2019 the second answer is correct

upvoted 5 times

Milad66 7 months 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 3 times

tome 5 months, 3 weeks ago

2nd answer is not correct. The question is about sensitivity labels not about labeling client.

See this. - <https://learn.microsoft.com/en-us/purview/sensitivity-labels-office-apps#office-file-types-supported>

"Generally, Office apps that have built-in labeling for Word, Excel, and PowerPoint files support the Open XML format (such as .docx and .xlsx) but not the Microsoft Office 97-2003 format (such as .doc and .xls), Open Document Format (such as .odt and .ods), or other formats. When a file type is not supported for built-in labeling, the Sensitivity button is not available in the Office app."

upvoted 1 times

tome 5 months, 3 weeks ago

\*is correct, sry!

upvoted 1 times

Tomtom11 Most Recent 2 months, 2 weeks ago

<https://learn.microsoft.com/en-us/information-protection/develop/concept-supported-filetypes>

<https://learn.microsoft.com/en-us/purview/sensitivity-labels-office-apps>

upvoted 1 times

Greatone1 8 months, 2 weeks 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.)

店铺：学习小店66

**Create retention label**

- Name
- Retention settings
- Finish

**Review and finish****Name**

Name  
6Months  
[Edit](#)

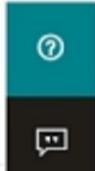
**Retention settings**

Retention period  
6 months  
[Edit](#)

Retention action  
Retain and Delete  
[Edit](#)

**Based on**

Based on when it was created  
[Edit](#)

[Back](#)[Create label](#)[Cancel](#)

You create a label policy as shown in the Label Policy exhibit. (Click the Label Policy tab.)

店铺：学习小店66

店铺：学习小店66

- Name
- Info to label
- Create content query
- Scope
- Label
- Finish

## Apply label to content matching this query

Conditions

ProjectX

+ Add condition ▾

?
...

Back
Next
Cancel

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                                                                                     | <b>Yes</b>            | <b>No</b>             |
|------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| 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                                                                                     | <b>Yes</b>                       | <b>No</b>                        |
|------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| 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] 7 months, 4 weeks ago

Should be N/Y/N

upvoted 19 times

✉ momowagdy 3 weeks, 3 days ago

It is actually N, Y, N

Maybe they have updated the answer

upvoted 3 times

✉ nordbymikael [Most Recent] 1 month, 1 week ago

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**  7 months, 1 week 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 8 times

✉  **Tomtom11**  2 months, 2 weeks ago

**Selected Answer:** C

<https://learn.microsoft.com/en-us/purview/sit-create-a-custom-sensitive-information-type>  
upvoted 2 times

✉  **RJTW070** 7 months, 3 weeks 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** 8 months, 2 weeks ago

Answer is correct

<https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide>

upvoted 2 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 (96%)	4%
---------	----

✉  **gbartumeu** Highly Voted 7 months, 3 weeks 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 should be "Regulatory Record".

upvoted 10 times

✉  **Motanel** Most Recent 3 weeks, 4 days ago

I am starting to believe that these provided answers are simply aleatory without checking any if it's correct or not.

upvoted 1 times

✉  **nordbymikael** 1 month, 1 week ago

**Selected Answer: B**

A regulatory record can never be deleted

upvoted 3 times

✉  **Tomtom11** 2 months, 2 weeks ago

**Selected Answer: B**

Important

The most important difference for a regulatory record is that after it is applied to content, nobody, not even a global administrator, can remove the label.

Retention labels configured for regulatory records also have the following admin restrictions:

The retention period can't be made shorter after the label is saved, only extended.

These labels aren't supported by auto-labeling policies, and must be applied by using retention label policies.

In addition, a regulatory label can't be applied to a document that's checked out in SharePoint.

Because of the restrictions and irreversible actions, make sure you really do need to use regulatory records before you select this option for your retention labels. To help prevent accidental configuration, this option is not available by default but must first be enabled by using PowerShell. Instructions are included in Declare records by using retention labels.

upvoted 2 times

✉  **Alex\_T77** 6 months, 1 week ago

<https://learn.microsoft.com/en-us/purview/records-management#compare-restrictions-for-what-actions-are-allowed-or-blocked>

upvoted 1 times

✉  **jt2214** 7 months, 1 week ago

**Selected Answer: B**

B all the way

upvoted 2 times

✉  **Jslei** 7 months, 3 weeks 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 2 times

✉  **letters1234** 8 months, 1 week 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 4 times

✉  **Greatone1** 8 months, 2 weeks ago

**Selected Answer: B**

Sorry I meant B

upvoted 4 times

✉  **Greatone1** 8 months, 2 weeks ago 66

**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

**HOTSPOT -**

You configure a data loss prevention (DLP) policy named DLP1 with a rule configured as shown in the following exhibit.

**Create rule****Conditions**

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

**Content contains**

Default Any of these

**Sensitive info types**

Credit Card Number High confidence Instance count 1 to Any

**Retention labels**

RetentionLabel1

Add Create group

+ Add condition

店铺：学习小店66

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**

DLP1 cannot be applied to [answer choice].

- Exchange email
- SharePoint sites
- OneDrive accounts

DLP1 will be applied only to documents that have [answer choice].

both a credit card number and the RetentionLabel1 label applied  
either a credit card number or the RetentionLabel1 label applied  
between 85 and 100 credit card numbers

**Answer Area**

DLP1 cannot be applied to [answer choice].

- Exchange email
- SharePoint sites
- OneDrive accounts

**Correct Answer:**

DLP1 will be applied only to documents that have [answer choice].

both a credit card number and the RetentionLabel1 label applied  
either a credit card number or the RetentionLabel1 label applied  
between 85 and 100 credit card numbers

✉ **hogehogehoge** Highly Voted 8 months, 2 weeks ago

Box1: Exchange email. I tested this configuration in my lab.

Box2: either a credit card number or the RetentionLabel1 label applied.

upvoted 27 times

店铺：学习小店66

✉ **sergioandresiq** 6 months, 1 week ago

Thanks for testing, I did the same thing and confirm the error message:

Retention labels are not supported in policy configured with Exchange workload.

upvoted 1 times

✉ **daye** 5 months, 1 week ago

Indeed, here you can find all the conditions you may set depending on the location

<https://learn.microsoft.com/en-us/purview/dlp-policy-reference#location-support-for-how-content-can-be-defined>

upvoted 3 times

✉ **Greatone1** Highly Voted 8 months, 1 week ago

Box1: Correct the policy cannot be applied to Exchange

Box2: either a credit card number or the RetentionLabel1 label will be applied

upvoted 11 times

✉️ **Shadowcatest** (Most Recent) 6 months, 3 weeks ago

Agree with hoge

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

Location Content can be defined by SIT, Content can be defined sensitivity label, Content can be defined by retention label  
Exchange email online Yes Yes No

SharePoint in Microsoft 365 sites Yes Yes Yes

OneDrive for work or school accounts Yes Yes Yes

Box1:Exchange email.

Box2:ether a credit card number or the Retention label1 label applied

upvoted 4 times

✉️ **letters1234** 8 months, 1 week 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%)

曰  nordbymikael 1 month, 1 week ago

**Selected Answer: B**

Not a permission issue. The user does not log in with a valid domain in the tenant.

upvoted 2 times

曰  Greatone1 8 months, 1 week 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 4 times

曰  Greatone1 8 months, 2 weeks ago

**Selected Answer: B**

Correct answer should be no

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 SharePoint Administrator role.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉  **nordbymikael** 1 month, 1 week ago

**Selected Answer: B**

Does not meet all the requirements.

upvoted 2 times

✉  **60ed5c2** 6 months, 1 week ago

someone commented this on another question but I'll say it here as well.....why can't they all be this straight forward?

upvoted 1 times

✉  **NrdAlert** 5 months, 3 weeks ago

yeah. I spend more time on this question looking for what weird detail I missed because it's too easy.

upvoted 1 times

✉  **Shadowcatest** 6 months, 3 weeks 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** 7 months, 2 weeks 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*

A (83%)

B (17%)

✉ aleksdij Highly Voted 5 months ago

**Selected Answer: A**

The question is misunderstood and therefore 50% are wrong! Correct Answer is YES

You should read the question like this:

"You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies WHICH APPLY TO Microsoft Teams, SharePoint, and OneDrive"

It doesn't say you have to be able to manage Teams, SP or Onedrive with an Security Administrator role, the clue is that the settings and policies are made within the Defender Portal.

upvoted 16 times

✉ tzzz1986 Highly Voted 7 months, 2 weeks 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 8 times

✉ sergioandresiq 6 months, 1 week ago

Security administrator grant access to defender portan and configure policies.

but this role doesn't grant permission as admin to Teams, SPO and OneDrive.

upvoted 1 times

✉ sergioandresiq 5 months, 3 weeks ago

and the requirement is: "SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies"

In this case with this role, the user can manage defender policies for those workloads, the security administrator has access to settings associated to security in different workloads.

there are other questions that assign to the SecAdmin1 roles: sharepoint admin, Teams admin, Exchange Admin.

However, the only role that can manage security settings for all the workloads at the same time is Security administrator.

the other roles assigned are for specific workload, however, the question is what is the role that can manager Teams, Sharepoint, And OneDrive at the same time?

upvoted 5 times

✉ Alscoran 6 months, 3 weeks 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 7 times

✉ AlfaExamPro 6 months ago

He is correct.

Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide>  
upvoted 1 times

□ **nordbymikael** Most Recent 1 month, 1 week ago

**Selected Answer: A**

I believe that A is the right answer. The question is spelled a bit wrong.  
upvoted 2 times

□ **TheMCT** 3 months ago

**Selected Answer: A**

Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.  
upvoted 2 times

□ **BLion** 5 months ago

**Selected Answer: A**

Answer A is correct  
upvoted 3 times

□ **Memdroid** 5 months ago

**Selected Answer: A**

A is correct  
upvoted 2 times

□ **2dwarf** 5 months, 1 week ago

**Selected Answer: A**

A Can manage policies  
upvoted 2 times

□ **ckanoz** 5 months, 2 weeks ago

Correct answer is A. The question is not asking if the role has permissions to administer Teams, Sharepoint or Exchange. The question is asking if the role can make Security policies FOR Teams, Sharepoint or Exchange.  
upvoted 2 times

□ **TP447** 5 months, 3 weeks ago

This is correct - the question isn't asking about managing Teams, SPO etc directly but in fact, managing Defender settings & policies for those workloads - "You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for".

Security Administrator would have the rights to create and manage policies for these workloads.

upvoted 3 times

□ **NrdAlert** 5 months, 3 weeks ago

**Selected Answer: A**

Pretty specific that they say Microsoft Defender Policies, not managing the services themselves. Additionally, I find it unfathomable that a SecOps admin would need full admin access to all these services to manage the security portion. I can see myself as an O365 admin saying to a guy on security team: "Here, I know you're a security guy that is already skeptical of Microsoft as it is, but I have to give you full unfettered access to the service configuration layer just so you can manage defender settings for these workloads. That's cool right?" No way. It's A or Microsoft has lost their mind.

upvoted 4 times

□ **TP447** 5 months, 3 weeks ago

I agree here.

upvoted 1 times

□ **NrdAlert** 5 months, 3 weeks ago

Or perhaps... possibly more like... there's a 3rd answer here. Like reader something or another. But that doesn't make sense either. Again that's way too convoluted, even for MS, to make sense.

upvoted 1 times

□ **60ed5c2** 6 months, 1 week ago

If I am following the comments correctly - people are saying A because the question is asking if the security administrator role gives you the ability to set policies within defender for Teams, SP, and OneDrive and because a security administrator role has full access to defender - the answer would be yes.

My counter point is there are not policies specifically for Teams, Sharepoint, or Onedrive within Defender. So how could the question mean that?

My answer would be B - No - security administrator gives you the ability to manage Defender, but it does not give you the ability to manage policies for Teams, SP, and OD.

upvoted 1 times

□ **EEMS700** 6 months, 2 weeks ago

**Selected Answer: A**

For me it's A

upvoted 2 times

PhoenixMan 6 months, 2 weeks 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 6 months, 3 weeks ago

**Selected Answer: A**

I agree with Darekmso based on

<https://www.examtopics.com/discussions/microsoft/view/76446-exam-ms-101-topic-2-question-50-discussion/>

upvoted 3 times

Darekmso 6 months, 3 weeks 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 7 months ago

ANSWER FOR ME IS A

upvoted 2 times

Greatone1 8 months, 1 week ago

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide>

upvoted 2 times

Question #108

Topic 1

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**

*Community vote distribution*

B (100%)

nordbymikael 1 month, 1 week ago

**Selected Answer: B**

Does not meet all the requirements.

upvoted 2 times

DiligentSam 7 months, 2 weeks ago

I think the answer is No

Because you are just assigned a Exchange Online Admin Role.

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.

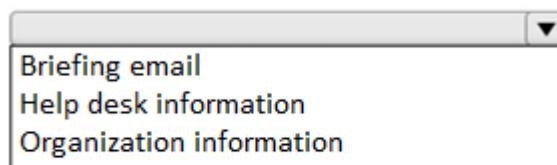
You need to configure the Office 365 service status notifications and limit access to the service and feature updates. The solution must meet the technical requirements.

What should you configure in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.

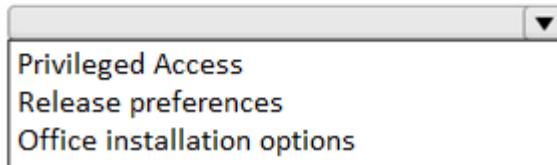
NOTE: Each correct selection is worth one point.

#### Answer Area

To configure the notifications:



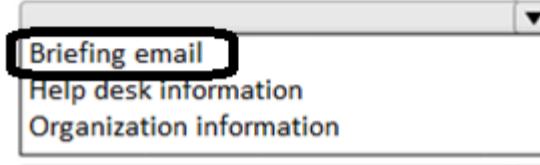
To limit access:



店铺: 学习小店

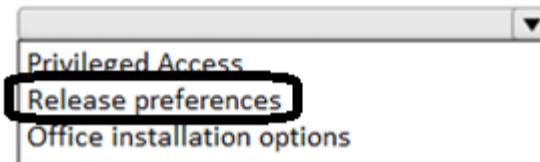
Answer Area

To configue the notifications:



Correct Answer:

To limit access:



店铺: 学习小店66

□ **Casticod** Highly Voted 8 months 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 16 times

□ **lali11** 4 months ago

Shouldn't this be helpdesk information?

upvoted 1 times

□ **lali11** 4 months ago

pls ignore.

upvoted 1 times

□ **lali11** Most Recent 4 months ago

1st answer: Organization information

<https://o365info.com/help-desk-information-microsoft-365/>

upvoted 2 times

□ **NrdAlrt** 5 months, 3 weeks ago

I too think the first answer is wrong. Org info is what you want. Googling Briefing email is Viva insights. Not even related.

upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

### 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** Highly Voted 8 months ago

**Selected Answer: C**

Correct <https://www.examtopics.com/discussions/microsoft/view/89165-exam-ms-100-topic-13-question-2-discussion/>  
upvoted 5 times

**nordbymikael** Most Recent 1 month, 1 week ago

**Selected Answer: C**

C should be correct, because there you can enable OU filtering.  
upvoted 2 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

**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%)

Casticod Highly Voted 8 months ago

**Selected Answer: C**

Not necessary Cname record to add Email Only TXT or 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 12 times

Motanel Most Recent 3 weeks, 4 days ago

**Selected Answer: C**

Obviously C.

upvoted 1 times

nordbymikael 1 month, 1 week ago

**Selected Answer: C**

TXT is the required DNS record for domain ownership validation.

upvoted 3 times

✉  **spektrum1988** 3 months ago

**Selected Answer: C**

TXT is correct

upvoted 3 times

✉  **cyp99** 4 months, 4 weeks ago

**Selected Answer: C**

TXT or MX for domain add/validation

upvoted 3 times

✉  **passy951** 5 months ago

**Selected Answer: C**

CNAME is for Autodiscover

upvoted 2 times

✉  **EEMS700** 6 months, 2 weeks ago

**Selected Answer: C**

You can add a domain only with TXT or MX.

So it's C

upvoted 3 times

✉  **AMDF** 8 months ago

**Selected Answer: C**

Vote for C

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**

*Community vote distribution*

B (100%)

✉️  **nordbymikael** 1 month, 1 week ago

**Selected Answer: B**

Security Administrator is required.

upvoted 3 times

✉️  **TonyManero** 4 months ago

**Selected Answer: B**

Needs Serurity Admin Role

upvoted 2 times

✉️  **daye** 5 months, 1 week ago

**Selected Answer: B**

Similar questions asking about assigning Teams, Sharepoint or Exchange admin. Always NO. It shoud be Security Admin since it will used witin Security Admin Center.

upvoted 2 times

**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:	<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 Highly Voted 7 months ago

Answers are correct

<https://www.examtopics.com/discussions/microsoft/view/49675-exam-ms-100-topic-3-question-37-discussion/>  
upvoted 9 times

nordbymikael Most Recent 1 month, 1 week ago

User10 is an on-prem user and can therefore manage all the passwords of the synced users an on-prem only users. Synced users credentials have to be managed on-premises because password writeback is turned off.

User20 is cloud-native and can only manage passwords of another cloud-native users.

upvoted 1 times

spektrum1988 3 months ago

Even if password writeback would be enabled. A password reset by the admin does not writeback to on-premise. Only password resets by the user itself. I have tested this thoroughly before.

upvoted 2 times

9711d59 3 months, 1 week ago

Unfortunately, you cannot reset this user's password because password writeback is not enabled in your tenant. Correct.

upvoted 1 times

EEMS700 6 months, 2 weeks ago

correct

upvoted 4 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:

店铺: 学习小店66

- Group1 only
- Group3 only
- Group1, and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

AMDf Highly Voted 8 months ago

1) Group 1, Group 2 and Group 3

2) Group 3 only

upvoted 45 times

EEMS700 6 months, 2 weeks ago

i would agree with AMDf

upvoted 1 times

⊕  **cyp99** 4 months, 4 weeks ago

agree as G4 is dynamic and G5 synced from onprem  
upvoted 1 times

⊕  **BigTone** Most Recent 5 months, 1 week ago

Security enabling a M365 group means you can share an app with the group, all M365 groups are created security disabled by default

<https://learn.microsoft.com/en-us/power-apps/maker/canvas-apps/share-app#share-an-app-with-microsoft-365-groups>

upvoted 1 times

⊕  **Festus365** 5 months, 2 weeks ago

- 1) You can add Azure AD cloud user to Group 1, 3, 4 only but group 2 is not security enabled
- 2) You can add group 5 to the Group 3 only

upvoted 2 times

⊕  **ckanoz** 5 months, 2 weeks ago

Group 4 is a Dynamic Group. You can not add any users or groups to it manually.  
店铺: 学习小店66

upvoted 4 times

⊕  **Festus365** 3 months, 3 weeks ago

Answers are correct!(1)Group 1 & 3 only  
(2) Group 3 only  
店铺: 学习小店66

upvoted 1 times

⊕  **NrdAlert** 5 months, 3 weeks ago

What does Group 2 not being security enabled mean though? Implications?

upvoted 2 times

⊕  **daye** 5 months, 1 week ago

you can assign Entra roles there. This attribute can be enabled if you create the group from Entra instead of M365 admin.  
店铺: 学习小店66

upvoted 2 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**

*Community vote distribution*

B (90%) 7%

✉  **gbartumeu** Highly Voted 7 months, 3 weeks 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 9 times

✉  **Fran22** Most Recent 2 months ago

I just checked. You can apply License to group from the License blade in Ms.365 Admin Center

upvoted 1 times

✉  **9711d59** 3 months, 1 week ago

**Selected Answer: A**

You can apply License to group with License blade in Admin 365

upvoted 2 times

✉  **Motanel** 3 weeks, 4 days ago

yes, but it's not done automatically. You need to manually add the groups.

upvoted 1 times

✉  **PhoenixMan** 5 months, 2 weeks ago

In today exam

upvoted 2 times

✉  **EEMS700** 6 months, 2 weeks ago

**Selected Answer: B**

Only B

upvoted 2 times

✉  **Paul\_white** 7 months ago

CORRECT ANSWER IS B WITHOUT A DOUBT

upvoted 3 times

✉  **sherifhamed** 7 months ago

**Selected Answer: B**

<https://www.examtopics.com/discussions/microsoft/view/48720-exam-ms-100-topic-3-question-83-discussion/>

upvoted 4 times

✉  **sherifhamed** 7 months, 1 week 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

✉  **NrdAlert** 5 months, 3 weeks ago

Which means your answer should be B, lol

upvoted 6 times

✉  **jt2214** 7 months, 3 weeks ago

**Selected Answer: B**

Should be B

upvoted 3 times

✉  **Master\_Tx** 7 months, 3 weeks ago

Should be done from Azure / Entra as best practice on dynamic assignment.

upvoted 2 times

✉  **AMDf** 8 months ago

**Selected Answer: B**

Vote for B

upvoted 4 times

✉  **Casticod** 8 months 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 4 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

店铺：学习小店66

**Correct Answer: D**

*Community vote distribution*

D (79%)      B (21%)

✉ **cb0900** Highly Voted 7 months, 3 weeks 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 17 times

✉ **daye** 5 months, 3 weeks ago

tricky question because based on this article you need to use a security group, but indeed you can select a M365 group (but It won't work)

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/role-based-access-control#role-assignments>  
upvoted 1 times

✉ **daye** 5 months, 3 weeks ago

So I will use B because you need to apply the role successfully  
upvoted 1 times

✉ **Darekms0** Highly Voted 6 months, 3 weeks ago

**Selected Answer: D**

Checked : From endpoint manager > tenant admin > roles > open "endpoint security manager" > assignments > .... you can choose M365, security & mail-enabled group  
upvoted 7 times

✉ **rass1981** 3 months, 3 weeks ago

I did the same and can confirm all options in D can be chosen.  
upvoted 1 times

✉ **nordbymikael** Most Recent 1 month, 1 week ago

**Selected Answer: D**

D should be the correct answer.  
It is possible to assign roles to Microsoft 365 groups.  
For both security groups and mail-enabled security groups, you can assign roles to the group only if you enabled an option for RBAC role support when you created the group.  
upvoted 2 times

✉ **Shuihe** 5 months, 1 week ago

D  
<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept>  
upvoted 1 times

✉ **Christianbrivio1991** 5 months, 2 weeks ago

dovrebbe essere la B  
<https://learn.microsoft.com/it-it/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>  
upvoted 1 times

✉ **Christianbrivio1991** 5 months ago

Sorry, the correct answer is C

店铺：学习小店66

upvoted 1 times

✉️ **TP447** 5 months, 3 weeks ago

Correct answer is C for me - Mail Enabled Security and Security Group types can both be used for delegation here.

upvoted 1 times

✉️ **sergioandreslq** 6 months, 1 week ago

I tested in my tenant from Intune to assign this role, I was able only to choose: mail-enabled security and security only.

When I tried MS365 or Distribution group, there is not any option to choose.

So, I will choose option C.

upvoted 4 times

✉️ **Darekms0** 6 months, 3 weeks 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 2 times

店铺: 学习小店66

✉️ **Darekms0** 6 months, 3 weeks ago

Update it should be D -> From endpoint manager > tenant admin > roles > open "endpoint security manager" > assignments > .... you can choose M365, security & mail-enabled group

upvoted 2 times

✉️ **MarkusSan** 6 months, 3 weeks ago

**Selected Answer: D**

<https://www.examtopics.com/discussions/microsoft/view/80188-exam-ms-100-topic-5-question-64-discussion/>

upvoted 4 times

✉️ **RJTW070** 7 months, 3 weeks 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 Manager<sup>1</sup>. You can create a role-assignable group by using the Azure portal, PowerShell, or Microsoft Graph<sup>2</sup>.

upvoted 2 times

✉️ **ae88d96** 8 months 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

✉️ **ThomasMcThomasface** 6 months ago

Yes, you SHOULD use a security group. But you CAN use the other groups apart from distribution. The question is what you can use. I go with D

upvoted 2 times

✉️ **NrdAlert** 5 months, 3 weeks ago

Ex-actly.

upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

## 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 type="radio"/>	<input checked="" type="checkbox"/>

Correct Answer:

Casticod 8 months 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 argument 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 45 times

CloudCanary 7 months, 2 weeks ago

Definitely N,N,Y, I agree 100%  
upvoted 6 times

cb0900 7 months, 3 weeks ago

Agree.

NO

NO

YES

upvoted 5 times

□ **daye** 5 months, 3 weeks ago

good catch

upvoted 1 times

□ **nordbymikael** [Most Recent ⓘ] 1 month, 1 week ago

1: No

2: No

3: Yes

No users are added to the administrative unit AU1. Therefore, Admin1 who has a role scoped to AU1 cannot make any changes on the users, because there are simply no users.

Global Administrator on the tenant scope has almost all rights in the whole tenant.

upvoted 2 times

□ **cyp99** 4 months, 3 weeks ago

I believe NNY

upvoted 2 times

□ **TP447** 5 months, 3 weeks ago

N/N/Y for me.

upvoted 2 times

□ **PhoenixMan** 6 months, 2 weeks ago

the answer should be N,N,Y

upvoted 4 times

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**

*Community vote distribution*

D (100%)

✉  **nordbymikael** 1 month, 1 week ago

**Selected Answer: D**

Should be D because you do not achieve anything without actually configuring the service outage actions outside the service health menu.  
upvoted 2 times

✉  **Greatone1** 6 months, 2 weeks ago

From Microsoft 365 Admin Center go to :  
Health / Service Health. Click on Customize and select the Email tab.  
Tick "Send me service health notifications in email", specify email address  
upvoted 2 times

✉  **Greatone1** 7 months ago

Correct answer is D  
upvoted 1 times

✉  **mhmyz** 7 months, 2 weeks ago

**Selected Answer: D**

D  
Service Health can mail only Exchange issue.  
Technical contact get mail M365 total issue.  
upvoted 2 times

✉  **Master\_Tx** 7 months, 3 weeks ago

You can do C and D.  
upvoted 1 times

✉  **daye** 5 months, 1 week ago

not really, within Service Health you can set the service, within global info you can set technical contact which means. So, D.

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

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

Add User3 to Admin1:

User2 only  
User3 only  
User4 only  
User2 and User3 only  
User1, User2, and User3 only  
User1, User2, User3, and User4

**Correct Answer:**

PhoenixMan Highly Voted 6 months ago

I'll go for  
1) 1,2,3 and 4  
2) 2  
upvoted 13 times

AAlmani 3 months ago

the request is to Create a guest user not to Invite one! so User 2 only for both! regards,  
upvoted 2 times

✉️ **Casticod** Highly Voted 8 months ago

A Standard use 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 5 times

✉️ **Casticod** 8 months ago

watch the question "External collaboration settings have default configuration" Confirm mi decision: first option, all users (user 1 user 2 user 3 and user 4)  
upvoted 5 times

✉️ **daye** 5 months ago

this is for b2b

Specify who can invite guests: By default, all users in your organization, including B2B collaboration guest users, can invite external users to B2B collaboration.

upvoted 1 times

✉️ **daye** 5 months ago

<https://learn.microsoft.com/en-us/entra/external-id/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

✉️ **Scotte2023** Most Recent 4 days, 18 hours ago

1) User 2  
2) User 2

<https://learn.microsoft.com/en-us/entra/external-id/b2b-quickstart-add-guest-users-portal>

Prerequisites

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

✉️ **cpaljhc4** 4 months, 1 week ago

Prerequisites

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".

Access to a valid email address outside of your Microsoft Entra tenant, such as a separate work, school, or social email address. You'll use this email to create the guest account in your tenant directory and access the invitation.

Ref: <https://learn.microsoft.com/en-us/entra/external-id/b2b-quickstart-add-guest-users-portal#prerequisites>

and below the prerequisites, it state:

Invite an external guest user

Tip

Steps in this article might vary slightly based on the portal you start from.

Sign in to the Microsoft Entra admin center as at least a "User administrator".

Browse to Identity > Users > All users.

I will go with user 2 & user 2 whether creates or invite it states User Adminstrator.

upvoted 3 times

✉️ **AncaMada112233** 5 months, 2 weeks ago

"Create" guest users or "Invite" guest users is the same action?

upvoted 3 times

✉️ **Contactfornitish** 6 months, 3 weeks ago

Default config means all users including those without any role can also invite guests  
only user admin can manage groups

upvoted 3 times

✉️ **Darekms0** 6 months, 3 weeks 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 2 times

✉️ **Shloeb** 6 months, 4 weeks 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 3 times

✉️ **Greatone1** 7 months 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 3 times

✉️ **cb0900** 7 months, 3 weeks 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 5 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**

*Community vote distribution*

D (100%)

✉️ **Amir1909** 2 months, 4 weeks ago

D is correct

upvoted 2 times

✉️ **solderboy** 4 months ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/microsoft-365/troubleshoot/miscellaneous/reports-show-anonymous-user-name>

upvoted 2 times

✉️ **cb0900** 7 months, 3 weeks ago

**Selected Answer: D**

D Uncheck "Display concealed user, group, and site names in all reports".

upvoted 3 times

## HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to configure the Org settings to meet the following requirements:

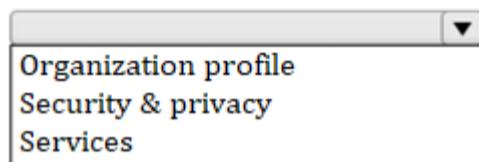
- Sign users out of Microsoft Office 365 web apps after one hour of inactivity.
- Integrate an internal support tool with Office.

Which settings should you configure for each requirement? To answer, select the appropriate options in the answer area.

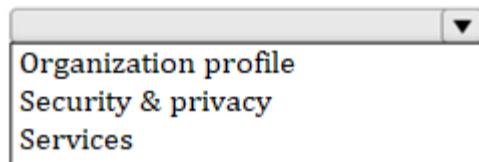
NOTE: Each correct selection is worth one point.

## Answer Area

Sign users out after one hour of inactivity:

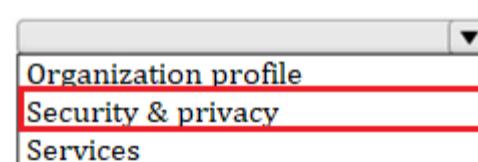


Integrate the internal support tool with Office:



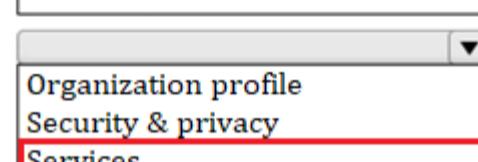
## Answer Area

Sign users out after one hour of inactivity:



## Correct Answer:

Integrate the internal support tool with Office:



 **ae88d96** Highly Voted 8 months ago

Security & privacy and Organization profile. Tested on my lab.  
upvoted 16 times

 **Amir1909** Most Recent 2 months, 4 weeks ago

- Security & Privacy  
- Organization Profile  
upvoted 1 times

 **smiff** 7 months, 1 week ago

Security and Privacy  
Org Profile

checked on my demo tenant  
upvoted 2 times

 **DiligentSam** 7 months, 3 weeks 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** 7 months, 2 weeks ago

Yes - "Support integration"  
upvoted 3 times

 **daye** 5 months, 3 weeks ago

Yes  
Idle session timeout from the Security & privacy tab.  
Support integration from the org profile tab.  
upvoted 1 times

Question #122

Topic 1

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**

*Community vote distribution*

B (100%)

✉  **NrdAlert** 5 months, 3 weeks ago

**Selected Answer: B**

A would be way less hassle to verify the domain, but B answers the question's requirement.

upvoted 3 times

✉  **Vaerox** 3 months, 1 week ago

I believe answer A is the actual attempt to verify the domain, which is what the question is about. So it looks like answer B is correct.

upvoted 2 times

## 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 Highly Voted 7 months, 3 weeks 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 8 times

Greatone1 Most Recent 6 months, 2 weeks ago

Group 1 for both  
upvoted 2 times

Greatone1 6 months, 2 weeks ago

<https://www.examtopics.com/discussions/microsoft/view/9954-exam-ms-101-topic-2-question-20-discussion/>  
upvoted 1 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 Highly Voted 7 months, 3 weeks 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 11 times

imlearningstuffagain 6 months, 2 weeks ago

this is nice wording, the Application Administrator didn't have access to begin with. So he/she doesn't lose access. Correct?

upvoted 5 times

✉️  **nils241** 4 months ago

Users with "Application Administor Role" can only create and manage all aspects of enterprise applications, application registrations, and application proxy settings.

upvoted 2 times

✉️  **sergioandreslq** 5 months, 3 weeks ago

Initially, only those with Microsoft Entra Global Administrator or Security Administrator rights will be able to create and assign roles in the Microsoft 365 Defender portal

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide#before-you-begin>

upvoted 1 times

✉️  **Jamesat** Most Recent 1 week ago

Agreed.

After enabling RBAC only Global Admin and Security Admin will have access so Admin 1 and Admin 2 is correct.

For the second question it is Admin 3 and Admin 4. The question is Users that will NO LONGER have access. The Application Admin never had access so shouldn't be included.

upvoted 1 times

✉️  **Tomtom11** 2 months, 2 weeks ago

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

Initially, only those with Microsoft Entra Global Administrator or Security Administrator rights will be able to create and assign roles in the Microsoft Defender portal, therefore, having the right groups ready in Microsoft Entra ID is important.

Turning on role-based access control will cause users with read-only permissions (for example, users assigned to Microsoft Entra Security reader role) to lose access until they are assigned to a role.

Users with admin permissions are automatically assigned the default built-in Defender for Endpoint global administrator role with full permissions. After opting in to use RBAC, you can assign additional users that are not Microsoft Entra Global or Security Administrators to the Defender for Endpoint global administrator role.

After opting in to use RBAC, you cannot revert to the initial roles as when you first logged into the portal.

upvoted 1 times

✉️  **m2L** 4 months, 2 weeks ago

NO2 : Admin3, Admin4, Admin5

upvoted 2 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?

店铺：学习小店66

- A. standard discovery
- B. device discovery exclusions
- C. basic discovery
- D. a network assessment job

**Correct Answer: B**

*Community vote distribution*

C (78%)      11%      6%

✉  **netbw** Highly Voted 7 months, 1 week 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 7 times

✉  **BossLG** Most Recent 1 month, 2 weeks ago

I agree its C

For further clarification read the FAQ

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-discovery-faq?view=o365-worldwide>  
upvoted 1 times

✉  **Iccen** 2 months, 1 week ago

To achieve the desired outcome of preventing onboarded devices from polling the network for device discovery while still allowing them to discover devices with which they communicate directly in the Microsoft 365 Defender portal, you should:

- B. Device discovery exclusions

Explanation: By configuring device discovery exclusions, you can specify certain devices or ranges of IP addresses that should be excluded from the device discovery process. This allows you to prevent onboarded devices from indiscriminately polling the network for device discovery while still enabling them to discover devices with which they communicate directly. This approach provides a targeted solution to meet the specific requirements outlined in the scenario.

upvoted 1 times

✉  **Amir1909** 2 months, 4 weeks ago

C is correct

upvoted 1 times

✉  **Vaerox** 3 months, 1 week ago

**Selected Answer: D**

I believe it's D. A basic or standard discovery will still scan for the entire network, the scan will just either be passive (less information, less network usage) or active (more information, more network usage).

Please read the article below:

<https://techcommunity.microsoft.com/t5/microsoft-defender-vulnerability/network-device-discovery-and-vulnerability-assessments/ba-p/2267548>

upvoted 1 times

✉  **RJTW070** 3 months, 2 weeks ago

**Selected Answer: A**

AI says A:

To prevent onboarded devices from polling the network for device discovery but still discover devices with which they communicate directly, you should configure the Standard discovery mode in the Microsoft Defender for Endpoint portal<sup>1</sup>. This mode allows endpoints to actively find devices in your network to enrich collected data and discover more devices - helping you build a reliable and coherent device inventory. In addition to devices that were observed using the passive method, standard mode also leverages common discovery protocols that use multicast queries in the network to find even more devices<sup>1</sup>.

Summary: To prevent onboarded devices from polling the network for device discovery but still discover devices with which they communicate directly, you should configure the Standard discovery mode in the Microsoft Defender for Endpoint portal.

upvoted 1 times

✉️ **TheMCT** 3 months, 2 weeks ago

**Selected Answer: A**

Standard discovery (recommended): This mode allows endpoints to actively find devices in your network to enrich collected data and discover more devices - helping you build a reliable and coherent device inventory.

When Standard mode is enabled, minimal, and negligible network activity generated by the discovery sensor might be observed by network monitoring tools in your organization.

upvoted 1 times

✉️ **Sesbri** 3 months, 2 weeks ago

For me it is B. See here for reference: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-device-discovery?view=o365-worldwide#exclude-devices-from-being-actively-probed-in-standard-discovery>

upvoted 1 times

✉️ **Festus365** 5 months, 2 weeks ago

It could be D; A network assessment job

upvoted 2 times

✉️ **Cfernandes** 6 months, 2 weeks ago

**Selected Answer: C**

C esta correta.

upvoted 4 times

✉️ **jt2214** 6 months, 3 weeks 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 3 times

✉️ **Sas2003** 7 months, 2 weeks 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** 7 months, 1 week 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

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

## Correct Answer:

cb0900 [Highly Voted] 7 months, 3 weeks 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 10 times

Cfernandes [Most Recent] 6 months, 1 week ago

Testado no meu laboratório, intune e script local

upvoted 1 times

Contactfornitish 6 months, 3 weeks 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 3 times

✉ **862e76c** 7 months, 2 weeks ago

Agree with the answer

upvoted 1 times

✉ **Casticod** 8 months 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

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

## 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.  
店铺: 学习小店66  
NOTE: Each correct selection is worth one point.

## Answer Area

Group1:	<input type="checkbox"/> Distribution <input type="checkbox"/> Dynamic distribution <input type="checkbox"/> Microsoft 365 <input checked="" type="checkbox"/> Security
Group2:	<input type="checkbox"/> Distribution <input type="checkbox"/> Dynamic distribution <input checked="" type="checkbox"/> Microsoft 365 <input type="checkbox"/> Security

## Answer Area

Group1:	<input type="checkbox"/> Distribution <input type="checkbox"/> Dynamic distribution <input checked="" type="checkbox"/> Microsoft 365 <input checked="" type="checkbox"/> Security
Group2:	<input type="checkbox"/> Distribution <input checked="" type="checkbox"/> Dynamic distribution <input checked="" type="checkbox"/> Microsoft 365 <input type="checkbox"/> Security

  **vercracked\_007** Highly Voted 7 months, 3 weeks ago

Box 1 Microsoft 365  
Box 2 Security

They are swapped  
upvoted 33 times

  **nordbymikael** Most Recent 1 month, 1 week ago

Group1: Microsoft 365 groups are mail enabled, can have RBAC roles assigned and can be used for SharePoint.  
Group2: Create a security group with no mail-enabled functionality and turn on the option for using RBAC roles for the group.  
upvoted 1 times

  **shaffer** 2 months, 1 week ago

It is answered backwards. It should be;  
1: MS365 Group (Mail-enabled with application access)  
2: Security (Non-mail-enabled)  
upvoted 1 times

  **Amir1909** 3 months ago

- Microsoft 365  
- Security  
upvoted 1 times

  **mickey88** 4 months, 1 week ago

Some groups allow dynamic membership or email.  
Microsoft 365 Groups Distribution groups Security groups Mail-enabled security groups Shared mailboxes Dynamic distribution groups  
Mail-enabled Yes Yes No Yes Yes Yes  
Dynamic membership in Microsoft Entra ID Yes No Yes No No

Answer is 1: M365 2 security  
upvoted 1 times

□ **cpaljchc4** 4 months, 1 week ago  
<https://learn.microsoft.com/en-us/answers/questions/732613/azure-ad-what-is-difference-between-security-group>

Add reference page for him  
upvoted 1 times

□ **jdrost\_11** 5 months ago  
Box 1 Microsoft 365  
Box 2 Security

Source: <https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>  
upvoted 1 times

□ **benpatto** 5 months, 1 week ago

To make it easy to understand, it can't be Dynamic distribution as distribution groups are always regarding groups that receive emails, the question at hand doesn't want mail to be enabled. Security groups can be created on an on-prem AD so doesn't require a mailbox (can be created in 365 too but easier to think of it this way IMO)  
upvoted 1 times

□ **Festus365** 5 months, 2 weeks ago

Box 1: Microsoft 365  
Box 2: Dynamic distribution  
upvoted 2 times

□ **jt2214** 6 months, 3 weeks ago

It's the other way around. Exam topics please fix this. :)  
Box 1 Microsoft 365  
Box 2 Security  
upvoted 2 times

□ **DiligentSam** 7 months, 2 weeks ago

Support dynamic membership  
why not choose Dynamic Distribution?  
upvoted 1 times

□ **netbw** 7 months, 1 week ago

Because it's gonna be email enabled  
upvoted 1 times

□ **Casticod** 8 months 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

店铺：学习小店66

店铺：学习小店66

## 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
<b>Correct Answer:</b>
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 8 months ago  
option 1 Service Health --> Report Issues  
option 2 new service request  
upvoted 32 times

✉  **jt2214** Highly Voted 6 months, 3 weeks ago  
Service Health  
New Service Requests

I do this at my organization.  
upvoted 8 times

✉  **Jamesat** Most Recent 1 week ago  
This question is so bad!

How can option 2 be Message Center? How is that going to help you with adding a new user?

Its clearly New Service Request  
upvoted 1 times

✉  **Tomtom11** 1 month ago  
Option 2 should be Health from the Entra ID portal?  
upvoted 1 times

✉  **shaffer** 2 months, 1 week ago  
I'm glad you all confirmed my suspicions  
upvoted 1 times

✉  **pri27** 4 months, 1 week ago  
Discussion ppl are Right, If you still have doubt go here...  
<https://www.examtopics.com/discussions/microsoft/view/96073-exam-ms-100-topic-2-question-87-discussion/>  
upvoted 1 times

✉  **Noble00** 5 months ago  
The answer is so wrong.

upvoted 3 times

曰  **benpatto** 5 months, 1 week ago

Man, I pay for the contributor access and they give us rubbish like this :p it's so obviously its 1. Service health & 2. Service request  
upvoted 3 times

曰  **Greatone1** 7 months ago

Service Health and second answer is new service requests  
upvoted 2 times

曰  **flim322** 7 months, 3 weeks ago

<https://www.examtopics.com/discussions/microsoft/view/96073-exam-ms-100-topic-2-question-87-discussion/>  
upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

You have a Microsoft 365 E5 subscription that contains the groups shown in the following exhibit.

**Groups | All groups**

Contoso Ltd. - Azure Active Directory

New group Download groups Refresh Manage view Delete Got feedback?

Search Add filter

Search mode Contains

4 groups found

<input type="checkbox"/>	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**

Community vote distribution

E (100%)

cb0900 Highly Voted 7 months, 3 weeks 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 15 times

CloudCanary Highly Voted 7 months, 1 week ago

**Selected Answer: E**

Microsoft 365 Groups with Security Enabled can be assigned with licences.

upvoted 5 times

Jamesat Most Recent 1 week ago

**Selected Answer: E**

Clearly Group 2, 3 and 4.

A Security-enabled M365 group can be used for license assignment.

Confirmed to still be the case in my lab.  
upvoted 1 times

曰  **Tomtom11** 1 month ago

security enabled means you can include these groups in DACLs  
upvoted 1 times

曰  **Cfernandes** 6 months, 1 week ago

Concordo com grupo, 2 3 e 4  
upvoted 2 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

## 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 店铺：学习小店66			
2F2747649D4150B686307383 店铺：学习小店66			
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

cb0900 [Highly Voted] 7 months, 3 weeks 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 22 times

m2L [Most Recent] 4 months, 2 weeks ago

Hello Guys,  
the answers are :  
1 : Reports in Org Setting by(Org Setting>Services)  
2: Columns In the raports by (Report Usage)  
Once On Usage, click on "Microsoft Teams apps" and scroll, after the last column you will see "Choose Column" and here you can select the columns you want to display  
upvoted 2 times

曰  **m2L** 4 months, 2 weeks ago

Hello Guys,  
the answers are :  
1 : Reports in Org Setting by(Org Setting>Services)  
2: Columns In the raports by (Report Usage)  
Once On Usage cliques on "Microsoft Teams apps" and scroll, after the last column you will see "Choose Column" and here you can then select the column you want to display

Regards

upvoted 1 times

曰  **Festus365** 5 months, 2 weeks ago

Box 1: Privacy profile in Org settings  
Box 2: Microsoft Teams in Org settings  
upvoted 1 times

曰  **spektrum1988** 3 months ago

100% sure box 1 is: Reports in Org settings.  
100% sure box 2 is: choose columns  
Tested and confirmed.  
upvoted 1 times

曰  **Casticod** 8 months 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 3 times

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**

*Community vote distribution*

AC (100%)

✉  **jt2214** Highly Voted 7 months, 3 weeks 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 9 times

✉  **AAlmani** Most Recent 3 months ago

**Selected Answer: AC**

A or C solve the issue.  
<https://www.examtopics.com/discussions/microsoft/view/14496-exam-ms-100-topic-2-question-18-discussion/>

upvoted 2 times

✉  **TP447** 5 months, 3 weeks ago

Technically A + D is valid too (if the agent is still installed but timed out after 30 days on inactivity - you would just start the service and run the PowerShell command).  
upvoted 1 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.

✉  **Festus365** Highly Voted 5 months, 2 weeks ago

1:Add a custom domain name  
2:verify the custom domain  
3:Modify the User1 email address or create an alternative email address for the user1(UPN)  
upvoted 10 times

✉  **BossLG** 1 month, 2 weeks ago

<https://www.examtopics.com/discussions/microsoft/view/49929-exam-ms-100-topic-2-question-7-discussion/>

Given answer is correct, we modify the user (UPN) not email address

upvoted 1 times

✉  **DiligentSam** Highly Voted 7 months ago

<https://www.examtopics.com/discussions/microsoft/view/49929-exam-ms-100-topic-2-question-7-discussion/>  
upvoted 6 times

✉  **Paul\_white** Most Recent 7 months ago

GIVEN ANSWER IS CORRECT !!!

upvoted 4 times

✉  **spectre786** 7 months 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 2 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**

*Community vote distribution*

B (100%)

nils241 4 months ago

**Selected Answer: B**

Correct

upvoted 2 times

DiligentSam 7 months, 1 week ago

Option B is correct

upvoted 3 times

862e76c 7 months, 2 weeks ago

Agree with the answer

upvoted 3 times

## HOTSPOT

Your company has a Microsoft 365 subscription that contains the domains shown in the following exhibit.

## Domains

<span style="color: blue;">+</span> Add domain <span style="color: green;">-</span> Buy domain <span style="color: cyan;">↻</span> Refresh		
Domain name ↑	Status	<span style="color: green;">-</span> Choose columns
<input type="checkbox"/> contoso221018.onmicrosoft.com (Default)	<span style="color: green;">✓</span> Healthy	
<input type="checkbox"/> contoso.com	<span style="color: blue;">i</span> Incomplete setup	
<input type="checkbox"/> east.contoso221018.onmicrosoft.com	<span style="color: blue;">i</span> No services selected	

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 8 months ago

Tested

option 1 contoso@221018.onmicrosoft.com and eastcontoso@221018.onmicrosoft.com

Option 2 contoso@221018.onmicrosoft.com only

upvoted 34 times

✉  **Fran22** Most Recent 2 months ago

The same question is in the test exams that Microsoft provides on its website: <https://learn.microsoft.com/en-us/credentials/certifications/exams/ms-102/>. Casticod's answers are correct !

upvoted 2 times

✉  **Vaerox** 3 months, 3 weeks ago

I added my own domain to a test tenant, verified it with a TXT record but didn't actually add MX records. Status = Possible service issues.

I was able to add a user with the e-mail address of the 'unfinished' tenant. So given answers seem to be correct.

upvoted 1 times

✉️ **Vaerox** 3 months, 1 week ago

So sorry, wrong status on the domain. The answer of Casticod is correct. I tested it again and was not able to create a new useraccount with the domain "Incomplete status".

A similar question is on the Practice Assessment. The correct answer there is the same as Casticod provided.

upvoted 2 times

✉️ **Testtest123** 4 months, 4 weeks ago

If the domain is registered with a hosting or service provider, and "No services selected" means that no hosting or other services are currently active, an administrator might still be able to create accounts related to domain management. These accounts could be for managing the domain's settings, renewals, or to activate services in the future. However, they would not be able to create service-specific accounts (like email accounts) if those services are not active.

店铺: 学习小店66  
So the first question is correct: contoso@221018.onmicrosoft.com and eastcontoso@221018.onmicrosoft.com

Question two is also correct.

upvoted 3 times

✉️ **TP447** 5 months, 3 weeks ago

You can create UPN with the incomplete status domain Contoso.com too (tested in my lab). I believe the given answer is correct.

upvoted 2 times

✉️ **TP447** 5 months, 3 weeks ago

Scratch this - it works for a subdomain that is incomplete but not a top level domain.

upvoted 1 times

✉️ **mhmyz** 7 months, 2 weeks 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 3 times

店铺: 学习小店66

店铺: 学习小店66

## 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 SharePoint site usage report	
The Teams usage report in Teams	
The User activity report in Teams	

Requirements
Correct Answer: The storage usage of files stored in Microsoft Teams: The SharePoint site usage report
Number of active users per Microsoft Team: The User activity report in Teams

✉  **Casticod**  8 months 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 18 times

✉  **Tomtom11**  1 month ago

<https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/microsoft-teams-usage-activity?view=o365-worldwide>  
 Answer for Question 2  
 Microsoft Teams usage activity  
 upvoted 1 times

✉  **Tomtom11** 1 month ago

<https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/sharepoint-site-usage-ww?view=o365-worldwide>  
 upvoted 1 times

✉  **m2L** 4 months, 2 weeks ago

The First is typically OneDrive Usage  
 upvoted 1 times

✉  **solderboy** 4 months ago

You are incorrect. OneDrive is for personal chat files, not for Teams. Teams files stored in SharePoint.  
 upvoted 2 times

✉  **Blagojche** 7 months 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 2 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

**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

店铺：学习小店66

店铺：学习小店66

✉  cb0900 Highly Voted 7 months, 3 weeks 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 17 times

✉  Amir1909 Most Recent 2 months, 4 weeks ago

- 1
  - 3
- upvoted 4 times

✉  Drubury 6 months, 2 weeks ago

All sub-domains need to be verified.

See this article about half way down: <https://learn.microsoft.com/en-us/azure/architecture/guide/multitenant/considerations/domain-names>  
upvoted 1 times

✉  Drubury 6 months, 2 weeks ago

My bad, you guys are correct. 1 and 3. See this article: <https://learn.microsoft.com/en-us/entra/identity/users/domains-manage>  
upvoted 5 times

✉  Darekms0 6 months, 3 weeks ago

<https://www.examtopics.com/discussions/microsoft/view/51183-exam-ms-100-topic-4-question-48-discussion/>  
upvoted 2 times

✉  Greatone1 7 months ago

Should be 1 and second is 3  
upvoted 4 times

店铺：学习小店66

店铺：学习小店66

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**

*Community vote distribution*

D (100%)

✉️  **Momskii**  7 months, 3 weeks 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 9 times

✉️  **Tomtom11**  1 month ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-data-sources>

upvoted 1 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** Highly Voted 8 months ago

Correct

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-quickstart-naming-policy>

upvoted 8 times

✉️  **Thomasname** Most Recent 2 months, 1 week ago

Correct

<https://learn.microsoft.com/en-us/entra/identity/users/groups-naming-policy#configure-a-naming-policy>

upvoted 1 times

 **Amir1909** 2 months, 4 weeks ago

Correct

upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

## 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

Correct Answer:

None of the groups

- 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

cb0900 Highly Voted 7 months, 3 weeks 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 14 times

vercracked\_007 Highly Voted 7 months, 3 weeks 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 8 times

vercracked\_007 7 months, 3 weeks ago

The other way around wont work. Group 4 cant be a member of group 5  
upvoted 1 times

vercracked\_007 7 months, 3 weeks ago

Sorry, group 3  
upvoted 2 times

Tomtom11 Most Recent 1 month ago

<https://learn.microsoft.com/it-it/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>  
upvoted 1 times

Thomasname 2 months, 1 week ago

Group1: none  
Group4: 3 + 5

"We currently don't support:

Adding groups to a group synced with on-premises Active Directory.  
Adding security groups to Microsoft 365 groups.  
Adding Microsoft 365 groups to security groups or other Microsoft 365 groups.  
Assigned membership to shared resources and apps for nested security groups.  
Applying licenses to nested security groups.  
Adding distribution groups in nesting scenarios.  
Adding security groups as members of mail-enabled security groups.  
Adding groups as members of a role-assignable group."  
<https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-groups#add-or-remove-a-group-from-another-group>  
upvoted 5 times

m2L 4 months, 2 weeks ago

Thank you @Flim322, you are right,  
Group nesting isn't supported. A group can't be added as a member of a role-assignable group.  
Therefore, Group 4: Group 5 only  
I complete your answer by this important link.

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept>  
upvoted 1 times

solderboy 4 months ago

I am not convinced about this. Noticed the statement "Group nesting isn't supported. A group can't be added as a member of a role-assignable group". However, Group4 is NOT a role-assignable group (but Group3 is a role-assignable group). But the question is asking to add Group3 to Group4, NOT the other way around. So, I think adding Group3 to Group4 is OK. But adding Group4 to Group3 won't be OK.  
So Box2 should be Group3 and Group5 only.

upvoted 3 times

benpatto 5 months, 1 week ago

seems no one has a good answer for this... :D  
upvoted 1 times

Festus365 5 months, 2 weeks ago

Group 1: a member of group 2 only (M365)  
Group 4: a member of group 3 and group 5 only  
upvoted 1 times

flim322 7 months, 3 weeks 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 3 times

solderboy 4 months ago

I am not convinced about this. Noticed the statement "Group nesting isn't supported. A group can't be added as a member of a role-assignable group". However, Group4 is NOT a role-assignable group (but Group3 is a role-assignable group). But the question is asking to add

Group3 to Group4, NOT the other way around. So, I think adding Group3 to Group4 is OK. But adding Group4 to Group3 won't be OK.  
So Box2 should be Group3 and Group5 only.

upvoted 2 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

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**

*Community vote distribution*

C (61%)

B (39%)

✉️  cb0900 Highly Voted 7 months, 3 weeks 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 11 times

✉️  JensV 7 months, 3 weeks 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 5 times

✉️  60ed5c2 6 months, 1 week ago

Because the location is not set - it will inherit the location and therefore the license will be set because the license is allowed in those locations. However, if the location were set to be someplace where the license is not allowed - then you would get an error message.....if I am reading the information correctly.

upvoted 1 times

✉️  Lud0 Highly Voted 7 months, 3 weeks ago

**Selected Answer: B**

Usage location is mandatory to affect license.

upvoted 9 times

✉️  darcone23 Most Recent 3 days, 19 hours ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/entra/identity/users/licensing-group-advanced#limitations-and-known-issues>

Group-based licensing currently doesn't support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied.

upvoted 1 times

✉️  Scotte2023 5 days, 22 hours ago

**Selected Answer: B**

I understand you are getting an error "License cannot be issued to a user without an use location specified." When assigning licenses in Azure Active Directory.

This is because some of these users do not have usage location specified in Azure Active Directory. To check for user location, sign in to Azure Active Directory > Users > select user > edit properties > check usage location.

<https://answers.microsoft.com/en-us/msoffice/forum/all/license-cannot-be-assigned-to-a-user-without-a/1239da04-1bf7-439b-a4b1-016cfbc2fa0d>

upvoted 1 times

✉️ **Motanel** 6 days, 20 hours ago

in the exercise is mentioned an Entra ID License, therefore you would do there the License assignment, where user location is NOT mandatory.

upvoted 1 times

✉️ **Tomtom11** 1 month ago

<https://learn.microsoft.com/en-us/entra/identity/users/licensing-group-advanced>

upvoted 1 times

✉️ **msmamrs** 1 month, 3 weeks ago

**Selected Answer: B**

definitely B!

upvoted 2 times

✉️ **692a0df** 3 months ago

**Selected Answer: B**

You need a Usage Location in order to set a license. Our tenant has a custom rule in play to auto assign Usage Location - so we never manually need to do it...

<https://answers.microsoft.com/en-us/msoffice/forum/all/license-cannot-be-assigned-to-a-user-without-a/1239da04-1bf7-439b-a4b1-016cfbc2fa0d>

upvoted 2 times

✉️ **Festus365** 3 months, 1 week ago

Answer is C=3. {User2 inherited United States as a location from User1 as a group membership Group1 and Group2}.

upvoted 1 times

✉️ **Vaerox** 3 months, 1 week ago

**Selected Answer: C**

We have 200 customer tenants at the company I work for and we never set Usage location.

upvoted 3 times

✉️ **Drumbum27** 5 months, 3 weeks ago

**Selected Answer: C**

For group license assignment, any users without a usage location specified inherit the location of the directory.

upvoted 4 times

✉️ **Darekms0** 6 months, 3 weeks ago

**Selected Answer: C**

<https://www.examtopics.com/discussions/microsoft/view/49561-exam-ms-100-topic-2-question-11-discussion/>

upvoted 3 times

✉️ **Lud0** 7 months, 3 weeks 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 3 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

Correct Answer:

- | 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"/>            |

✉ cb0900 [Highly Voted] 7 months, 3 weeks 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 36 times

✉️  **Fran22** 2 months ago

Is correct. 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. In other words, an administrator scoped to the administrative unit can manage properties of the group, such as group name or membership, but they cannot manage properties of the users or devices within that group.

upvoted 2 times

✉️  **oopspruu** Most Recent 1 week, 6 days ago

When you add a group to an AU, the AU actions only apply to group but not it's members. So NNY

upvoted 1 times

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

Y - user1 is member of group1, so member of AU1. since au1 is no group itself, there is no nested group, so this works.  
N - User 4 is not a member of AU1  
Y: user3 can assign licenses to the entire organisation

upvoted 1 times

✉️  **CheMetto** 6 months, 1 week ago

I confirm NNY, Nested group aren't supported from Administrative Unit!

upvoted 2 times

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

*Community vote distribution*

E (100%)

✉️  **Casticod** Highly Voted 8 months ago

**Selected Answer:** E

Correct <https://learn.microsoft.com/en-us/microsoft-365/admin/adoption/adoption-score?view=o365-worldwide#adoption-score-prerequisites>  
upvoted 8 times

✉️  **Greatone1** Highly Voted 6 months, 4 weeks 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 5 times

✉️  **Amir1909** Most Recent 2 months, 4 weeks ago

E is correct  
upvoted 1 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

店铺：学习小店66

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.

店铺：学习小店66

店铺：学习小店66

## 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

店铺: **Statements**

User1 can invite guest users.

**Yes**

**No**

User2 can invite guest users.

User3 can invite guest users.

### 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"/>

曰 **INSOMEA** Highly Voted 7 months, 2 weeks ago

correct  
upvoted 8 times

店铺：学习小店66

曰 **jt2214** Highly Voted 6 months, 2 weeks ago

This is correct. HelpDesk Administrator cannot invite guest users.  
Only users assigned to specific admin roles can invite guest users: To allow only those users with administrator roles to invite guests, select this radio button. The administrator roles include Global Administrator, User Administrator, and Guest Inviter.

<https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure>

upvoted 7 times

曰 **Tomtom11** Most Recent 1 month ago

<https://learn.microsoft.com/en-us/microsoft-365/admin/adoption/adoption-score?view=o365-worldwide#adoption-score-prerequisites>

Only users assigned to specific admin roles can invite guest users: To allow only those users with administrator roles to invite guests, select this radio button. The administrator roles include Global Administrator, User Administrator, and Guest Inviter.  
upvoted 1 times

曰 **PhoenixMan** 5 months, 2 weeks ago

in today exam  
upvoted 3 times

店铺：学习小店66

店铺：学习小店66

**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**

<b>Statements</b>	<b>Yes</b>	<b>No</b>
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**

<b>Statements</b>	<b>Yes</b>	<b>No</b>
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"/>

✉ cb0900 Highly Voted 7 months, 3 weeks ago

Y  
Y  
Y

<https://www.examtopics.com/discussions/microsoft/view/96500-exam-ms-100-topic-3-question-100-discussion/>  
upvoted 14 times

✉ Paul\_white 7 months ago

THANK YOU BROTHER  
upvoted 1 times

✉ de0e20a Most Recent 1 week, 1 day ago

For the "You can assign Admin2 the User administrator role for AU1"  
I think the trick in assumption here is in the not in the fact you could do this action, but as the tenant is setup currently you need to do additional steps. As it stands Admin2 is not an assigned security principal for AU1 nor is AU1 assigned the user administrator role currently. So you would first need to assign that role to the AU and then assign that user to the AU and then it would be given the User Administrator role.

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-assign-roles>  
upvoted 1 times

 Greatone1 7 months ago

Should be Y,Y,Y  
upvoted 4 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

## 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	None
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

✉ siulas Highly Voted 8 months ago

1. Correct.
  2. All users
- <https://www.examtopics.com/discussions/microsoft/view/50897-exam-ms-100-topic-3-question-79-discussion/>  
upvoted 12 times

✉ aleksdj 5 months, 2 weeks ago

The first one is wrong, it is users 1 and 2 for sure!

upvoted 4 times

✉ siulas 8 months ago

1. User1 and User2 only
  2. All users
- upvoted 18 times

cb0900 7 months, 3 weeks ago

Agree:

1. User 1 and User 2
2. All users

Tested in a lab.

upvoted 5 times

Casticod 8 months ago

I think The same

1. User1 and User2 only
2. All users

upvoted 9 times

EEMS700 6 months, 1 week ago

1. User1 and User2 only

2. All users

upvoted 8 times

Jamesat [Most Recent] 1 week ago

This is the second time this question has come up. And both times the wrong answer.

If the external collaboration settings are default then All Users can invite guest users.

upvoted 1 times

TonyManero 3 weeks, 5 days ago

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#security-administrator>

User 1 and User 2 because Global and Security admin can modify password protection.

All Users can invite Guest (default)

upvoted 1 times

Frippy 4 months, 1 week ago

Wait wait wait...

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

Before you begin: You must be a global administrator to perform this task.

So

- 1: User1 and User2

2. User1

upvoted 4 times

m2L 4 months, 2 weeks ago

1. User1 & User2(Tested)

upvoted 1 times

Festus365 5 months ago

Both box: 1&2 answers should be User 1, user 2 and user 4 because user 3 has no role and shouldn't be included as an administrative role.( Global administrator, security administrator and password administrator could modify password protection policy as well as create new guest users)

upvoted 1 times

Drumbum27 5 months, 3 weeks ago

I think this is word play.. All users can invite a guest user. All users can not create a guest user

upvoted 4 times

Vaerox 3 months, 1 week ago

No it's not. No one can simply 'create' a guest user. It will always be an invite, no matter who's inviting the guest.

upvoted 1 times

5e0d3df 2 months, 4 weeks ago

Correct, even when you're doing it through AAD "Create user" option, it will show "Invite external user". Just tested it without any active role.

So:

- 1: User 1 & User 2

2: All users

upvoted 1 times

imlearningstuffagain 6 months, 2 weeks ago

Invite Guest users:

"External collaboration settings have default configuration." the table states "Invite Guest Users"

<https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions?context=%2Fazure%2Factive-directory%2Froles%2Fcontext%2Fuser-context#compare-member-and-guest-default-permissions>

So answer should be: Users 1, 2 3,4

upvoted 1 times

rfree 7 months, 2 weeks 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

曰  **JensV** 7 months, 3 weeks 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 3 times

曰  **Casticod** 8 months ago

Try in my lab tenant, Standard user (not assigned rol) to be able to create a Guest user.

upvoted 2 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

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

✉  **sigvast** 5 months, 3 weeks ago

Correct.

To add, modify, or remove domains, you must be a Domain Name Administrator or Global Administrator

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

✉  **Greatone1** 7 months 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** 7 months, 2 weeks 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.  
店铺：学习小店66  
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

*Community vote distribution*

C (100%)

✉️ **Vincent1966** [Highly Voted] 7 months, 3 weeks 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 7 times

✉️ **Vaerox** 3 months, 1 week ago

So the answer is D? Both User 1 and User 3?  
upvoted 1 times

✉️ **Tomtom11** [Most Recent] 2 months, 1 week ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/location-condition>  
GPS location doesn't work with passwordless authentication methods.  
upvoted 3 times

✉️ **Amir1909** 2 months, 4 weeks ago

C is correct  
upvoted 2 times

✉️ **Vaerox** 3 months, 1 week ago

**Selected Answer: C**

Given answer is correct. I was confused because normally a CA policy would be able to help defend all users but...using GPS named locations requires a user to have the MS Authenticator app:  
"

If you select Determine location by GPS coordinates, the user needs to have the Microsoft Authenticator app installed on their mobile device. Every hour, the system contacts the user's Microsoft Authenticator app to collect the GPS location of the user's mobile device.  
"  
upvoted 2 times

✉️ **faeem** 7 months, 1 week 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 4 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

## 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

店铺：学习小店66

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 7 months, 3 weeks 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 11 times

✉ **Craigg** Most Recent 2 months, 1 week ago

Hi  
 Box 2 should only be user 2. As Administrator Roles cannot use security questions as part of SSPR. As explained in this link.  
<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy>.  
 upvoted 1 times

✉ **de0e20a** 1 week, 1 day ago

In the Link you gave:

Administrator reset policy differences

By default, administrator accounts are enabled for self-service password reset, and a strong default two-gate password reset policy is enforced.

upvoted 1 times

benpatto 5 months, 1 week ago

Agree with vincent, use entra / intune every day and 100% correct.

upvoted 1 times

vercracked\_007 7 months, 3 weeks 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

Vaerox 3 months, 1 week ago

You forgot User4, he's an admin. Admins are always enabled for SSPR:

"By default, administrator accounts are enabled for self-service password reset, and a strong default two-gate password reset policy is enforced."

upvoted 1 times

Casticod 7 months, 4 weeks 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 3 times

Casticod 7 months, 4 weeks ago

Sorry error in the responses.

Option 1: User1, user2, and user4 (user 1and 4 by admins, user 2 for group assignment)

Option 2: User 2 Only (the admins can't use the security Questions)

upvoted 7 times

Casticod 8 months 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 8 months ago

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr#enable-self-service-password-reset>

upvoted 2 times

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

*Community vote distribution*

C (100%)

✉  **de0e20a** 1 week, 1 day ago

This is a case of what is the Microsoft approved method versus what will work, Option D will work without option C being put in place but its not the Microsoft approved method as is documented.

upvoted 1 times

✉  **DiligentSam** 7 months ago

Given Answer is correct

upvoted 2 times

✉  **spectre786** 7 months 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** 7 months 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 3 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**

*Community vote distribution*

B (88%)	13%
---------	-----

✉️  **Demoster** Highly Voted 7 months, 3 weeks 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 10 times

✉️  **Amir1909** Most Recent 3 months ago

- anonymous IP address and atypical travel only  
upvoted 2 times

✉️  **benpatto** 5 months, 1 week ago

Agree with NrdAlrt, for atypical travel etc, it would make a difference if the user wasn't connecting over an RDP. Seeing as there's a RDP connection setup by the IT team, these would have to be trusted locations in the network to be able to access Sharepoint in the first place.  
upvoted 1 times

✉️  **NrdAlrt** 5 months, 4 weeks ago

**Selected Answer: B**

Just looking at this, the only thing the system should care about is the anonymous login since the user is new. Microsoft likes to paint their security products as being useful, not generating false positives for normal behavior. NYC login isn't bad by itself and remote desktop connections almost certainly have some sort of reputation/trust associated with them established by the IT department. The fact that they call out the recent user creation date lends further credence they want you to demonstrate we know what detections require time to learn a new user.  
upvoted 4 times

✉️  **poesklap** 6 months, 1 week ago

**Selected Answer: E**

Anonymous IP address: User1 signed in from an anonymous IP address.

Atypical travel: User1 established Remote Desktop connections to hosts in Berlin and Hong Kong, indicating atypical travel from New York City.

Unfamiliar sign-in properties: The sign-in from an anonymous IP address and the sign-in from the Remote Desktop connections could be considered unfamiliar sign-in properties, as they deviate from the usual patterns of sign-ins.  
upvoted 2 times

✉️  **JensV** 7 months, 3 weeks 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 2 times

□ **poesklap** 6 months, 1 week ago

In the scenario described, actions like signing in from an anonymous IP address, atypical travel, and establishing remote desktop connections to locations like Berlin and Hong Kong could be considered unusual and may trigger risk assessments, even during the learning period. The learning period allows the system to better understand the user's typical behavior and adapt its risk assessments accordingly.

upvoted 1 times

□ **NrdAlert** 5 months, 4 weeks ago

Good point, but tough question still. I question why they include the info about when the user was created. That seems to be an intentiona callout. Also remote desktops in a corporation would likely be excluded from those policies if they are allowing people to login from wherever.

upvoted 1 times

□ **vercracked\_007** 7 months, 3 weeks ago

should be E

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#risk-types-and-detection>

upvoted 3 times

□ **vercracked\_007** 7 months, 3 weeks 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

店铺：学习小店66

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"/>

店铺：学习小店66

**Answer Area**

Correct Answer:	Statements	Yes	No
	User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	<input checked="" 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 checked="" type="radio"/>
	User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	<input checked="" type="radio"/>	<input type="radio"/>

aleksdj Highly Voted 5 months, 2 weeks ago

Y = User1 is on the MFA block list BUT IP range 133.107.10.20 is Montreal which is EXCLUDED from MFA so user1 can access  
 N = User1 is on the MFA block list AND IP range 193.77.10.15 is Toronto which is INCLUDED in MFA so User cannot access

Y = User2 is not in the MFA block list and is a member of Group2 which is excluded from the conditional access policy and therefore can access from 193.77.10.20 Toronto. User2 is even allowed to access M365 from Montreal because the policy is not applied to User2.  
upvoted 8 times

✉️ **Motanel** 1 week ago

But since the policy is a grant access, and not block access, doesn't that mean all answers are the other way around?  
which would be  
N,  
Y  
N  
upvoted 1 times

✉️ **2dwarf** Highly Voted 5 months, 1 week ago

I think it is NNY, because MFA is not enforced by policy. When you are blocked with MFA you cannot sign in any way.  
upvoted 7 times

✉️ **pali5178** Most Recent 4 days, 22 hours ago

Statement 1: User1 can sign in to Microsoft SharePoint Online from Toronto.

店铺：学习小铺66

No. Even though Toronto is included in the locations, User1 is on the MFA blocked users list. This means they will be blocked from signing in regardless of the conditional access policy's rules.

Statement 2: User2 can sign in to SharePoint Online from Montreal.

No. While User2 is part of a group excluded from the policy, the location Montreal is specifically excluded. Any access attempt from that location will be blocked.

Statement 3: User3 can sign into SharePoint Online from Montreal if the user performs multi-factor authentication.

Yes. Here's why:

User3 is in the included Group1.

Montreal is explicitly excluded, HOWEVER, the policy grants access if MFA is performed.

Therefore, if User3 performs MFA successfully, the location restriction is bypassed.

upvoted 1 times

✉️ **de0e20a** 5 days, 5 hours ago

The issue here is that "Blocked MFA users List" according to Microsoft Learn is actually a report that says why a user's MFA was blocked. In this case the second option would cause an entry in that "list"

This is the only reference I could find to a "List"

<https://techcommunity.microsoft.com/t5/microsoft-entra/unblock-mfa/m-p/408018>

There is however a section in Azure MFA that you can block or unblock the ability for the app to send requests to the Azure Tenant. This however is not seen as a list in the Microsoft documentation.

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-mfasettings#block-and-unblock-users>

So the user being on a blocked MFA list just means that they have had failed MFA attempts which wouldn't matter to the Conditional Access Policies.

upvoted 1 times

✉️ **SBGM** 2 months, 4 weeks ago

Can't figure this one out and don't have the time to set up a lab scenario, but:

Azure blocked users page states:

'A blocked user will not receive multifactor authentication requests. Authentication attempts for that user will be automatically denied. A user will remain blocked for 90 days from the time they are blocked.'

ChatGPT:

If a user is on the blocked MFA users list in Azure, their sign-in attempts will be blocked regardless of the location from which they are attempting to sign in. Exclusions based on location for not requiring MFA typically apply to users who are not on the blocked list. Once a user is on the blocked list, their sign-in attempts will be blocked regardless of other factors such as location exclusions. Therefore, even if the user is trying to sign in from a location excluded from MFA requirements, their login attempt will still be blocked if they are on the blocked MFA users list.'

I am convinced that User 1 is unable to sign in regardless of location/IP address

upvoted 3 times

✉️ **itguys** 4 months, 2 weeks ago

NNY

user MFA is enabled in legacy settings....

upvoted 3 times

✉️ **itguys** 4 months, 2 weeks ago

\*legacy

upvoted 1 times

✉️ **TP447** 5 months, 3 weeks ago

NNY is correct. User1 would not trigger the CA Policy from Montreal due to the exclusion so would be granted access without requiring MFA.  
upvoted 2 times

✉️ **jt2214** 5 months, 3 weeks ago

I would assume since User 1 is on the blocked list they cannot access?

upvoted 3 times

✉️ 🚩 **rfree** 6 months, 2 weeks ago

NNY. Question is, Can User 1 connect? NOT can User1 connect with MFA. And the CA doesn't apply to montreal anyway since its excluded.

upvoted 2 times

✉️ 🚩 **Darekmso** 6 months, 2 weeks ago

<https://www.examtopics.com/discussions/microsoft/view/55435-exam-ms-100-topic-4-question-36-discussion/> NNY

upvoted 2 times

✉️ 🚩 **netbw** 7 months ago

Answer is correct. User1 can connect from Montreal.

upvoted 1 times

✉️ 🚩 **BlackCat9588** 7 months, 2 weeks ago

NNY?

MFA of user1 is blocked

upvoted 3 times

店铺: 学习小店66

✉️ 🚩 **BlackCat9588** 7 months, 1 week ago

Exclude: Montreal

upvoted 1 times

✉️ 🚩 **NrdAlert** 5 months, 4 weeks ago

But an exclusion just means they are excluded from the policy and the policy grants access. I guess it's assumed they are still allowed access by skipping this policy being applied to them(and that nothing else is denying them access).

upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

**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

Enable

Include Exclude

Target  All users  Select groups

[Add groups](#)

Name	Type	Registration	Authentication mode	
Group1	Group	Optional	Passwordless	<input type="button" value="X"/>
Group2	Group	Optional	Passwordless	<input type="button" value="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 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"/>

店铺：学习小店66

店铺：学习小店66

## 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:

Scotte2023 5 days, 21 hours ago

How does multifactor authentication work?

Let's say you're going to sign into your Microsoft account or work or school account, and you enter your username and password. If that's all you need then anybody who knows your username and password can sign in as you from anywhere in the world!

But if you have multifactor authentication enabled, things get more interesting. The first time you sign in on a device or app you enter your

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

店铺：学习小店66

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 7 months, 3 weeks 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 9 times

NrdAirt 5 months, 4 weeks ago

Agree, the answers here don't make sense. They are only a user administrator which doesn't give them access to the sign-in reports.  
upvoted 3 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**

*Community vote distribution*

B (100%)

✉️  **TonyManero** 3 weeks, 4 days ago

**Selected Answer: B**

Correct

upvoted 1 times

✉️  **DiligentSam** 7 months, 1 week ago

<https://www.examtopics.com/discussions/microsoft/view/45311-exam-ms-100-topic-3-question-66-discussion/>

upvoted 4 times

✉️  **GLL** 7 months, 1 week ago

correct

upvoted 1 times

✉️  **CloudCanary** 7 months, 1 week 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**

✉️ 🚩 **Festus365** 5 months, 2 weeks ago

Answer is NO! B: because Active directory is unavailable for Pass through authentication.

upvoted 4 times

✉️ 🚩 **momowagdy** 1 week, 6 days ago

I dont get the point of ur answer. but it is because if active directory goes unavailable, microsoft will need AD to authenticate the password since pass through authentication is on. the solution here is to use password hash

upvoted 2 times

✉️ 🚩 **Paul\_white** 7 months ago

ANSWER IS B !!!!!!

upvoted 2 times

店铺：学习小店66

店铺：学习小店66

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**

*Community vote distribution*

B (68%)

A (32%)

✉️  **BSVIT**  5 months, 3 weeks ago

**Selected Answer: B**

B, WHY?

Solution only partly meets requirements.

solution does meet the goal for requirement 1: 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.

solution does NOT meet the goal for requirement 2: "When password hash synchronization is enabled, the password complexity policies in your on-premises Active Directory instance override complexity policies in the cloud for synchronized users. You can use all of the valid passwords from your on-premises Active Directory instance to access Microsoft Entra services."

So configuring password complexity policies in AzureAD is pointless as is gets overwritten.

Source: <https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-password-hash-synchronization>  
upvoted 11 times

✉️  **Hard1k**  7 months, 3 weeks 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 11 times

✉️ **Frippy** 4 months, 1 week ago

There is no "minimum length and complexity" in AzureAD  
upvoted 3 times

✉️ **Milad666** 6 months, 4 weeks ago

WRONG! User that synchronized with PHS will just inherit Policies and attributes from Active Directory. So Solution doesn't meet the goal.  
upvoted 14 times

✉️ **EEMS700** 5 months, 3 weeks ago

I agree with Milad  
Policies they will be used are from Active Directory  
Correct answer is B  
upvoted 3 times

✉️ **oopspruu** [Most Recent] 1 week, 4 days ago

**Selected Answer: B**  
The solution doesn't satisfy the 2nd requirement. The password policies need to be enforced in on-prem AD if PHS is used. With PHS, AD password policies always override AAD password policies.

upvoted 1 times

✉️ **CharlesS76** 4 weeks ago

**Selected Answer: B**  
Password policies that will be used are from Active Directory...  
upvoted 1 times

✉️ **Tomtom11** 4 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad-on-premises>  
Microsoft Entra Password Protection detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization. On-premises deployment of Microsoft Entra Password Protection uses the same global and custom banned password lists that are stored in Microsoft Entra ID, and does the same checks for on-premises password changes as Microsoft Entra ID does for cloud-based changes. These checks are performed during password changes and password reset events against on-premises Active Directory Domain Services (AD DS) domain controllers.

upvoted 1 times

✉️ **Tomtom11** 4 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad-combined-policy>  
upvoted 1 times

✉️ **Tomtom11** 4 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-password-hash-synchronization>  
There are two types of password policies that are affected by enabling password hash synchronization:

Password complexity policy  
Password expiration policy  
upvoted 1 times

✉️ **Fran22** 2 months ago

The answer is no.  
<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-password-hash-synchronization>.  
Says: When password hash synchronization is enabled, the password complexity policies in your on-premises Active Directory instance override complexity policies in the cloud for synchronized users.  
Passwords for users that are created directly in the cloud are still subject to password policies as defined in the cloud.

upvoted 1 times

✉️ **Tomtom11** 2 months, 1 week ago

**Selected Answer: A**  
<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-password-hash-synchronization>  
Generally, password hash synchronization is simpler to implement than a federation service. It doesn't require any additional servers, and eliminates dependence on a highly available federation service to authenticate users.  
Password hash synchronization can also be enabled in addition to federation. It may be used as a fallback if your federation service experiences an outage  
upvoted 1 times

✉️ **SBGM** 2 months, 4 weeks ago

**Selected Answer: B**  
Hybrid deployments where user accounts are synced from AD to Azure AD will keep the Active Directory password restrictions, even when Pass Through Authentication is not active. The Azure AD Password restrictions only restrict cloud-native accounts.  
upvoted 1 times

✉️ **AAlmani** 3 months ago

**Selected Answer: B**  
the given scenario is about synchronizing users from op-prem AD to Azure AD, so password protection should be applied on-prem AD. Correct Solution: Implement password hash synchronization and modify the password settings from the Default Domain Policy in Active Directory.  
upvoted 1 times

✉️ **shubu2276** 3 months, 1 week ago

**Selected Answer: B**

No, this does not meet the goal. Password hash synchronization and password protection in Azure AD are two different features that serve different purposes. Password hash synchronization allows users to sign in to Microsoft 365 services using the same password as their on-premises Active Directory account, but it does not provide any backup or failover mechanism if Active Directory becomes unavailable. Password protection helps to enforce strong passwords by blocking common or weak terms, but it does not affect the length of the passwords. To meet the goal, you need to implement a different solution, such as Azure AD Connect Health with AD FS or Pass-through Authentication, and configure a password policy in Active Directory that requires passwords to be 10 characters or more.

upvoted 1 times

□ **Christianbrivio1991** 5 months, 2 weeks ago

**Selected Answer: B**

Correct Answer B

upvoted 1 times

□ **Festus365** 5 months, 2 weeks ago

Answer is YES! A: When Active directory is unavailable then Pass hash synchronization works while password protection and modification is configured for users to be authenticated.

upvoted 2 times

□ **TP447** 5 months, 3 weeks ago

B for me is correct. PHS addresses 1st issue but password policy would be inherited from On-prem (Entra ID policy is redundant in this PHS scenario).

upvoted 1 times

□ **jt2214** 5 months, 3 weeks ago

**Selected Answer: B**

What's weird is the "Majority voted" says A but you click in the discussion the "selected answer" is mostly B. I'm going with B.

upvoted 2 times

□ **EEMS700** 5 months, 3 weeks ago

**Selected Answer: B**

Policy must be set in Active Directory

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 configure password protection in the Azure AD tenant.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉  **EEMS700** 5 months, 3 weeks ago

**Selected Answer: B**

Correct

pass-through will not work if AD is down.

upvoted 3 times

✉  **imlearningstuffagain** 6 months, 2 weeks ago

**Selected Answer: B**

pass-through authentication needs the on-prem domain to be available to check the credentials at signin.

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 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**

*Community vote distribution*

A (100%)

✉️  **Fran22** 2 months ago

Answer is correct.

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-password-hash-synchronization>

When password hash synchronization is enabled, the password complexity policies in your on-premises Active Directory instance override complexity policies in the cloud for synchronized users. You can use all of the valid passwords from your on-premises Active Directory instance to access Microsoft Entra services.

upvoted 2 times

✉️  **PhoenixMan** 5 months, 2 weeks ago

Correct answer I had the question in today exam

upvoted 1 times

✉️  **EEMS700** 5 months, 3 weeks ago

**Selected Answer: A**

Answer is correct

upvoted 2 times

✉️  **Vincent1966** 7 months, 3 weeks ago

The Default Domain Policy should only set the following: Password Policy. Domain Account Lockout Policy. Domain Kerberos Policy

upvoted 2 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

店铺：学习小店66

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 with three items: User1, User2, and User3. The menu has a small downward arrow icon at the top right.

Configure Azure AD Connect Health settings:

A dropdown menu with three items: User1, User2, and User3. The menu has a small downward arrow icon at the top right.

**Answer Area**

店铺：学习小店66

店铺：学习小店66

View sync errors in Azure AD Connect Health:

A dropdown menu with three items: User1, User2, and User3. The item User2 is highlighted with a black rectangular box.

Correct Answer:

Configure Azure AD Connect Health settings:

A dropdown menu with three items: User1, User2, and User3. The item User1 is highlighted with a black rectangular box.

cb0900 Highly Voted 7 months, 3 weeks 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 21 times

imlearningstuffagain 6 months, 2 weeks ago

Source at Microsoft Site.

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-health-operations#roles>

upvoted 3 times

Fran22 Most Recent 2 months ago

Only there are 3 roles for Microsoft Entra Connect Health.

Owner, Contributor and reader, and they can see all information

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-health-operations>

upvoted 1 times

SabicomSistemi 3 months, 3 weeks ago

CHATGPT:

1) View sync errors in Azure AD Connect Health: User2 or User3. User2 is a contributor for Azure AD Connect Health, which means they have access to view the health data and alerts for the service instances1. User3 is an application administrator in Azure AD, which means they have the Microsoft.EntraConnectHealth/read permission that allows them to view the health data and alerts for all service instances2.

2) Configure Azure AD Connect Health settings: User3. User3 is an application administrator in Azure AD, which means they have the Microsoft.EntraConnectHealth/write permission that allows them to configure the settings for the service instances2. User2 does not have this permission, and User1 is the Azure AD Connect sync account, which is not related to Azure AD Connect Health3.

upvoted 1 times

Festus365 5 months ago

View sync errors = User 1(Azure AD connect sync account)

Configure AADConnect health settings = User 2(Role: Contributor)

upvoted 1 times

NrdAlert 5 months, 4 weeks ago

I think the first account is supposed to be Azure AD Connector Account which wouldn't have rights to what they're asking about. Its purpose is strictly to write exports to Azure AD.

upvoted 2 times

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**

*Community vote distribution*

D (100%)

✉️  **TonyManero** 1 week ago

**Selected Answer: D**

In a conditional access policy you can set a location  
upvoted 1 times

✉️  **DiligentSam** 7 months ago

correct  
upvoted 1 times

✉️  **Paul\_white** 7 months 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**

*Community vote distribution*

A (100%)

✉  **oopspruu** 1 week, 4 days ago

**Selected Answer: A**

The section where you choose which OUs to sync is called "Domain and OU Filtering". The option is a big ambiguous. Technically it is a filtering setting so it can count as A.

upvoted 1 times

✉  **Fran22** 2 months ago

The correct answer is A: Filtering options: Organizational unit (OU)  
<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-configure-filtering>  
Filtering options: Group-based, Domain-based, Organizational unit (OU)-based and Attribute-based

upvoted 1 times

✉  **SBGM** 3 months, 4 weeks ago

**Selected Answer: A**

Just checked, the OU selection menu is called 'Domain/OU Filtering' so I guess that counts as Filter.

upvoted 1 times

✉  **EEMS700** 5 months, 3 weeks ago

**Selected Answer: A**

Would agree with A

upvoted 2 times

✉  **NrdAlert** 5 months, 4 weeks ago

**Selected Answer: A**

Just realized filters are also considered the part where you pick OU's. Oops. A it is.

upvoted 3 times

✉  **NrdAlert** 5 months, 4 weeks ago

It's A simply because a filter is meant to be exclusive, not inclusive. Given all users except a single OU are syncing, it's not the culprit, unless, technically, someone created a group and added all users to it except people from the OU(very unlikely as that's not the point).  
upvoted 2 times

□ **NrdAlrt** 5 months, 4 weeks ago

I meant B.

upvoted 1 times

□ **jt2214** 6 months, 3 weeks ago

**Selected Answer: A**  
<https://www.examtopics.com/discussions/microsoft/view/59313-exam-ms-100-topic-3-question-22-discussion/>  
upvoted 2 times

□ **Paul\_white** 7 months ago

ANSWER IS A !!!!!

upvoted 1 times

□ **Sas2003** 7 months, 2 weeks ago

**Selected Answer: A**  
No error just remove filtering or U exclusion  
upvoted 4 times

□ **jakke91** 7 months, 2 weeks ago

A indeed

<https://www.examtopics.com/discussions/microsoft/view/59313-exam-ms-100-topic-3-question-22-discussion/>  
upvoted 2 times

□ **vercracked\_007** 7 months, 3 weeks ago

Should this nog be A?

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-sync-configure-filtering>  
upvoted 4 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

店铺: 学习小店66

<input type="checkbox"/>	Admin name	Last sign-in	Scope
<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

店铺: 学习小店66

#### Statements

User1 can reset the password of User3.

Yes

No

Correct Answer:

User2 can reset the password of User3.

Yes

No

User2 can reset the password of User1.

Yes

No

✉ **VikC** 6 months, 3 weeks 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 11 times

✉️ **NrdAlert** 5 months, 4 weeks ago

Good point, thanks.  
upvoted 1 times

✉️ **ITCALegends** 5 months, 1 week ago

by your logic then user 2 would also be no  
upvoted 2 times

✉️ **aleksdj** Highly Voted 5 months, 1 week ago

YES  
User1 can reset password of User3 because User1 is User Administrator Organization and User3 is direct member of AU1 which is inside Scope Organization

YES 店铺：学习小店66  
User2 can reset password of User3 because User2 is member of Group2 and Group2 has assigned role for User Administrator for Scope AU1, User3 is direct user member of AU1 店铺：学习小店66

NO

User2 can NOT reset password of User1 because both User2 and User1 are member of a role-assignable group and you cannot change a password of user in a role-assignable group  
upvoted 9 times

✉️ **TonyManero** Most Recent 3 weeks, 4 days ago

Y/Y/N  
Here the point is that: User 2 is an Admin only of the AU scope, so cannot reset password for users out of the scope.  
upvoted 2 times

✉️ **Tomtom11** 2 months, 1 week ago

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#user-administrator>  
Users with this role cannot do the following:

Cannot manage MFA.  
Cannot change the credentials or reset MFA for members and owners of a role-assignable group.  
Cannot manage shared mailboxes.  
upvoted 1 times

✉️ **Ranger\_DanMT** 7 months 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 3 times

店铺：学习小店66

店铺：学习小店66

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**

*Community vote distribution*

A (100%)

✉️  **de0e20a** 5 days, 5 hours ago

I think the trick here is that the test questions has not stated that these groups are role assignable. If you do not do this at the creation of the group then "isAssignableToRole" is automatically set to false and no role is applied or can be applied to the group afterwards as this setting cannot be changed once the group is created. So we are meant to assume that the role was never added to the group because its the AU that is giving the role not the groups listed in the first section.

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept>  
upvoted 1 times

✉️  **benpatto** 5 months, 1 week ago

**Selected Answer: A**

A due to least privilege  
upvoted 2 times

✉️  **Paul\_white** 7 months ago

SECURITY READER  
upvoted 1 times

✉️  **DiligentSam** 7 months, 2 weeks ago

Should be A  
upvoted 1 times

✉️  **cb0900** 7 months, 2 weeks 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:

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:

User2 only  
**User3 only**  
User1 and User3 only  
User2 and User3 only  
User1, User2, and User3

店铺：学习小店66

店铺：学习小店66

✉  cb0900  7 months, 2 weeks ago

Answers are correct.

Reset pwd of User4: User1 and User3

Modify value or User4: User3

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

Community vote distribution

C (100%)

✉  Vaerox 3 months, 3 weeks ago

**Selected Answer: C**

MS Authenticator app is the way to go if you want to go passwordless when taking into consideration that both devices must be supported.  
upvoted 1 times

✉  DiligentSam 7 months, 2 weeks ago

I think The MS recommend MFA by using Authenticator App  
upvoted 2 times

✉  cb0900 7 months, 2 weeks 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.

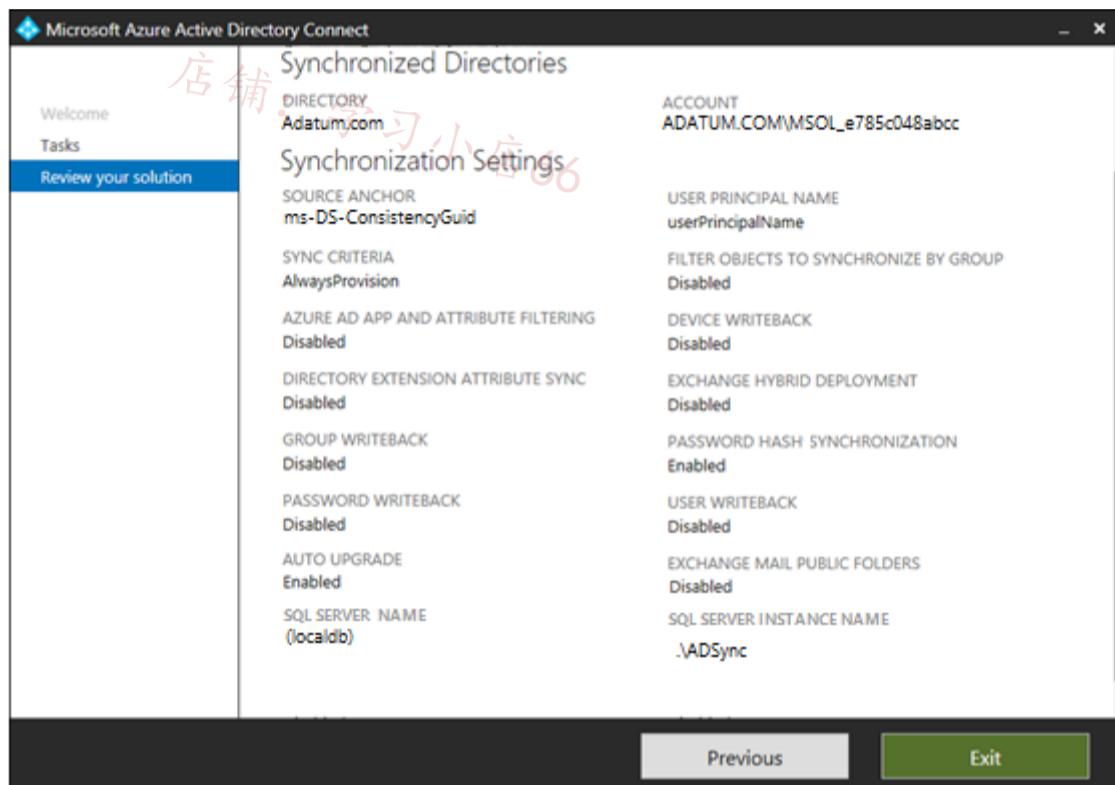
<https://www.examtopics.com/discussions/microsoft/view/81291-exam-ms-100-topic-5-question-73-discussion/>  
upvoted 4 times

**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

✉ **sergioandreslq** Highly Voted 6 months, 1 week ago

Box 1: Cannot change her password from any Microsoft Portal:

Password writeback is disabled, if the user changes the password in cloud services, the new password will be overridden in the next Azure AD connect sync process with the password in Active directory.

Box 2: the new password hash will be synchronized to Azure AD  
if the user updates the password in AD, the new hash will be synced to AAD in the next ADSYNC.

upvoted 9 times

✉ **OliwerCiecwierz** Highly Voted 7 months, 3 weeks 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 6 times

□ **Paul\_white** 7 months ago

GIVEN ANSWER IS VERY CORRECT !!!!!!

upvoted 3 times

□ **oopspruu** Most Recent 1 week, 4 days ago

Given answers are correct.

1. Cannot change password from MS because password writeback is disabled.
2. PHS is enabled so hash of password will be synced to EID.

upvoted 1 times

□ **Vaerox** 3 months, 3 weeks ago

Given answer is correct. Password writeback is Disabled, so changing your password from the cloud will NOT be synced back to the local AD server.

upvoted 2 times

□ **ChikeAmazu** 6 months, 1 week ago

Answer is wrong

To configure the usage location for users in Azure, you need to have the appropriate permissions. The following roles can configure the usage location for users in Azure:

Groups Administrator: This role can specify the usage location property on a user 12.

Global Administrator: This role has access to all administrative features in Azure AD and can manage all aspects of users, groups, and domains 3.

To view BitLocker recovery keys in Azure AD, you need to have the appropriate permissions. The following roles can view BitLocker recovery keys in Azure:

Cloud Device Administrator

Helpdesk Administrator

Security Administrator

Global Administrator

upvoted 1 times

□ **ITCALegends** 5 months, 2 weeks ago

what the hell are you on about

upvoted 10 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 Admin1 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 ⓘ

店铺

店铺：学习小店66

### 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 ⓘ

店铺

店铺：学习小店66

## 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:

店铺：学习小店66

✉  **Amir1909** Highly Voted 2 months, 4 weeks ago

- Cloud Device Administrator
  - Licence Administrator
- upvoted 11 times

✉  **OliwerCiecwierz** Highly Voted 7 months, 3 weeks 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 7 times

✉  **Jamesat** Most Recent 1 week ago

I think I agree with this.

Cloud Device Admin would allow disabling and deleting of devices from Entra ID. Helpdesk Admin would therefore by least privileged as it can only reset passwords.

Hard as is deleting accounts less privileged than password resets? Hmmm  
upvoted 2 times

✉  **oopspruu** 1 week, 4 days ago

The key here is Least privileged role.  
1. Cloud Device Admin is least privileged for Bitlocker keys.  
2. License Admin for usage location.

upvoted 1 times

✉  **Motanel** 2 weeks, 4 days ago

Cloud Device Admin is the least privilege role for viewing Bitlocker keys:

店铺：学习小店66

□ **OwerGame** 1 month, 2 weeks ago

I guess Helpdesk Admin is less privileged than Cloud device admin  
upvoted 1 times

□ **Vaerox** 3 months, 3 weeks ago

Are we sure that it's Helpdesk Administrator?

Cloud Device Administrator:

Users in this role can enable, disable, and delete devices in Microsoft Entra ID and read Windows 10 BitLocker keys (if present) in the Azure portal.  
upvoted 3 times

□ **Kmkz83510** 4 months, 2 weeks ago

I think the first answer is a tossup between Intune Admin and HelpDesk Admin. Yes, if you compare them via the M365 admin portal, Intune Admin has more checkboxes, but could one argue that Intune Admin is less privilege since it's only scoped to devices?

店铺: 学习小店66  
Agree with answer 2 - License Admin.

upvoted 1 times

店铺: 学习小店66

□ **OwerGame** 1 month, 1 week ago

Bro the amount of reach that Intune admin has compared to Cloud device and Helpdesk admin is clearly beyond your grasp. If You don't work in the industry, I can suggest that You setup that free tenant and join all Your spare/old devices/vm's. Good luck anyway.  
upvoted 1 times

□ **Bouncy** 2 months, 3 weeks ago

Claiming that Cloud Device Administrator is less privileged due to its device scope sounds valid. Intune Admin not so much, way too powerful...  
upvoted 2 times

□ **NrdAirt** 5 months, 4 weeks ago

correct, see <https://practical365.com/license-admin-role-and-other-improvements-in-azure-ad-administration/> for confirmation a license admin can set usage location in azure ad.  
upvoted 2 times

□ **DiligentSam** 7 months, 2 weeks ago

correct  
upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

**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 ✓

**Assignments**

Users or workload identities ⓘ

All users

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

**Access controls**

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

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****Exclude** None All users Select users and groups

⚠ 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.

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

Assignments

Users or workload identities ①

All users

Cloud apps or actions ①

No cloud apps, actions, or authentication contexts selected

Conditions ①

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 ①

0 controls selected

Session ①

0 controls selected

Enable policy

Report-only

On

Off

Correct Answer:

o oopspruu 1 week, 4 days ago

Given answer is correct.

You will add app in Cloud apps section, and Grant is required to enforce MFA, and then policy needs to be Enabled.

upvoted 1 times

cb0900 7 months, 2 weeks ago

The given answer is correct:

1. Add the app in Cloud Apps
2. Require MFA in Grant
3. Enable the policy

upvoted 4 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**

*Community vote distribution*

C (100%)

✉  **Amir1909** 2 months, 4 weeks ago

C is correct

upvoted 1 times

✉  **Vaerox** 3 months, 1 week ago

**Selected Answer: C**

Answer given seems correct. Take a look at this article:

<https://www.petervanderwoude.nl/post/conditional-access-and-named-locations/>

"

Named locations is a feature of Azure AD that enables administrators to label trusted IP address ranges in their organizations. In the environment, administrators can use named locations in the context of the detection of risk events to reduce the number of reported false positives for the Impossible travel to atypical locations risk event type.

"

upvoted 2 times

✉  **Festus365** 5 months, 2 weeks ago

Can I get more evidence to this answer C: named locations

upvoted 1 times

✉  **coyoteee** 5 months, 2 weeks ago

he add corporate network address as C: named locations and i guess user login from that address more oftne so user doest trigger the high risk sign in

upvoted 1 times

✉  **862e76c** 7 months, 2 weeks 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**

*Community vote distribution*

A (100%)

店铺：学习小店66

✉️  **Demonster** Highly Voted 7 months, 3 weeks ago

**Selected Answer: A**

<https://admin.microsoft.com/Adminportal/Home#/Contact>  
upvoted 10 times

✉️  **Amir1909** Most Recent 2 months, 4 weeks ago

A is correct  
upvoted 2 times

✉️  **2dwarf** 5 months, 1 week ago

You can add it in Exchange portal aswell  
upvoted 3 times

✉️  **poesklap** 6 months, 1 week ago

**Selected Answer: A**

The Microsoft 365 admin center is the portal where you can manage various aspects of your Microsoft 365 subscription, including creating mail-enabled contacts. The other options (B, C, and D) are not typically used for creating mail-enabled contacts.  
upvoted 3 times

✉️  **Darekms0** 6 months, 3 weeks ago

**Selected Answer: A**

A definitely  
upvoted 4 times

✉️  **Vincent1966** 7 months, 3 weeks ago

A: <https://admin.microsoft.com/#/Contact>  
upvoted 4 times

✉️  **vercracked\_007** 7 months, 3 weeks ago

Should be A  
upvoted 4 times

店铺：学习小店66

**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

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

## 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

Correct Answer:

店铺：学习小店66

店铺：学习小店66

User3:

Email address only  
Phone number only  
Security questions only  
Phone number and email address

✉️ **Casticod** Highly Voted 7 months, 4 weeks 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 13 times

✉️ **oopspruu** Most Recent 1 week, 4 days ago

Admin accounts are enforced to have at least 2 methods setup for SSPR and cannot use Security Questions.

upvoted 1 times

店铺：学习小店66

店铺：学习小店66

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**

*Community vote distribution*

AD (100%)

✉️  **poesklap** 6 months, 1 week ago

**Selected Answer: AD**

A. Password Hash Synchronization: This option minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources by synchronizing password hashes to Azure AD.

D. Enable single sign-on: This option helps minimize the number of times users are prompted for credentials by providing single sign-on capabilities.

Options B (Password writeback), C (Directory extension attribute sync), and E (Pass-through authentication) do not directly address the specific requirements mentioned in the scenario.

So, the correct options are A and D.

upvoted 4 times

✉️  **Bouncy** 2 months, 2 weeks ago

Correct answer, wrong explanation.

A. PHS fulfills the requirements for "Supports the use of Azure AD Identity Protection" and specifically its Leaked Credential Protection feature. This is unrelated to SSO

upvoted 3 times

✉️  **Paul\_white** 7 months ago

ANSWER IS A & D

upvoted 2 times

✉️  **Vincent1966** 7 months, 3 weeks 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 2 times

✉️  **sergioandresiq** 6 months, 1 week ago

And SSO reduces the number of times that the users need to ingest credentials.

upvoted 1 times

✉️  **Vincent1966** 7 months, 3 weeks ago

Must be A and D: SSO  
upvoted 10 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

## HOTSPOT

Your network contains an Active Directory domain and an Azure AD tenant.

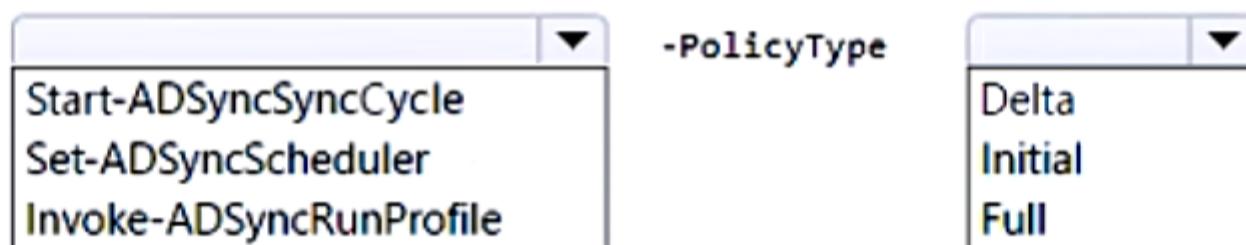
You implement directory synchronization for all 10,000 users in the organization.

You automate the creation of 100 new user accounts.

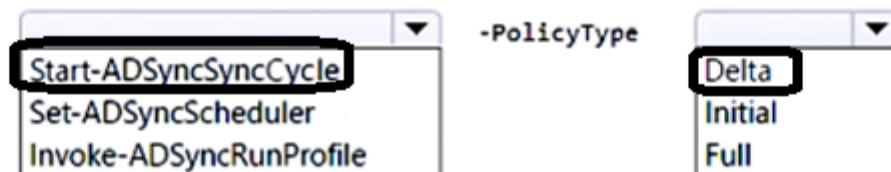
You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.

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:**



✉ **DiligentSam** Highly Voted 7 months, 2 weeks ago

It's correct

I often type this cmdlet. trust me

upvoted 10 times

✉ **Bouncy** 2 months, 2 weeks ago

You know you can simply put in a batch to avoid typing it, right?

upvoted 3 times

✉ **cb0900** Highly Voted 7 months, 2 weeks ago

Answer is correct.

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

upvoted 5 times

✉ **oopspruu** Most Recent 1 week, 1 day ago

If you work with hybrid AAD, you know this cmd by heart lol

If someone didn't know it or needs looking up to confirm if its true, stay away from this exam. Might be too advanced for you.

upvoted 1 times

✉ **Tomtom11** 2 months ago

It could be that you have an urgent change that must be synchronized immediately, which is why you need to manually run a cycle.

If you need to manually run a sync cycle, then from PowerShell run Start-ADSyncSyncCycle -PolicyType Delta.

To initiate a full sync cycle, run Start-ADSyncSyncCycle -PolicyType Initial from a PowerShell prompt.

Running a full sync cycle can be very time consuming, read the next section to read how to optimize this process.

upvoted 1 times

✉️ **Vaerox** 3 months, 2 weeks ago

The answer given is correct. This cmdlet forces Entra Connect sync to create the new users (Delta = What changed since the last sync) in the Entra ID tenant.

upvoted 2 times

✉️ **Paul\_white** 7 months ago

ANSWER IS CORRECT

upvoted 2 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

## 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



**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"/>

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** Highly Voted 7 months ago

1 - Y (registered and in scope)  
2 - N (out of scope)  
3 - N (unregistered but in scope)

upvoted 7 times

✉  **Jamesat** Most Recent 1 week ago

This has got to be

1 - Y Authenticator App Installed and in scope  
2 - Y Authenticator App Installed and as per the banner ALL users of Authenticator can have number matching NOT JUST PASSWORDLESS  
3 - N Authenticator App Not Installed.

Think people are getting confused by the mentioning of Passwordless.

upvoted 2 times

✉  **OwerGame** 1 month, 1 week ago

Number matching is not used only for passwordless, it's used also alongside MFA confirmation. My guess here would be that Users one and two can use number matching, and user 3 since there's an auth method lacking (he has Authenticator app, but it's not added as a method) Not eligible for numbers matching.

upvoted 1 times

✉  **AAlmani** 3 months ago

under the user table it says: (Each user has a device with the Microsoft Authenticator app installed.) and MFA settings shows that passwordless sign in configured to Group 1.

Based on the details here (<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-passwordless-phone#:~:text=To%20change%20the%20mode%2C%20for%20each%20row%20for%20Authentication%20mode%20%2D%20choose%20Any%20or%20Passwordless.%20Choosing%20Push%20prevents%20the%20use%20of%20the%20passwordless%20phone%20sign%2Din%20credentials.>)

The answer should be: No No Yes

upvoted 1 times

✉  **Vaerox** 3 months, 1 week ago

This is a dangerous one. It asks you for "number matching" but it shows you a screenshot of Password less settings. This is not exactly the same. The Authenticator app with Push setting will ask you to perform number matching as of september 2023.

It's gotta be Y Y N.

upvoted 1 times

✉  **faeem** 7 months, 1 week 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** 7 months, 2 weeks ago

I think answer is correct. User 2 is not in group 1 for passwordless. Thoughts?

upvoted 1 times

✉  **ExamCheater1993** 7 months, 2 weeks ago

Shouldn't this be YYN ?

upvoted 2 times

✉  **60ed5c2** 6 months ago

I thought the same thing. Because it is only being forced for group 1 it doesn't mean it can't be used for group 2. It is capable and registered so they could use it - they just aren't forced to use it.

upvoted 2 times

✉  **NrdAlert** 5 months, 4 weeks ago 

This part they are configuring doesn't force it, it enables Authenticator and passwordless to be used as factor period. Although Microsoft enabled number matching for all Authenticator users by default as of May 2023.

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 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>

店铺: 学习小店66

Users:

- Admin1 only
- Admin1 and Admin3 only**
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Blade:

- Reports
- Service Health**
- Message center

店铺: 学习小店66

#### Correct Answer:

Blade:

- Reports
- Service Health**
- Message center

✉  **Demonster** Highly Voted 7 months, 3 weeks ago

All admins of Litware can view Service health

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

upvoted 14 times

✉  **Greatone1** Highly Voted 6 months, 3 weeks ago

Answer: Admin1, Admin2, Admin3, Admin4 and Service Health

All can view the service Health Blade.

upvoted 6 times

✉  **Jamesat** Most Recent 1 week ago

It should be ALL admins.

All have access to view Service Health via the Service Health Blade.

upvoted 1 times

✉  **mickey88** 4 months, 2 weeks ago

Note

People who are assigned the global admin role can view service health, as well as people assigned to other admin roles such as Service Support admin and Helpdesk admin. For more information about roles that can view service health, see About admin roles.

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

upvoted 2 times

✉  **NrdAlert** 5 months, 4 weeks ago

They all can. Just looked up each role and they all say in text they can see service health which makes sense since it's not a secret based on your role, just something only admins need to worry about.

upvoted 2 times

✉  **Greatone1** 6 months, 3 weeks ago

<https://www.examtopics.com/discussions/microsoft/view/81381-exam-ms-100-topic-8-question-3-discussion/>

upvoted 1 times

✉  **rfree** 6 months, 3 weeks 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

✉  **JensV** 7 months, 3 weeks 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

*Community vote distribution*

C (100%)

✉️  **poesklap** 6 months, 1 week ago

**Selected Answer: C**

The Live Response Session feature allows you to interactively run scripts and collect forensic information on the device. This option will give you the capability to execute PowerShell scripts and perform other live investigation actions on the device.

upvoted 3 times

✉️  **Vincent1966** 7 months, 3 weeks 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>	Managers
<b>Description</b>		If the email is sent to: IrvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com
<b>Applied to</b>		Except if the email is sent to member of: test1ww@M365x289755.onmicrosoft.com
		<a href="#">Edit</a>
<b>Impersonation</b>	<b>Users to protect</b>	On - 3 User(s) specified
	<b>Protect all domains I own</b>	On
	<b>Protect specific domains</b>	On - 2 Domain(s) specified
	<b>Action &gt; User impersonation</b>	Move message to the recipients' Junk Email folders
	<b>Action &gt; Domain impersonation</b>	Delete the message before it's delivered
	<b>Safety tips &gt; User impersonation</b>	<a href="#">Edit</a>
	<b>Safety tips &gt; Domain impersonation</b>	Off
	<b>Safety tips &gt; Unusual characters</b>	Off
	<b>Mailbox intelligence</b>	Off
<b>Spoof</b>	<b>Enable antispoofing protection</b>	On
	<b>Action</b>	Quarantine the message
<b>Advanced settings</b>	<b>Advanced phishing thresholds</b>	3 - More Aggressive
		<a href="#">Edit</a>

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

To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].

- 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

To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].

- Domain impersonation
- Enable antispoofing protection
- Mailbox intelligence

 Festus365 Highly Voted 6 months ago

I think the second one answer should be Enable Anti-spoofing protection because the MAILBOX INTELLIGENCE is off on the configuration box upvoted 6 times

 Vaerox 3 months, 2 weeks ago

If you look closely at the image, you can see that Anti-spoofing protection is already set to "On". The best answer I think is still to enable Mailbox Intelligence (because it is not turned on).

upvoted 3 times

✉️ 🚩 **TonyManero** 3 weeks, 3 days ago

I agree with Vaerox because the Anti-spoofing is already enabled!

upvoted 1 times

✉️ 🚩 **NrdAlert** 5 months, 4 weeks ago

I agree. This is confusing. Mailbox Intelligence is another layer of impersonation protection that operates at the client level. Turning it on you can configure what it does, but it won't necessarily reduce false positives given what is already in place. More likely, you need to loosen up your anti-spoofing.

upvoted 1 times

✉️ 🚩 **benpatto** Most Recent ⓘ 5 months, 1 week ago

We had this previously after changing our domain name from example.co.uk to exampleplus.co.uk - After thorough discussions with Microsoft, the only options are the allow for trust to be built, which relies on mailbox intelligence. So 2. is correct - Mailbox intelligence.

upvoted 3 times

✉️ 🚩 **Festus365** 5 months, 2 weeks ago

Answer for the second box is correct! MAILBOX INTELLIGENCE

Enable intelligence based impersonation protection: This setting is available only if Enable mailbox intelligence is on (selected). This setting allows mailbox intelligence to take action on messages that are identified as impersonation attempts. You specify the action to take in the If mailbox intelligence detects an impersonated user setting on the next page.(I'm sorry for my previous comment after series of research I was able to get it right lol)

upvoted 3 times

✉️ 🚩 **cb0900** 7 months, 2 weeks ago

Answers look correct.

<https://www.examtopics.com/discussions/microsoft/view/71890-exam-ms-101-topic-3-question-5-discussion/>

upvoted 3 times

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**

*Community vote distribution*

D (65%)

C (35%)

 **cb0900** Highly Voted 7 months, 2 weeks 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 15 times

 **poesklap** 6 months, 1 week ago

While it's possible to configure the global settings to adjust the notification time frame, it's a broad change that would affect all policies and may not be the best approach if you want to make changes specifically for email recipients to be notified within 24 hours.

upvoted 1 times

 **Thomasname** Most Recent 2 months, 1 week ago

**Selected Answer: C**

C is Correct.

quarantine policy is preferred.

Otherwise, to turn on quarantine notifications in quarantine policies, you need to create and configure a new quarantine policy.

Admins can also use the global settings in quarantine policies to customize quarantine notifications in the following ways...

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-quarantine-notifications?view=o365-worldwide>

upvoted 2 times

 **Amir1909** 2 months, 4 weeks ago

D is correct

upvoted 1 times

 **benpatto** 5 months, 1 week ago

In this case, I would say D just because it's very broad and uses 'all recipients'. If it said only one group of a large business were affected, then I would go C.

upvoted 1 times

 **NrdAlert** 5 months, 4 weeks ago

**Selected Answer: C**

It does repeatedly say "the email recipients" which isn't the same as all email recipients or all users. Sounds like a trick question based on very slight differences in words.... again.

upvoted 2 times

 **poesklap** 6 months, 1 week ago

**Selected Answer: C**

By adding a custom quarantine policy, you can define specific actions, including the notification time frame, for quarantined messages. This allows you to customize the notification process according to your requirements.

upvoted 4 times

 **re\_zen** 2 months, 2 weeks ago

Admins can also use the global settings in quarantine policies to customize quarantine notifications in the following ways:

Add translations in up to three languages.

Customize the sender and logo that's used in the notification.

Notification frequency (every four hours, daily, or weekly).

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-quarantine-notifications?view=o365-worldwide>  
upvoted 1 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**

*Community vote distribution*

B (80%)

C (20%)

✉️  **JMB7448** 1 month ago

**Selected Answer: B**

Answer is correct, tested in lab environment.

see:

<https://www.examtopics.com/discussions/microsoft/view/93909-exam-ms-101-topic-2-question-119-discussion/>

Defender for Cloud Apps > Control > Policies > select "Activity from suspicious IP addresses" policy > go to Alerts section and set up email alert  
upvoted 4 times

✉️  **msmamrs** 1 month, 2 weeks ago

**Selected Answer: C**

should be C

upvoted 1 times

✉️  **vogs7** 2 months, 1 week ago

C - incident notification rule. Risky sign in is not available under alert policy

upvoted 3 times

✉️  **Paul\_white** 7 months 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**

*Community vote distribution*

B (100%)

✉️  **TonyManero** 3 weeks, 3 days ago

**Selected Answer: B**

Reference:

<https://learn.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

upvoted 1 times

✉️  **Kmkz83510** 4 months, 2 weeks ago

Agree with given answer.

<https://learn.microsoft.com/en-us/microsoft-365/solutions/manage-devices-with-intune-monitor-risk?view=o365-worldwide#monitor-device-risk-as-a-condition-for-access>

upvoted 2 times

✉️  **Paul\_white** 7 months ago

GIVEN ANSWER IS CORRECT AS STATED!!!

upvoted 3 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

**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

**Correct Answer:****cb0900** Highly Voted 7 months, 2 weeks 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 11 times

**Vaerox** Most Recent 3 months, 2 weeks ago

Answers seem to be correct.

1. Using anti-spam policies, you can set-up an outbound anti-spam policy limiting the amount of e-mails a user is allowed to send (per day).
2. Tenant allow/block list feature allows you to add a file based on its hash.

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**

*Community vote distribution*

BC (100%)

曰  **benpatto** 5 months, 1 week ago

**Selected Answer: BC**

Agree with cb0900

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/preset-security-policies?view=o365-worldwide>  
ctrl+f for Built-in protection

upvoted 2 times

曰  **cb0900** 7 months, 2 weeks 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 4 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.



User2 can send a maximum of 50 email messages per day.

**Answer Area****Statements****Yes****No**

**Correct Answer:** User1 can send a maximum of 150 email messages per day.



User2 can send a maximum of 50 email messages per day.



✉  **Milad666**  7 months, 1 week 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 10 times

✉️  **poesklap** Highly Voted 6 months, 1 week ago

Based on the information provided and the anti-spam policies, let's evaluate the statements:

User1 can send a maximum of 150 email messages per day.

User1 is included in AntiSpam2, which has a daily message limit of 50.

User1 is not mentioned in AntiSpam1.

User1 is not a member of Group3 (as it's in the "Exclude" list in AntiSpam2).

User1 can send a maximum of 50 email messages per day (as per AntiSpam2).

Answer: No

User2 can send a maximum of 50 email messages per day.

User2 is a member of Group1, which is included in AntiSpam1.

User2 is also a member of Group2, but Group2 is excluded in AntiSpam1.

User2 is not mentioned in AntiSpam2.

User2 can send a maximum of 100 email messages per day (as per AntiSpam1).

Answer: No

So, both statements are false.

upvoted 6 times

✉️  **apokavk** 6 months, 1 week ago

User2 is a member of Group 2 which is included in AntiSpam 1, but not a member of group 3 which is excluded. So I think second answer is Yes

upvoted 3 times

✉️  **Vaerox** Most Recent 3 months, 1 week ago

Well, I guess it could be N / N:

"The priority order matters if you have the same recipient intentionally or unintentionally included in multiple policies, because only the first policy of that type (anti-spam, anti-malware, anti-phishing, etc.) is applied to that recipient, regardless of how many other policies that the recipient is included in. There's never a merging or combining of the settings in multiple policies for the recipient. The recipient is unaffected by the settings of the remaining policies of that type."

upvoted 3 times

✉️  **Christianbrivio1991** 4 months, 3 weeks ago

the correct answer must be:

1. NO

2. NO

upvoted 2 times

✉️  **TP447** 5 months, 3 weeks ago

I think the given answer is correct on the basis that the most restrictive policy would apply for User 2 (Policy 2 in this case).

upvoted 1 times

✉️  **kt\_thomas** 5 months, 3 weeks ago

I will side with the given answer on this one. Since this one is really confusing and I do not know who will create this kind of policy logic. I will just base my answer on my experience with intune policies. If I create a policy and assign it to a group then a member of a group is also added to the exclusion, the exclusion takes precedence. So the given answer here is correct in this scenario

upvoted 1 times

✉️  **NrdAlert** 5 months, 4 weeks ago

What a bad question. There's literally nothing out there that explains whether this would exclude or include a user when they are set for both on a single policy. Only thing I can find is this link with the author talking about inclusion vs exclusion with user groups in InTune and how it doesn't mix well when mixing with device groups: <https://www.petervanderwoude.nl/post/exclude-specific-groups-of-users-or-devices-from-an-app-assignment/>

Per his information though, excluded user groups take precedence over included ones when the service calculates the combined results. So Group2 does not get the first policy applied because those member would be removed from the final combined inclusion calculation. It would only apply the second one. Per this logic, the answer provided is correct assuming InTune treats user group inclusions/exclusions the same as EOF. I'm betting this is something that is consistent across services.

I could test this in a lab but I'm too busy rippling through questions :-)

upvoted 3 times

✉️  **60ed5c2** 6 months ago

I know these questions are supposed to be confusing but I find this one extra confusing. According to this - <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/how-policies-and-protections-are-combined?view=o365-worldwide> - only 1 policy is applied if a user is in two policies - and the first policy is the one that is applied. For User 2 - they are in both group 1 and group 2. Only antispam1 policy

would come into play because it is rank 0. But which takes precedence - inclusion or exclusion? Group 1 is included and Group 2 is excluded from the policy. I would guess that inclusion would take precedence because it is more restrictive? Therefore the answer would be No user B cannot send a max of 50 messages - they can send a max of 100 messages.

upvoted 2 times

✉️ **Casticod** 8 months ago

I think NO for both options.

User 1 and 2 are members of group 1. first apply the policy with the most low priority (policy 1, priority 0)

upvoted 4 times

✉️ **EM1234** 7 months 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**

*Community vote distribution*

A (100%)

✉️ **Demonster** [Highly Voted] 7 months, 3 weeks ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-about?view=o365-worldwide#quarantine-retention>  
upvoted 6 times

✉️ **DiligentSam** [Most Recent] 7 months, 2 weeks ago

correct

upvoted 2 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

店铺: 学习小店66  
Rank Recommended action

店铺: 学习小店66  
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**

曰 cb0900 Highly Voted 7 months, 2 weeks 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 7 times

曰 Amir1909 Most Recent 2 months, 4 weeks ago

A is correct

upvoted 1 times

曰 lali11 4 months, 1 week ago

Risk accepted - Security should always be balanced with usability, and not every recommendation will work for your environment. When that is the case, you can choose to accept the risk, or the remaining risk, and not enact the recommended action. You won't be given any points for this status. You can view this action in history or undo it at any time

upvoted 1 times

benpatto 5 months, 1 week ago

I know they're meant to trick you but agree with both, they made the changes and chose not to get the points. It's like winning the lottery and giving it away

upvoted 2 times

NrdAlert 5 months, 4 weeks ago

Why someone would make the recommended changes and then give up the points by choosing Risk Accepted is beyond me, but provided answer is correct. Risk Accepted would decrease the total possible points achievable and leave number of points accumulated the same.

upvoted 3 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

## 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:  Microsoft Intune

BYOD:  Integration with Microsoft Defender for Cloud

✉ aleksdj Highly Voted 5 months, 1 week ago

I don't understand how someone can agree with the given answer. Do your study before you post something.

Integration with Microsoft Defender for Cloud is designed for Windows Servers and has nothing to do with BYOD.

First answer = Intune

Second answer = Local Script

Remember this:

Devices enrolled = Intune

Devices not enrolled = Local Script

upvoted 16 times

✉ KerrAvon 2 months, 1 week ago

There are 25 BYOD - local script is limited to 10 devices

upvoted 2 times

✉ oopspruu 1 week, 4 days ago

The local script is "advised" to be used only up to 10 devices because it has different parameters and is meant to be for testing only. There is nothing stopping you from running it on 25 devices.

upvoted 1 times

👤 NrdAlert Highly Voted 5 months, 4 weeks ago

I disagree specifically with BYOD answer provided. The question is how do you extend Defender for Endpoint to these BYOD devices. Since they are not enrolled, you have no control over them. Defender for Cloud Apps is a CASB. I don't see how people walking around with BYOD PC's would be accessing anything through a CASB service and it's not endpoint protection.

I found this: <https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/microsoft-defender-for-endpoint-for-byod-devices/mp/2488318>

A locally executed script is your only option here. VDI would work if these users were forced to use VDI's from their BYOD devices, but it's not as straight forward an answer to the question.

upvoted 7 times

👤 Jamesat Most Recent 1 week ago

Surely the answer is Intune and Intune.

Local Script is support for up to 10 devices. Group Policy is out. But if you are using Intune for MDM you are likely also using it for MAM on the BYOD.

However you can't enforce a required app for BYOD only make it available so maybe the given answer is correct?

Some of these questions are just confusing.

upvoted 1 times

👤 SabicomSistemi 3 months, 3 weeks ago

chatgpt question:

You need to onboard DEVICE A and DEVICE B to Microsoft Defender for Endpoint. The solution must minimize administrative effort.  
DEVICE A

Type: Corporate

Operating system: Windows 11

Enrollment status: Azure AD-joined, Microsoft Intune-managed

DEVICE B

Type: Bring your own device (BYOD)

Operating system: Windows 11

Enrollment status: Unmanaged

What should you use to onboard each type of device?

A local script

Group Policy

Integration with Microsoft Defender for Cloud

Microsoft Intune

Virtual Desktop Infrastructure (VDI) scripts

There's only one answer for DEVICE A and DEVICE B

The answer of chatgpt:

To onboard DEVICE A, which is a Corporate device running Windows 11 and is Azure AD-joined and Microsoft Intune-managed, you can use Microsoft Intune to onboard the device to Microsoft Defender for Endpoint 12.

To onboard DEVICE B, which is a Bring your own device (BYOD) running Windows 11 and is unmanaged, you can use Integration with Microsoft Defender for Cloud to onboard the device to Microsoft Defender for Endpoint 13.

Using Microsoft Intune for DEVICE A and Integration with Microsoft Defender for Cloud for DEVICE B will minimize administrative effort 1.

upvoted 1 times

👤 Jamesat 1 week ago

People should stop posting Chat GPT answers as they are often wrong or just waffle.

Please stop posting this as it is not helpful at all.

upvoted 1 times

👤 Bouncy 2 months, 2 weeks ago

ChatGPT in its current state - old data, no Internet access - is not exactly a great companion for Azure-related tasks. Don't trust it and please don't post its answers..

upvoted 5 times

👤 lali11 4 months, 1 week ago

I'd go with 1. Intune 2. local script

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

upvoted 1 times

👤 m2L 4 months, 2 weeks ago

According to the below link,

You can also manually onboard individual devices to Defender for Endpoint by using a local script. I think that individual Device means BYOD.

Therefore answers are:

Local Script

Microsoft Intune

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

upvoted 1 times

👤 gomezmax 4 months, 2 weeks ago

To me it is: Intune In both I use it in my environment I have policy to corporate devices and another policy to BYOD

upvoted 2 times

曰  **gomezmax** 4 months, 3 weeks ago

I do Agree with aleksdj The First Answer should be Intune and the second Should be Intune

upvoted 1 times

曰  **862e76c** 7 months, 2 weeks ago

Agree with the answer

upvoted 1 times

曰  **Casticod** 8 months ago

Correct <https://techcommunity.microsoft.com/t5/microsoft-defender-vulnerability/unmanaged-device-protection-capabilities-are-now-generally/ba-p/2463796>

upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

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**

*Community vote distribution*

BD (92%) 8%

✉  **ExamCheater1993** Highly Voted 7 months, 2 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 11 times

✉  **Thomasname** Most Recent 2 months, 1 week ago

**Selected Answer: AD**

first create a web content filter policy (A) and then make an indicator (C) for the website (url) you want to filter: <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 1 times

✉  **Amir1909** 3 months ago

B and D is correct  
upvoted 1 times

✉  **Sesbri** 3 months, 2 weeks ago

I agree. Seems to be BD. <https://blog.ciaops.com/2022/01/31/custom-web-filtering-for-microsoft-defender-for-endpoint/>  
upvoted 2 times

✉  **rfree** 7 months ago

Web content filtering only seems to block Categories, not a single site. BD  
upvoted 1 times

✉  **Paul\_white** 7 months ago

BD IS THE RIGHT ANSWER  
upvoted 1 times

✉  **Ranger\_DanMT** 7 months 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

✉  **NrdAlert** 5 months, 4 weeks ago

No where in that link does it say you can specify a specific site to block. Just categories and exclusions(no inclusions).  
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.

<b>Yes</b>	<b>No</b>
<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input checked="" type="radio"/>

**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.

✉ **ninjanaja** Highly Voted 7 months, 3 weeks ago

My answer: YNN

upvoted 12 times

✉ **vercracked\_007** Highly Voted 7 months, 3 weeks ago

Should this not be YYN

two different notification rules

upvoted 9 times

✉ **Tomtom11** Most Recent 1 week, 1 day ago

<https://learn.microsoft.com/en-us/defender-xdr/configure-email-notifications>

upvoted 1 times

✉ **benpatto** 5 months, 1 week ago

<https://www.examtopics.com/discussions/microsoft/view/81762-exam-ms-101-topic-2-question-101-discussion/#>

Go to bacOn answer (roller coaster) which perfectly describes this. N/N/N

upvoted 4 times

✉ **OwerGame** 1 month, 1 week ago

bacOn 1 year, 3 months ago

Was able to get a test VM set up on my homelab and onboard it to Defender for Endpoint using script; set up two device groups and added the same machine to each and just made them check for All (I didn't want to do anything unsafe). Downloaded test EICAR\_TEST\_FILE virus (look it up, it's safe) and I got ONE notification, NOT TWO, for the alert. NNN.

upvoted 1 times

✉ **jt2214** 6 months, 3 weeks 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** 7 months 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** 6 months, 4 weeks 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 7 times

✉ **Nail** 5 months, 3 weeks ago

N,N,N makes sense. #1 rule: thou shalt never make Microsoft look bad. It would make MS look bad if a user received two alerts when they only need to get one. They are showing you the awesomeness of MS that they will not send you more alerts than are necessary. MS products are way too awesome for that!

upvoted 2 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 **Add a description** Severity **Low**

Category **Threat management** Policy contains tags **-**

---

**Create alert settings**

Conditions **Activity is FileMalwareDetected** Aggregation **Aggregated**

Scope **All users** Threshold **20**

Window **2 hours**

---

**Set your recipients**

Recipients **User1@sk220912outlook.onmicrosoft.com** Daily notification limit **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

店铺：学习小店66

店铺：学习小店66

### 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

5  
12  
20  
100

Correct Answer:

The maximum number of email messages that Policy1 will generate per day is [answer choice].

✉  ninjanaja  7 months, 3 weeks ago

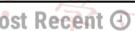
I think  
"Onedrive and Sharepoint Only" and "12"  
upvoted 13 times

✉  Casticod  8 months 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 6 times

✉  Casticod 8 months 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 14 times

✉  Tomtom11  1 week, 1 day ago

I created an Alert Policy.  
Detected Malware in File = SharePoint or OneDrive

Threshold is when the volume of matched activities reach's a Threshold trigger an alert  
In this case 20 activities within with in 2 hours = Alert created

Daily notification limit = Number of alerts that can be created  
upvoted 1 times

✉  Tomtom11 2 months ago

Alert aggregation  
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.

upvoted 1 times

✉  Tomtom11 2 months ago

<https://learn.microsoft.com/en-us/purview/alert-policies>  
upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

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**

*Community vote distribution*

D (52%)      B (48%)

✉  **siulas**  8 months ago

**Selected Answer: B**

<https://www.examtopics.com/discussions/microsoft/view/94443-exam-ms-101-topic-2-question-107-discussion/>  
upvoted 7 times

✉  **TonyManero**  5 days, 18 hours ago

**Selected Answer: D**

This microsoft page explain it all (unusual usage patterns):  
<https://learn.microsoft.com/en-us/defender-cloud-apps/policies-cloud-discovery#detect-unusual-usage-patterns-on-your-network>  
upvoted 1 times

✉  **1435b1b** 1 month, 3 weeks ago

**Selected Answer: D**

According to this you can in fact create alert policies in both Microsoft Purview Compliance portal AND Microsoft Defender Portal:

<https://learn.microsoft.com/en-us/purview/alert-policies?view=o365-worldwide>

However this article is more targeted towards "unusual usage patterns" which is specifically what the question is asking:

<https://learn.microsoft.com/en-us/defender-cloud-apps/policies-cloud-discovery#detect-unusual-usage-patterns-on-your-network>

D. the Microsoft 365 Defender Portal  
upvoted 3 times

✉  **Tomtom11** 2 months ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/purview/alert-policies>  
Suspicious email sending patterns detected Generates an alert when someone in your organization has sent suspicious email and is at risk of being restricted from sending email. This is an early warning for behavior that may indicate that the account is compromised, but not severe enough to restrict the user. Although it's rare, an alert generated by this policy may be an anomaly. However, it's a good idea to

upvoted 1 times

✉  **Amir1909** 3 months ago

D is correct

upvoted 2 times

✉  **m2L** 4 months, 2 weeks ago

**Selected Answer: D**

D for me

upvoted 2 times

✉  **Dahkoh** 4 months, 4 weeks ago

**Selected Answer: B**

With MS's line of thought , it seems that they want you to create the policy in Purview , manage the alerts in Defender.  
upvoted 1 times

✉  **Shuihe** 5 months, 2 weeks ago

D

<https://learn.microsoft.com/en-us/defender-cloud-apps/policies-cloud-discovery#detect-unusual-usage-patterns-on-your-network>  
upvoted 3 times

范esa1 5 months, 3 weeks ago

D. the Microsoft 365 Defender portal

The Microsoft Purview compliance portal, on the other hand, is primarily focused on data discovery, classification, and compliance related to data governance. It is not specifically designed for monitoring and alerting on usage patterns or security incidents within the Microsoft 365 environment.

Therefore, for creating a policy to trigger an alert when unusual Microsoft Office 365 usage patterns are detected, you should use the Microsoft 365 Defender portal.

upvoted 2 times

Armins 5 months, 4 weeks ago

**Selected Answer: D**

D agree

upvoted 2 times

NrdAlert 5 months, 4 weeks ago

By all accounts both B & D is equally right. The alerts are functionally the same. Without knowing the purpose for these alerts(compliance or security team focused) we can't pick one over the other. Another really bad question.

<https://learn.microsoft.com/en-us/purview/alert-policies>

You can use alert policies and the alert dashboard in the Microsoft Purview compliance portal or the Microsoft 365 Defender portal to create alert policies and then view the alerts generated when users perform activities that match the conditions of an alert policy. There are several default alert policies that help you monitor activities such as assigning admin privileges in Exchange Online, malware attacks, phishing campaigns, and unusual levels of file deletions and external sharing.

upvoted 2 times

phlegmbot 6 months ago

**Selected Answer: D**

Is this not UEBA?

upvoted 1 times

poesklap 6 months, 1 week ago

**Selected Answer: D**

it's the platform specifically designed for advanced threat protection, security, and detecting unusual usage patterns.

So, the correct answer is:

D. the Microsoft 365 Defender portal

upvoted 2 times

jt2214 6 months, 3 weeks ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide>

upvoted 1 times

Paul\_white 7 months ago

CORRECT ANSWER IS B

upvoted 1 times

DiligentSam 7 months, 1 week ago

Why not D?

upvoted 2 times

ITCALegends 5 months, 1 week ago

its recommended to create in purview and then manage alerts in defender

upvoted 1 times

店铺：学习小店

店铺：学习小店66

学习小店66

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

曰  **Tomtom11** 2 months ago

<https://learn.microsoft.com/en-us/mem/mem/analytics/overview>

Endpoint analytics is part of the Microsoft Adoption Score. These analytics give you insights for measuring how your organization is working and the quality of the experience you're delivering to your users. Endpoint analytics can help identify policies or hardware issues that might be slowing down devices and help you proactively make improvements before end-users generate a help desk ticket

upvoted 2 times

曰  **DiligentSam** 7 months ago

<https://www.examtopics.com/discussions/microsoft/view/98504-exam-ms-100-topic-2-question-85-discussion/>

upvoted 1 times

曰  **Paul\_white** 7 months ago

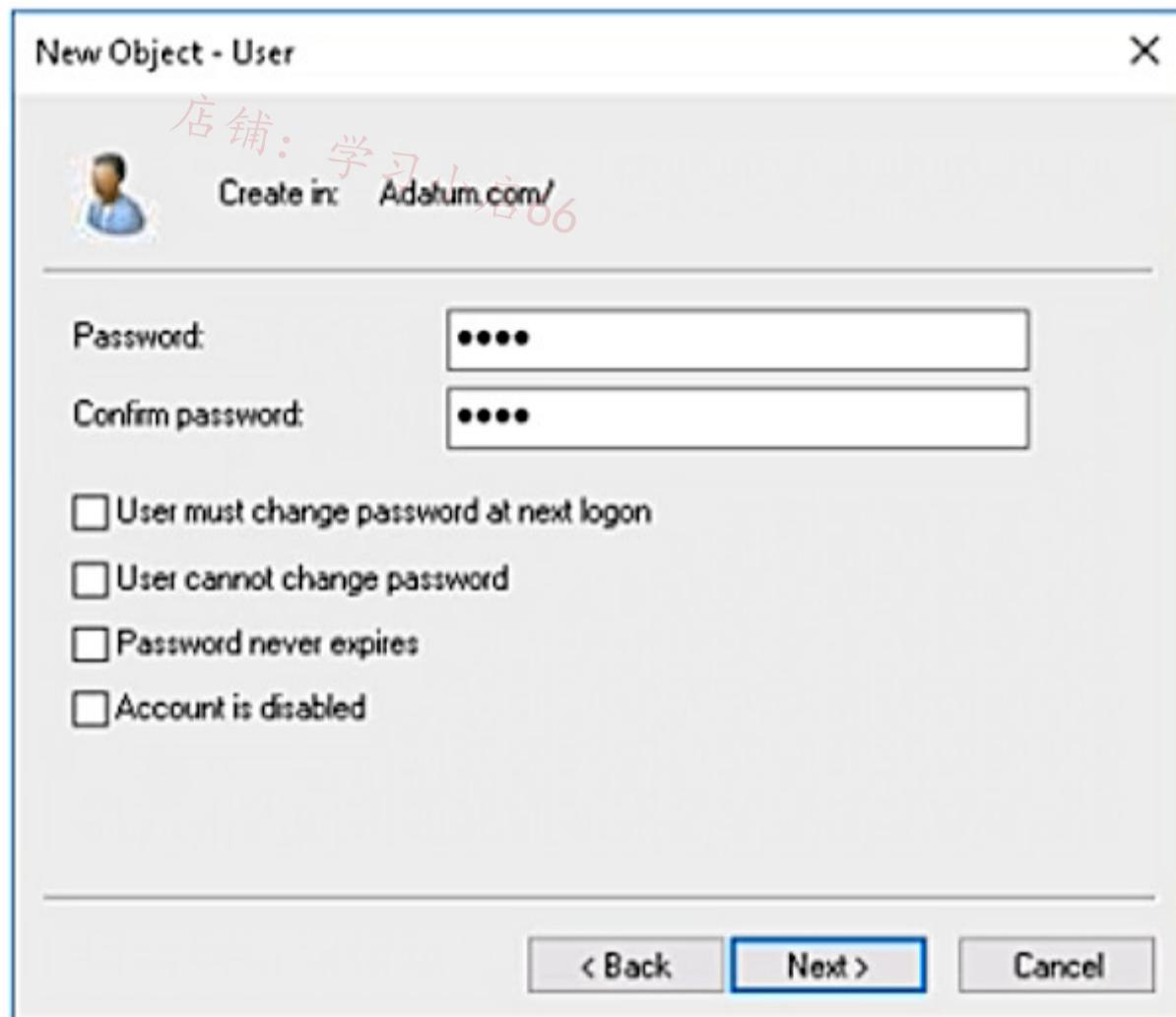
CORRECT!!!

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"/>

店铺：学习小店66

Statements	Yes	No
User1 can sign in to Azure AD.	<input checked="" type="checkbox"/>	<input type="radio"/>
User1 can change the password immediately by using the My Apps portal.	<input type="radio"/>	<input checked="" type="checkbox"/>
From Azure AD, User1 must change the password every 90 days.	<input checked="" type="checkbox"/>	<input type="radio"/>

Correct Answer:

User1 can change the password immediately by using the My Apps portal.

From Azure AD, User1 must change the password every 90 days.

店铺：学习小店66

✉  **Casticod** Highly Voted 8 months 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 22 times

✉  **ninjanaja** Highly Voted 7 months, 3 weeks ago

Because " Password writeback is disabled."

YNN

upvoted 5 times

✉  **m2L** Most Recent 4 months, 2 weeks ago

Hello,

Accordin to link below, you must enable CloudPasswordPolicyForPasswordSyncedUsersEnabled before cloud Pasword can apply to Synced User this feature is not enabled here therefore the answer is no

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-password-hash-synchronization>

upvoted 1 times

✉  **gomezmax** 4 months, 3 weeks ago

YES,NO, NO the writeback is disabled

upvoted 1 times

✉  **PhoenixMan** 5 months, 2 weeks ago

In today exam

upvoted 1 times

✉  **kt\_thomas** 5 months, 3 weeks ago

whoever created the answer to this question should be fired

upvoted 3 times

✉  **sergioandreslq** 6 months, 1 week ago

1. Yes, the user is synced.
2. No, the password must be changed in Active directory, if the user change the password in the My Apps portal, it will be overridden by the password from AD in the next ADDC sync process
3. No, The expiration period comes from Active directory, the policy to expire 90 days in Azure AD doesn't apply. For users synced from on-premises, the password policy is inherited from AD and the policies from Azure AD don't apply.

upvoted 1 times

✉  **Ranger\_DanMT** 7 months 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** 7 months ago

I misread. should be YNN

upvoted 1 times

👤 **rfree** 7 months 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** 6 months, 3 weeks ago

No as it's a hybrid environment it should be changed from AD.

upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

## 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="checkbox"/>	<input type="radio"/>
After you create the suppression rule, Alert3 is visible in the alerts queue.	<input checked="" type="checkbox"/>	<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="checkbox"/>

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 5 times

✉️  **DiligentSam** Most Recent ⓘ 7 months, 2 weeks ago

Given answers seem correct  
upvoted 2 times

✉️  **cb0900** 7 months, 2 weeks 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 4 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

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

*Community vote distribution*

A (100%)

✉  **Greatone1** Highly Voted 6 months, 4 weeks ago

Enable sensitivity labels for files in Microsoft SharePoint Online and OneDrive is the correct answer   
upvoted 6 times

✉  **cb0900** Highly Voted 7 months, 2 weeks 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 5 times

✉  **Fran22** Most Recent 2 months ago

Enable sensitivity labels for files in Microsoft SharePoint Online and OneDrive is the correct answer:  
Enable built-in labeling for supported Office files and PDF 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.  
<https://learn.microsoft.com/en-us/purview/sensitivity-labels-sharepoint-onedrive-files?view=o365-worldwide>  
upvoted 1 times

✉  **siulas** 8 months ago

**Selected Answer: A**  
<https://www.examtopics.com/discussions/microsoft/view/82514-exam-ms-101-topic-2-question-103-discussion/>  
upvoted 5 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

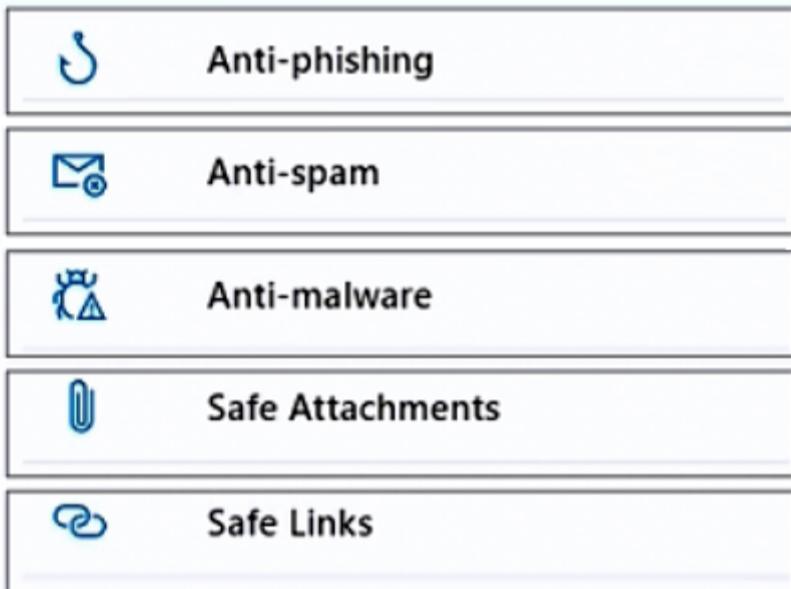
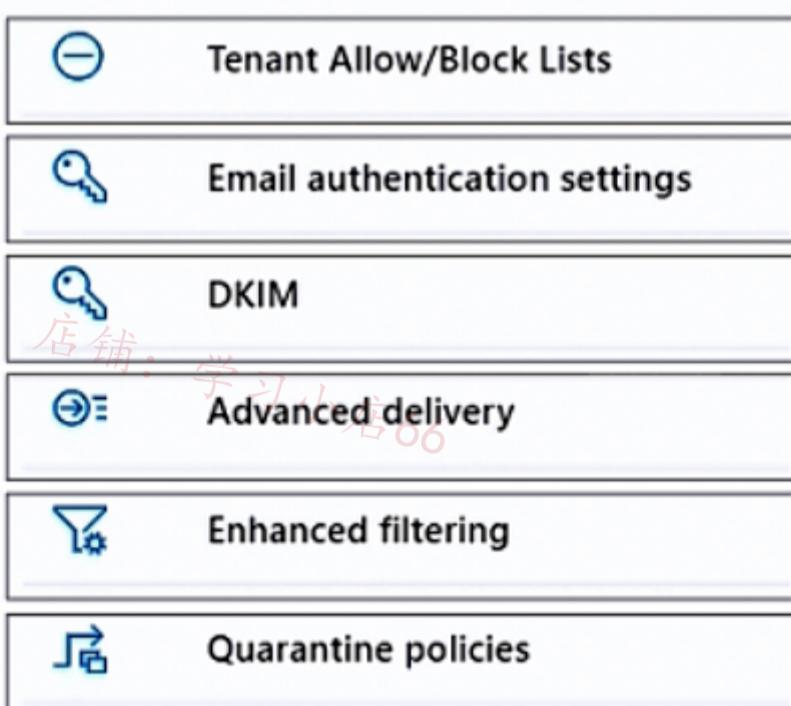
You plan to use a mailbox named Mailbox1 to analyze malicious email messages.

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

店铺: 学习小店66

店铺: 学习小店66

Correct Answer:

### Rules

-  Tenant Allow/Block Lists
-  Email authentication settings
-  DKIM
-  Advanced delivery
-  Enhanced filtering
-  Quarantine policies

siulas Highly Voted 8 months ago

Advanced Delivery  
Anti-phishing  
<https://www.examtopics.com/discussions/microsoft/view/94445-exam-ms-101-topic-2-question-111-discussion/>  
upvoted 23 times

Tomtom11 Most Recent 2 months ago

Ensure that incoming email is NOT filtered for Mailbox1

Answer is

Advanced delivery rules

Advanced delivery rules allow you to manage overrides for special system use cases. These rules allow you to specify dedicated mailboxes that are used by security teams to collect and analyze unfiltered messages that Exchange Online Protection would otherwise block. Email delivered to these mailboxes bypasses EOP and is delivered unfiltered.

upvoted 1 times

NrdAlert 5 months, 4 weeks ago

Provided answer is wrong. You need to use Advanced Delivery to allow a complete bypass of the EOP message hygiene services to a designated mailbox you specify. Spoofing protection is configured under Anti-phishing.

upvoted 2 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

## 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:

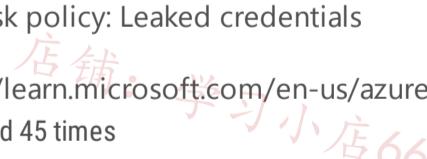
## User risk policy:

- Leaked credentials
- Malicious IP address**
- Suspicious browser

✉  **Kizzik** Highly Voted  7 months, 3 weeks 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 45 times

✉  **Fran22** 2 months ago

Correct !!!!

upvoted 2 times

✉  **Cazz123** Highly Voted  7 months 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 19 times

✉  **oopspruu** 1 week, 1 day ago

I think the goal here is to get the questions and then work/research your answers. We all know by now the answers here are mostly incorrect and site maintainers clearly never corrects them based on user discussion.

So i focus on questions, learn concept and see if I come up with same answers.

upvoted 1 times

✉  **Motanel** 2 weeks, 5 days ago

You actually pay for these questions to see, because most of them are also in the exam + you get to see the comments from people like Kizzik  
:)  
upvoted 3 times

□ **TomBoy25** 3 months, 3 weeks ago

The answers will never be perfect, but if you use it as a tool to understand the material and explain your answers you will actually understand the study material and be qualified in the real world.  
upvoted 3 times

□ **Bouncy** 2 months, 2 weeks ago

Short answer: they don't care. Long answer: still useful thanks to you guys  
upvoted 4 times

□ **Tomtom11** [Most Recent] 2 months ago

<https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#sign-in-risk-detections>

Risk types and detection

Risk can be detected at the User and Sign-in level and two types of detection or calculation Real-time and Offline. Some risks are considered premium available to Microsoft Entra ID P2 customers only, while others are available to Free and Microsoft Entra ID P1 customers.

A sign-in risk represents the probability that a given authentication request isn't the authorized identity owner. Risky activity can be detected for a user that isn't linked to a specific malicious sign-in but to the user itself.

Real-time detections might not show up in reporting for 5 to 10 minutes. Offline detections might not show up in reporting for 48 hours.  
upvoted 1 times

□ **Amir1909** 2 months, 4 weeks ago

- Atypical travel  
- Leaked credentials  
upvoted 1 times

□ **Festus365** 6 months ago

First one: Sign-in risk policy answer should be possible attempt to primary refresh token, second one: User risk policy answer should be leaked credential  
upvoted 1 times

□ **Kmkz83510** 4 months, 2 weeks ago

There should be a downvote button.  
upvoted 4 times

□ **Greatone1** 6 months, 3 weeks ago

I believe that it's worth the investment. Examtopics has helped me pass as many exams as I have fingers!!  
upvoted 2 times

□ **jt2214** 6 months, 4 weeks ago

I believe that it's worth the investment. Examtopics has helped me to successfully pass all of my exams.  
upvoted 2 times

□ **DiligentSam** 7 months, 1 week ago

Correct  
upvoted 2 times

□ **DiligentSam** 7 months, 1 week ago

I mean Kizzik's Answer is correct  
upvoted 1 times

店铺：学习小店66

店铺：学习小店66

**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  7 months, 2 weeks ago

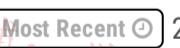
Given answers are correct.

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 8 times

✉  Tomtom11  2 months ago

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

Global settings for safe attachments is the correct answer

upvoted 1 times

✉  Tomtom11 2 months ago

Safe Attachments policy

Safe Attachments policies protect an organization from malicious content in email attachments.

They also apply to files stored in SharePoint and OneDrive and distributed through

Microsoft Teams. By default, existing policies already provide adequate protection against threats of this type. If necessary, you can create a custom safe attachments policy by performing

Is the answer not Safe Attachments policy

upvoted 1 times

✉  Fran22 2 months ago

Correct

upvoted 1 times

✉  **Amir1909** 2 months, 4 weeks ago

Correct

upvoted 1 times

Question #198

Topic 1

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

You plan to ~~automate~~ 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

*Community vote distribution*

C (100%)

✉  **Hard1k**  7 months, 4 weeks 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 5 times

✉  **Tomtom11**  2 months ago

<https://techcommunity.microsoft.com/t5/microsoft-defender-vulnerability/network-device-discovery-and-vulnerability-assessments/ba-p/2267548>

upvoted 2 times

✉  **cb0900** 7 months, 2 weeks ago

**Selected Answer: C**

<https://www.examtopics.com/discussions/microsoft/view/94572-exam-ms-101-topic-3-question-141-discussion/>

upvoted 3 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**

*Community vote distribution*

B (100%)

✉️  Hard1k Highly Voted 7 months, 4 weeks 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 6 times

✉️  Tomtom11 Most Recent 2 months ago

**Selected Answer: B**

Alert policy in Defender as this setting. I just checked  
upvoted 1 times

✉️  Amir1909 2 months, 4 weeks ago

B is correct

upvoted 1 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**

*Community vote distribution*

D (58%)      C (42%)

✉️  Hard1k  7 months, 4 weeks 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 9 times

✉️  nils241  4 months ago

**Selected Answer: D**

D: notification rule

Why? I have tried to configure it with an alert policy and have not found a way to find an activity based on an incident.

You can find activities in the alert policy like:

Common user activities (e.g. document sharing)  
Common endpoint user activities (e.g. printing)  
File and folder activities (delete file)  
File sharing activities (e.g. Share File, Folder Site)  
Filtering events (e.g. Malicious email detected)  
Common tenant activities (e.g. Insight generated)

and so on. So this is about events/activities by users and not about an event caused by an incident.

Just try it out for yourself.

upvoted 5 times

✉️  Scotte2023  5 days, 16 hours ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/defender-xdr/m365d-notifications-incidents>

Create a rule for email notifications

Follow these steps to create a new rule and customize email notification settings.

Go to Microsoft Defender XDR in the navigation pane, select Settings > Microsoft Defender XDR > Incident email notifications.

Select Add item.

On the Basics page, type the rule name and a description, and then select Next.

On the Notification settings page, configure:

upvoted 1 times

✉️  MarcMouelle 6 days, 10 hours ago

**Selected Answer: C**

politiques d'alerte vous permettent de catégoriser les alertes déclenchées par une politique, d'appliquer cette politique à tous les utilisateurs de votre organisation, de définir un niveau de seuil pour le déclenchement d'une alerte et de décider si vous souhaitez recevoir des notifications par courriel lorsque des alertes sont déclenchées

upvoted 1 times

✉️  Tomtom11 2 months ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/m365d-notifications-incidents?view=o365-worldwide>  
upvoted 2 times

✉ **Festus365** 4 months, 4 weeks ago

Notification rule is the answer with severe investigation. D  
upvoted 1 times

✉ **NrdAlert** 5 months, 4 weeks ago

Looks like both C and D could be used here. Alert policies will allow you get notifications from Defender for high severity incidents, but going with the method D is broader and easier to turn on everything quickly. Another highly ambiguous question. Thanks MSFT.  
upvoted 1 times

✉ **Greatone1** 6 months, 2 weeks ago

**Selected Answer: D**

D is the correct answer  
upvoted 1 times

✉ **rfree** 6 months, 2 weeks ago

**Selected Answer: D**

D, this does use the same language for setting up a Rule.  
"For example, if you only want to be informed about high-severity incidents, select High."

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/m365d-notifications-incidents?view=o365-worldwide>  
upvoted 3 times

✉ **jbuexamtopics** 6 months, 3 weeks ago

**Selected Answer: D**

Notification Rule

<https://www.examtopics.com/discussions/microsoft/view/94056-exam-ms-101-topic-2-question-115-discussion/>  
upvoted 2 times

✉ **agittunc** 6 months, 3 weeks ago

Check the link, it's C. not D.  
upvoted 2 times

✉ **Greatone1** 7 months ago

notification rule is the correct answer ✍  
upvoted 1 times

✉ **Blagojche** 7 months 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 2 times

店铺：学习小店66

店铺：学习小店66

Question #201

Topic 1

HOTSPOT

- 店铺: 学习小店66

You have a Microsoft 365 E5 subscription.

店铺: 学习小店66

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

店铺: 学习小店66

To view the device configuration assessment:

Add a connected application.  
**Create a baseline assessment profile**  
Filter the Vulnerable devices report.

Correct Answer:

To protect C:\Folder1, enable:

**Controlled folder access**  
Exploit protection  
Removable storage protection

✉  **Amir1909** 2 months, 4 weeks ago

Correct

upvoted 2 times

✉️ **TonyTe0** 3 months, 3 weeks ago

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide>  
upvoted 1 times

✉️ **NrdAirt** 5 months, 4 weeks ago

Looks right to me.  
upvoted 2 times

Question #202

Topic 1

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

店铺：学习小店66

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**

*Community vote distribution*

B (100%)

✉️ **cb0900** Highly Voted 7 months, 2 weeks 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 8 times

✉️ **DiligentSam** Most Recent 7 months, 2 weeks ago

Agree with cb0900  
upvoted 1 times

店铺：学习小店66

店铺：学习小店66

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**

*Community vote distribution*

C (100%)

✉️  Hard1k Highly Voted 7 months, 4 weeks 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 5 times

✉️  Tomtom11 Most Recent 19 hours, 5 minutes ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-overview?view=o365-worldwide>

upvoted 1 times

✉️  benpatto 5 months, 1 week ago

C. is literally the only viable option here. I mean if anyone picks B. I'd hold fire on taking the exam :p

upvoted 1 times

✉️  cb0900 7 months, 2 weeks ago

**Selected Answer: C**

<https://www.examtopics.com/discussions/microsoft/view/33967-exam-ms-101-topic-2-question-27-discussion/>

upvoted 2 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

店铺：学习小店66

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 8 months 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 34 times

imlearningstuffagain 6 months, 2 weeks ago

Yup:

Configuration policy, so it will know how configure

Compliance policy, so it will know what the device must meet.  
Conditional Access Policy, so you can block if needed  
upvoted 5 times

✉️ **stib** 1 month ago

Just checked in a tenant. I can create a Configuration Profile and Compliance Policy for Windows, Android, iOS and more. Then a Conditional Access policy is needed where the Grant option needs a tick in the checkbox for compliant devices.  
upvoted 1 times

✉️ **ExamCheater1993** 7 months, 2 weeks ago

I agree with this guy.  
upvoted 3 times

✉️ **DiligentSam** 7 months, 2 weeks ago

Agree with Casticod  
upvoted 1 times

✉️ **Tomtom11** Most Recent ⓘ 18 hours, 53 minutes ago

<https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection#onboard-devices-by-using-a-configuration-profile>  
upvoted 1 times

✉️ **m2L** 4 months, 2 weeks ago

For the second choice you just need a conditional access policy,  
By creating a conditional access Policy, you can filter devices by configuring the option "Device Filtering"  
upvoted 1 times

✉️ **itguys** 4 months, 2 weeks ago

You cannot configure device policies for iOS and Android - they need to be App protection policies.  
For all devices listed - just a compliance and a CA policy will fulfill the requirement.  
upvoted 1 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.

**Correct Answer:****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.

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 13 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

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**  
Retention1

**File plan descriptors**

**Retention settings**

Retention period 6 months	Retention action Retain and Delete
Edit	Edit

**Based on**  
Based on when it was created

**Create label**

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

曹甫: 学习小店66 **Paul\_white** (Highly Voted) 7 months ago

GIVEN ANSWER IS CORRECT

upvoted 6 times

**Kmkz83510** 4 months, 3 weeks ago

Agree - I couldn't find a good written explanation, but I think the left side of this flowchart explains it. <https://learn.microsoft.com/en-us/purview/retention-flowchart>

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

**Sensitive info types**

IP Address   Instance count  to

Add

+ 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

店铺：学习小店66

#### Statements

User1 can open File2.

Yes



No



User2 can open File1.

Yes



No



Admin1 can open File2.

Yes



No



Correct Answer:

Christianbrivio1991 Highly Voted 5 months, 1 week ago

my opinion is Y-Y-Y

@sigvast is right

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

upvoted 9 times

Tomtom11 Most Recent 2 months ago

Actions

Any item that makes it through the conditions filter will have any actions that are defined in the rule applied to it. You'll have to configure the required options to support the action. For example, if you select Exchange with the Restrict access or encrypt the content in Microsoft 365 locations action, you need to choose from these options:

Block users from accessing shared SharePoint, OneDrive, and Teams content

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

Block only people from outside your organization. Users inside your organization will continue to have access.

Encrypt email messages (applies only to content in Exchange)

The actions that are available in a rule depend on the locations that have been selected. The available actions for each individual location are listed below.

upvoted 1 times

SBGM 3 months, 3 weeks ago

I think this is a typical Microsoft question. A SITE admin has access to blocked files. A SharePoint admin does not. A SharePoint admin could make himself site admin, but that's not part of the question here. So I do not think the SharePoint admin can access the file.

upvoted 3 times

cpaljchc4 4 months ago

You have a Microsoft 365 E5 subscription that contains a SharePoint site named Site1.

You have a SharePoint site named Site 1.

Sorry, my logic was stucked by Microsoft exams, I could not tell whether 'You have a Microsoft 365 E5 subscription that contains a SharePoint site named Site1' is the correct logic.

upvoted 1 times

cpaljchc4 4 months ago

sorry I mean, whether SharePoint admin = site admin, as SharePoint site = site 1..

I'm totally confused with Microsoft exam logic...

upvoted 1 times

itguys 4 months, 2 weeks ago

Admin1 is 'SharePoint Admin' not 'Site Admin'

upvoted 2 times

cpaljchc4 4 months ago

If you have a SharePoint site named Site 1, then is SharePoint admin = site admin?

Sorry, I'm totally confused with Microsoft exam

upvoted 1 times

benpatto 5 months, 1 week ago

Agree with Christian, Owners & Admin can always open files if even if it says 'block everyone'  
There needs to be people who can resolve these problems, if only the 'owner' can access it, say a member of reception, they'll have no idea how to resolve. Needs an admin to resolve

upvoted 2 times

□ **cyp99** 4 months, 3 weeks ago

Sharepoint admin is not site admin so I think that Admin1 (Sharepoint admin) has no access.

upvoted 1 times

□ **OliwerCiecwierz** 6 months, 3 weeks 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 4 times

□ **sigvast** 5 months, 3 weeks 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>

upvoted 4 times

□ **Casticod** 8 months 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.

- 店铺：学习小店66**
- 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

**店铺：学习小店66**

**Correct Answer: AB**

*Community vote distribution*

AB (80%)

AF (20%)

✉ **Paul\_white** Highly Voted 7 months ago

A, B IS THE RIGHT ANSWER  
upvoted 10 times

✉ **Amir1909** Most Recent 3 months ago

A and B is correct  
upvoted 1 times

✉ **SBGM** 3 months, 3 weeks ago

**Selected Answer: AB**

I think it is AB because yes, you can use a sensitivity label for your DLP policy, but the labels themselves won't do anything in this scenario, the DLP policy prevents content from being shared externally.  
upvoted 1 times

✉ **nils241** 4 months ago

**Selected Answer: AB**

Answer: A and B  
Retains all data for 10 years: Retention Policy  
Prevents the sharing of data outside the organization: DLP Policy

For all A + F Persons:  
you dont need a sensitiv label for DLP + SharePoint and you ignore the "Retains all data for 10 years" requirement.

New DLP Policy -> Only SharePoint (maybe specific site) -> Condition: Content is shared for M365 (Detects when content is sent in email message, Teams chat or channel message, or shared in a SharePoint or OneDrive document.) -> Action: Block access  
upvoted 1 times

✉ **m2L** 4 months, 2 weeks ago

I choose  
DLP  
create a retention label  
Because you might have the retention label before making a label policy.  
You make a label policy by publishing a label.  
upvoted 1 times

✉ **Christianbrivio1991** 5 months, 1 week ago

**Selected Answer: AB**  
AB is correct  
upvoted 1 times

👤 NrdAlert 5 months, 4 weeks ago

Would be ABF if that was an option. Need a retention policy obviously for 10 yr requirement obviously, but you should create a DLP policy that looks at sensitivity labels to determine if a file should be shared externally. However sensitivity labels alone won't stop sharing without a DLP policy in place to act on them.

<https://microsoft.github.io/ComplianceCxE/notes/mip-dlp/DLP-policy-externalshare/>  
upvoted 2 times

👤 RJTW070 6 months ago

**Selected Answer: AB**

AB for sure

upvoted 1 times

👤 VikC 6 months, 2 weeks ago

**Selected Answer: AF**

1. Retention Policy
2. Sensitivity Label

<https://techcommunity.microsoft.com/t5/microsoft-365/sensitivity-labels-control-external-sharing-for-sharepoint/m-p/1970242>

upvoted 1 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?

店铺：学习小店66

店铺：学习小店66

- 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**

*Community vote distribution*

B (54%)

D (46%)

✉️  **Chapo** Highly Voted 6 months ago

Answer is D. DLP is already blocking Teams internally. To block external sharing you use the DLP rules.  
upvoted 12 times

✉️  **GeorgeMar** 3 weeks, 5 days ago

DLP policy customize access and override settings allows to Block only people outside your org  
upvoted 1 times

✉️  **AlfaExamPro** Highly Voted 7 months, 1 week ago

**Selected Answer: B**

because DLP rules talk about DLP threshold, action etc  
DLP location more specific to set up DLP scope/location  
upvoted 10 times

✉️  **TonyManero** Most Recent 3 weeks ago

**Selected Answer: B**

I think location is the most appropriate:  
<https://learn.microsoft.com/en-ie/purview/dlp-policy-reference#locations>  
upvoted 1 times

✉️  **Tomtom11** 2 months ago

**Selected Answer: B**

The Rule option is the answer. As you edit the rule by creating a condition option  
<https://learn.microsoft.com/en-ie/purview/dlp-policy-design#complex-rule-design>  
upvoted 2 times

✉️  **Craig** 2 months, 1 week ago

Hi,  
I would have to go for B as it states that one to one chats are already block. One to one chats use one drive, teams chats do not. So we know the policy is correctly configured by you need to add the Teams chat location.  
upvoted 1 times

✉️  **Vaerox** 3 months, 1 week ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/purview/dlp-microsoft-teams#recommended-dlp-policy-structure>

Everyone, please take a look at this URL. It's a condition inside a DLP rule, so the answer has to be D.  
upvoted 4 times

□ **Sesbri** 3 months, 2 weeks ago

For me it must be B. Here is my explanation:

1. Definition of locations in DLP: <https://learn.microsoft.com/en-us/purview/dlp-create-deploy-policy#policy-scope>

- We see that locations are more like a cluster for which defines the platform

2. Definition of DLP rules: <https://learn.microsoft.com/en-us/purview/dlp-create-deploy-policy#policy-scope>

- DLP rules consolidate the details of a rule. In this case the conditions are relevant. Here we can modify the actions to match the input from the question.

upvoted 1 times

□ **cpaljchc4** 4 months ago

"We need to block all sharing of SharePoint and OneDrive items to all external recipients..." - Administrative scope: Full directory

- Where to monitor: SharePoint sites, OneDrive accounts

- Conditions for a match: First Condition > Shared outside my org

- Action: Restrict access or encrypt the content in Microsoft 365 locations > Block users from receiving email or accessing shared SharePoint, OneDrive > Block only people outside your organization.

Think B is more direct to the question.

Ref:<https://learn.microsoft.com/en-us/purview/dlp-create-deploy-policy>

upvoted 2 times

店铺：学习小店66

□ **timkuo1009** 5 months ago

B is correct. Edit DLP policy->location and select sharepoint sites.

Files that you upload to a channel are stored in your team's SharePoint folder. These files are available in the Files tab at the top of each channel.

<https://support.microsoft.com/en-us/office/file-storage-in-microsoft-teams-df5cc0a5-d1bb-414c-8870-46c6eb76686a>

upvoted 3 times

□ **aleksdj** 5 months ago

**Selected Answer: D**

It is D 100%!

When you edit the policy through the Wizard, you will see that you can select the location for this policy, here you can choose to select all users or specific users, whatever option you choose it is only valid from internal to internal users, this option doesn't affect the sharing from internal to external.

Therefore you must click on "Next" and create a new "Advanced DLP Policy" rule where you can make a new condition : Content is shared from M365 > with people outside my organization.

upvoted 4 times

□ **jt2214** 5 months, 3 weeks ago

**Selected Answer: D**

I agree with Chapo - D

upvoted 3 times

□ **60ed5c2** 6 months ago

But when I look at location in my tenant you can't differentiate between teams channels and chats - it is either on or off. So if it is working for chats - it would be working for channels if the location was set. It appears that editing the policy rules you can add an additional policy to apply if shared externally. I think D is correct.

upvoted 3 times

□ **GLL** 7 months ago

Edit the Locations settings of DLP1

upvoted 2 times

店铺：学习小店66

店铺：学习小店66

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**

*Community vote distribution*

A (100%)

曰  **Greatone1**  7 months ago

Headers equals email or exchange  
upvoted 5 times

曰  **Tomtom11**  2 months ago

**Selected Answer: A**  
Selecting the location as Exchange. Is the only way to get the option for Headers in the conditions  
upvoted 2 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

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

Admin1 can view the contents of File1 by using Content explorer.

Correct Answer:

Admin2 can view the contents of File1 by using Content explorer.

店铺：学习小店66

Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.

✉ Paul\_white Highly Voted 7 months 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 9 times

✉ aleksdj 5 months ago

its` not! NNY

upvoted 1 times

✉️  **NrdAlert**  5 months, 3 weeks ago

N, N, Y

Admin1 does not have access to Content Explorer as they have not been assigned an appropriate admin role to access the tab.

<https://learn.microsoft.com/en-us/purview/data-classification-content-explorer>

In order to get access to the content explorer tab, an account must be assigned membership in any one of these roles or role groups.

Microsoft 365 role groups

Global administrator  
Compliance administrator  
Security administrator  
Compliance data administrator

upvoted 6 times

✉️  **0ef58a2** 5 months, 1 week ago

NYN

There are two roles that grant **access** to content explorer and it is granted using the Microsoft Purview compliance portal:

Content Explorer List viewer: Membership in this role group allows you to see each item and its location in list view. The data classification list viewer role has been pre-assigned to this role group.

Content Explorer Content viewer: Membership in this role group allows you to view the contents of each item in the list. The data classification content viewer role has been pre-assigned to this role group.

<https://learn.microsoft.com/en-us/purview/data-classification-content-explorer>

upvoted 8 times

✉️  **oopspruu**  1 week, 3 days ago

NNY

Only these 4 roles can see the Content Explorer tab: Global administrator  
Compliance administrator  
Security administrator  
Compliance data administrator

The other 2 roles, Content Viewer and List Viewer, don't let you access Content Explorer tab on their own. They must be added on top of the above 4 roles before you can use them with the content.

upvoted 1 times

✉️  **Tomtom11** 1 month, 4 weeks ago

Content Explorer Content Viewer View the contents files in Content Explorer.

Content Explorer List Viewer View all items in Content Explorer in list format only.

upvoted 1 times

✉️  **itguys** 4 months, 2 weeks ago

from MS:

<https://learn.microsoft.com/en-us/purview/data-classification-content-explorer>

"Membership in these role groups does not allow you to view the list of items in content explorer or to view the contents of the items in content explorer.

There are two roles that grant access to content explorer and it is granted using the Microsoft Purview compliance portal:

Content Explorer List viewer: Membership in this role group allows you to see each item and its location in list view. The data classification list viewer role has been pre-assigned to this role group.

Content Explorer Content viewer: Membership in this role group allows you to view the contents of each item in the list. The data classification content viewer role has been pre-assigned to this role group."

upvoted 2 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:

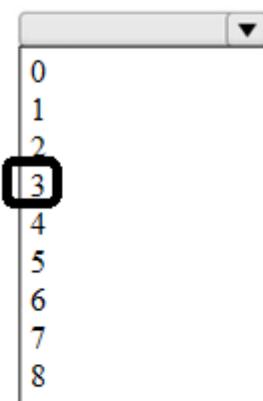
 0  
 1  
 2  
 3  
 4  
 5  
 6  
 7  
 8

User2@contoso.com:

 0  
 1  
 2  
 3  
 4  
 5  
 6  
 7  
 8

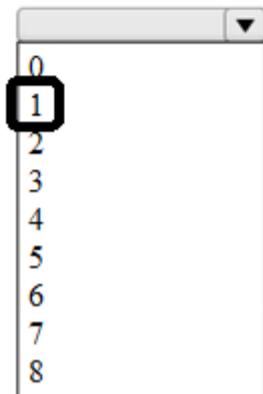
### Answer Area

User1@contoso.com:



Correct Answer:

User2@contoso.com:



店铺：学习小店66

店铺：学习小店66

□ **MvdSpoel** Highly Voted 4 months, 2 weeks ago

txt file is in scope don't get confused with sentitify label see <https://learn.microsoft.com/en-gb/exchange/security-and-compliance/mail-flow-rules/inspect-message-attachments>

Answer is 4 and 0

upvoted 6 times

□ **Wuhao** 1 week ago

4 file so 4 notification

upvoted 1 times

□ **TonyManero** Most Recent 3 weeks ago

The explanation is:

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:

Rule 1: only notifies users

Rule 2: notifies users, restricts access, and allows user overrides

Rule 3: notifies users, restricts access, and doesn't allow user overrides

Rule 4: restricts access

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 because the most restrictive rule, I think :

User1--> 4

User2--> 3

upvoted 4 times

□ **Motanel** 2 weeks, 4 days ago

only that, if txt files are not supported, then it's

- 3

- 2

upvoted 1 times

□ **Dave\_Holden** 1 week, 5 days ago

txt files are included. As are csv and pdf. Plus all of the old and new office document types, doc docx etc.

upvoted 1 times

□ **nicvig01** 3 weeks, 4 days ago

- 4

- 0

upvoted 1 times

□ **Tomtom11** 1 month, 4 weeks ago

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

upvoted 1 times

□ **Tomtom11** 1 month, 4 weeks ago

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

upvoted 1 times

✉ **Amir1909** 2 months, 4 weeks ago

- 2

- 1

upvoted 2 times

✉ **cpaljchc4** 4 months ago

Rule priority order When an item matches multiple rules in a policy and those rules have identical actions, the actions from the highest priority rule is applied.

According to the rule priority , I think User 1 - 4 , User 2 - 0 should be right?

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

upvoted 4 times

✉ **Vaerox** 3 months, 2 weeks ago

Can you explain why user 2 gets 0 notifications? There are 2 files (if you exclude TXT files) that contain 2 or more IP-addresses, so User 2 should get 2 notifications?

upvoted 3 times

✉ **sergioandresiq** 6 months, 1 week ago

I tested it in my tenant demo,

Box 1: I got 15 notifications to user1 mailbox, the answer is not there

Box 2: I got 8 notifications to user2 mailbox, I got with 8.

Why this is happening, No idea, this question was difficult to answer, that is why I created the DLP to see the results but, unfortunately, it is not clear.

Sorry team, I will just choose this one to 8-8 but in this case, it is guessing because I believe even Microsoft doesn't know.

upvoted 1 times

✉ **northgaterebel** 6 months, 1 week ago

User1 = 4. All file types are now supported. <https://learn.microsoft.com/en-us/purview/endpoint-dlp-learn-about#files-monitored-via-policy>  
User2 = 0. Agree with Paul\_white about the ranking.

upvoted 4 times

✉ **northgaterebel** 6 months, 1 week ago

Nope wrong lol. User1 = 3. Sharepoint DLP supports fewer file types than PC. <https://learn.microsoft.com/en-us/purview/sensitivity-labels-sharepoint-onedrive-files#supported-file-types>

upvoted 3 times

✉ **Kmkz83510** 4 months, 2 weeks ago

But that link is specifically for sensitivity labels. I would be shocked if txt files were not supported in Sharepoint.

upvoted 1 times

✉ **NrdAlert** 5 months, 3 weeks ago

So the DLP scanner for SPO can only scan Office documents, not txt files? So people wanting to bypass DLP in SPO can upload basic text files that anyone can open on any device. How does Microsoft not scan txt files?

upvoted 1 times

✉ **Paul\_white** 7 months 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 4 times

✉ **Greatone1** 7 months 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** 7 months, 1 week ago

i think

user 1 receive 3 notification

User2 receive 3 notification

upvoted 3 times

✉ **faeem** 7 months, 1 week ago

For user2, there are 3 files with 3 or more IP's. Why would user2 not receive 3 notifications?

upvoted 2 times

✉ **BlackCat9588** 7 months, 1 week ago

It should be 3 & 0 ?

upvoted 1 times

✉ **kavikumar** 7 months, 1 week ago

It should be 4 & 3 ..right?

upvoted 7 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**

*Community vote distribution*

D (100%)

✉ **Hard1k** Highly Voted 7 months, 4 weeks 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 7 times

✉ **Tomtom11** Most Recent 1 month, 4 weeks ago

A notification is required and not block the sharing of a file. I would go with Defender  
upvoted 1 times

✉ **nils241** 4 months ago

**Selected Answer: D**

I go to D.

Yes, you can also do it with DLP and there would be one or two arguments in favor of it:

Do I want to block access: DLP  
If I want an alert and notification: DLP, Alert Policy  
If I only want a notification, but no alert: DLP

Con DLP: I have to define 2 conditions (internal and external sharing)

Blocking access and only notifications (without alert) are not listed as a requirement and DLP would be "more difficult" to configure.

Therefore I go for Alert Policy.

upvoted 1 times

✉ **itguys** 4 months, 2 weeks ago

Data Loss Prevention.  
Yes, can be done in Defender - but its a compliance action in principle  
upvoted 1 times

✉ **60ed5c2** 6 months ago

<https://learn.microsoft.com/en-us/purview/alert-policies?view=o365-worldwide> - "You can use alert policies and the alert dashboard in the Microsoft Purview compliance portal or the Microsoft 365 Defender portal to create alert policies and then view the alerts generated when users perform activities that match the conditions of an alert policy" Because C is saying to create a DLP policy (not alert) The answer would be D.  
upvoted 1 times

✉ **sergioandreslq** 6 months, 1 week ago

The answer is C: DLP is used to notify users and auditors about data sharing intentionally or unintentionally, This portion is associated with protecting data and DLP is used for this objective.  
upvoted 1 times

✉ **jt2214** 6 months, 1 week ago

**Selected Answer: D**

Answer is D  
upvoted 1 times

✉ **Paul\_white** 7 months ago

ANSWER IS A!!!!

upvoted 1 times

□ **Paul\_white** 7 months ago

D. From the Microsoft 365 Defender portal, create an alert policy.

upvoted 1 times

□ **Greatone1** 7 months ago

A. From the Microsoft 365 Defender portal, create an alert policy

upvoted 2 times

□ **DiligentSam** 7 months, 1 week ago

Ref:

<https://www.examtopics.com/discussions/microsoft/view/94880-exam-ms-101-topic-2-question-118-discussion/>

upvoted 2 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**

*Community vote distribution*

B (89%) 11%

✉️  **ninjanaja** Highly Voted 7 months, 3 weeks ago

**Selected Answer: B**

Correct Answer

<https://www.examtopics.com/discussions/microsoft/view/68006-exam-ms-101-topic-2-question-32-discussion/>  
upvoted 8 times

✉️  **NrdAlert** Most Recent 5 months, 3 weeks ago

Documentation here confirms the answer most people have given:

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

To turn Allow or block files on:

In the navigation pane, select Settings > Endpoints > General > Advanced features > Allow or block file.

Toggle the setting between On and Off.

Select Save preferences at the bottom of the page.

After turning on this feature, you can block files via the \*\*\*\*Add Indicator\*\*\*\* tab on a file's profile page.

upvoted 3 times

✉️  **Paul\_white** 7 months 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 4 times

✉️  **Hard1k** 7 months, 4 weeks 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** 7 months ago

PLEASE STOP MISLEADING PEOPLE

upvoted 8 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**

*Community vote distribution*

B (85%) D (15%)

✉️ **Casticod** Highly Voted 8 months 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 13 times

✉️ **DiligentSam** 7 months, 1 week ago

Check it in my tenant

Role - Role assignments - Azure AD / Intune / Billing - Choosing 2 Role - click button "compare Roles"

upvoted 3 times

✉️ **Vincent1966** 7 months, 3 weeks ago

I agree B: <https://admin.microsoft.com/#/rbac/directory/compare>

upvoted 3 times

✉️ **ExamCheater1993** 7 months, 2 weeks ago

Checked it in a tenant, this guy is right.

upvoted 3 times

✉️ **stib** Most Recent 1 month ago

**Selected Answer: B**

Vincent1966 is correct.

upvoted 1 times

✉️ **dfsdf12333323123** 2 months, 2 weeks ago

Answer is B

The same question is in Microsoft 102 exam practice test which is free to take

upvoted 1 times

✉️ **Amir1909** 2 months, 4 weeks ago

B is correct

upvoted 1 times

✉️ **Sesbri** 3 months, 2 weeks ago

I agree that it can not be A. See here: <https://learn.microsoft.com/en-us/purview/purview-compliance-portal-permissions>. I'll take B also.

upvoted 1 times

✉️ **jt2214** 5 months, 3 weeks ago

**Selected Answer: B**

It's B. This tool is actually pretty useful when figuring out what roles give what permissions

upvoted 1 times

✉️  **NrdAlert** 5 months, 3 weeks ago

**Selected Answer: B**

Minimizing "administrative effort" means B over D(which would work but is not as easy)  
upvoted 1 times

✉️  **Windows311** 6 months ago

**Selected Answer: B**

Tested in my tenant, B works very well and even have Application administrator shown (ref earlier comment about App admin missing).  
upvoted 1 times

✉️  **AK\_1234** 6 months, 4 weeks ago

D- Entra Admin center

upvoted 3 times

✉️  **Greatone1** 7 months ago

Answer is Entra Admin center

<https://www.examtopics.com/discussions/microsoft/view/122192-exam-sc-300-topic-1-question-62-discussion/>

upvoted 2 times

✉️  **Hard1k** 7 months, 4 weeks 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 3 times

✉️  **smiff** 7 months, 1 week ago

yes it is possible, but when it comes to built-in comparison feature, admin center is the answer, you can try

upvoted 2 times

✉️  **sergioandresiq** 6 months, 1 week ago

Yes, Agreed, I thought at first was Microsoft Entra in the portion of roles, however, when I used the admin.microsoft.com roles and the feature of comparison, it was great how Microsoft compared each role.

Definitely, the correct answer is B.

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.

店铺：学习小店66

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

## Correct Answer:

File extension is condition:

- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

店铺：学习小店66

店铺：学习小店66

cb0900 Highly Voted 7 months, 1 week 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 5 times

1435b1b Most Recent 1 month, 3 weeks ago

Sender is condition: DLP1 only

File extension is condition: DLP1, DLP2, and DLP3

Confirmed in tenant. Answers are correct.

upvoted 2 times

Tomtom11 1 month, 4 weeks ago

I checked this in a DLP Policy and the answers are correct  
upvoted 3 times

 **DiligentSam** 7 months, 1 week ago

Correct  
upvoted 2 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

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**

*Community vote distribution*

A (100%)

✉️  **NrdAlert** 5 months, 3 weeks ago

**Selected Answer: A**

Going back to on-prem Exchange admin days, A is correct.

upvoted 1 times

✉️  **sergioandreslq** 6 months, 1 week ago

This question is difficult, there is no specific documentation that informs us we can start the sync process of retention label to EXO, it takes a maximum of 7 days for retention policy and the same concept appears for retention label, in theory, the only thing we can do when we publish a retention policy or retention label is wait until the backend process run automatically.

option A: MFA is the only option feasible for this question because this command restarts the review for the item for the retention policy or retention label.

but personally, I don't think there is a correct answer, I just go with the A because it makes more sense based on the explanation for each command.

<https://learn.microsoft.com/en-us/purview/create-retention-policies?view=o365-worldwide&tabs=teams-retention#how-long-it-takes-for-retention-policies-to-take-effect>

upvoted 2 times

✉️  **Paul\_white** 7 months 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 3 times

✉️  **AlfaExamPro** 7 months, 1 week 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.

店铺：学习小店66

**Correct Answer: A**

✉️  **Paul\_white** Highly Voted 7 months 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 7 times

✉️  **NrdAlert** 5 months, 3 weeks ago

Stops people from being dumb no doubt.  
upvoted 1 times

店铺：学习小店66

店铺：学习小店66

## 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.

店铺: 学习小店66

店铺: 学习小店66

**Answer Area**

Set-ComplianceTag
Set-HoldCompliancePolicy
<b>Set-RetentionCompliancePolicy</b>
Set-RetentionPolicy
Set-RetentionPolicyTag

-Identity "Policy1" \$true

-enabled
-Force
<b>-RestrictiveRetention</b>
-RetentionPolicyTagLinks
-SystemTag

店铺: 学习小店66

**Correct Answer:**

Set-ComplianceTag
Set-HoldCompliancePolicy
<b>Set-RetentionCompliancePolicy</b>
Set-RetentionPolicy
Set-RetentionPolicyTag

-Identity "Policy1" \$true

-enabled
-Force
<b>-RestrictiveRetention</b>
-RetentionPolicyTagLinks
-SystemTag

✉ **sergioandreslq** 6 months, 1 week ago

Answer provided is correct:

This is preservation lock for retention policies

How to configure Preservation Lock:

<https://learn.microsoft.com/en-us/purview/retention-preservation-lock#how-to-lock-a-retention-policy-or-retention-label-policy>

upvoted 2 times

✉ **DiligentSam** 7 months, 1 week ago

The Given answer is correct

upvoted 2 times

✉ **cb0900** 7 months, 1 week ago

Supplied answer correct.

<https://www.examtopics.com/discussions/microsoft/view/52125-exam-ms-101-topic-3-question-81-discussion/>

upvoted 2 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

店铺：学习小店66

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉  **jt2214**  7 months, 2 weeks 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 7 times

✉  **Y2**  2 months, 3 weeks ago

**Selected Answer: A**

Watch out!! - A similar question appears in the Microsoft Practice Assessment for Exam MS-102: Microsoft 365 Administrator - You have a Microsoft 365 E5 subscription that contains the following device types:

Windows 11  
Android  
macOS  
You plan to implement Endpoint data loss prevention (Endpoint DLP).

Which device types can you onboard to Microsoft Purview?

Answer - Win 11 & MacOS  
upvoted 4 times

✉  **Paul\_white** 7 months ago  
A SI CORRECT

<https://www.examtopics.com/discussions/microsoft/view/93905-exam-ms-101-topic-1-question-100-discussion/>  
upvoted 2 times

店铺：学习小店66

**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="checkbox"/>	<input type="radio"/>
User2 can remove SharePoint sites from Policy1.	<input type="radio"/>	<input checked="" type="checkbox"/>
User2 can add the word Acquisition to Policy1.	<input checked="" type="checkbox"/>	<input type="radio"/>

**Correct Answer:**

✉ **vercracked\_007** Highly Voted 7 months, 3 weeks ago

Correct, can add not remove  
upvoted 7 times

✉ **Casticod** Highly Voted 8 months 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 6 times

□ **Tomtom11** Most Recent 1 month, 4 weeks ago

<https://learn.microsoft.com/en-us/powershell/module/exchange/set-retentioncompliancepolicy?view=exchange-ps>

-RestrictiveRetention

The RestrictiveRetention parameter specifies whether Preservation Lock is enabled for a retention policy or retention label policy. Valid values are

\$true: Preservation Lock is enabled for the policy. No one (including an administrator) can turn off the policy or make it less restrictive.

\$false: Preservation Lock isn't enabled for the policy. This is the default value.

After a policy has been locked, no one can turn off or disable it, or remove content from the policy. And it's not possible to modify or delete content that's subject to the policy during the retention period. The only way that you can modify the retention policy are by adding content to it or extending its duration. A locked policy can be increased or extended, but it can't be reduced, disabled, or turned off.

upvoted 1 times

□ **vogs7** 3 months, 1 week ago

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#compliance-data-administrator>  
I don't think data compliance administrator can modify a policy. NNY

upvoted 4 times

□ **king001** 2 months, 3 weeks ago

N: Compliance Data Admin does not have sufficient privilege.

N: You cannot remove location once the preservation lock is in place.

Y: You can still add.

upvoted 5 times

□ **DiligentSam** 7 months, 1 week ago

Correct

upvoted 3 times

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**

*Community vote distribution*

A (100%)

✉️  **Wazery** 1 month, 2 weeks ago

**Selected Answer: A**

Correct answer. Tested in lab. It's A because the policy already exists and is working. You are just changing the locations.  
upvoted 2 times

✉️  **Greatone1** 6 months, 3 weeks ago

The answer is correct  
<https://www.examtopics.com/discussions/microsoft/view/16568-exam-ms-101-topic-3-question-40-discussion/>  
upvoted 3 times

✉️  **Paul\_white** 7 months ago

A IS CORRECT

<https://www.examtopics.com/discussions/microsoft/view/16568-exam-ms-101-topic-3-question-40-discussion/>  
upvoted 2 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 site interface. At the top, there's a blue header bar with the SharePoint logo and navigation icons. Below it, a large blue ribbon bar displays the site name "Site1". Underneath, there's a search bar labeled "Search Documents" and a toolbar with options like "New", "Upload", "Quick edit", "Sync", and "All Documents". The main area is titled "Documents" and lists three items:

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

曹白 Highly Voted 7 months 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 14 times

Wazery Most Recent 1 month, 2 weeks ago

File3 cannot be access by anyone apart from the owner, last user modified the document and site owner.  
File2 seems to only have a notification and not block applied. Visitor or member does not play a role in this case. Therefore I believe the right answer is File1 and File2 for both users.

upvoted 1 times

lali11 4 months, 1 week ago

Given answer seems to be correct.  
upvoted 1 times

lali11 4 months, 1 week ago

Members can access all the sites.  
<https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/>  
Visitors can access files as defined by DLP policies, if the file is being scanned they can't access the file. The file has dlp warning so guessing it may be blocked for visitors?  
<https://learn.microsoft.com/en-us/sharepoint/sensitive-by-default>

upvoted 1 times

m2L 4 months, 2 weeks ago

Guys,  
This link may help  
<https://gcc.mGuysMicrosoftcrmpartals.com/blogs/office365-news/190220SPIcons/>  
upvoted 1 times

NrdAlert 5 months, 3 weeks ago

File 3 is owned by Prvi(last modified). They will be allowed to access the file even though it's flagged as blocked.

So User 1: All files  
User 2: 1 & 2  
upvoted 2 times

momowagdy 1 week, 1 day ago

Take note that user 1 is neither priva nor user 2. u must have got confused here.  
upvoted 1 times

erranj 3 months, 2 weeks ago

Prvi is not user 1 or 2  
upvoted 3 times

JensV 7 months, 2 weeks 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 7 months, 3 weeks ago

File1 and File2 for both users.  
upvoted 4 times

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**

*Community vote distribution*

AD (100%)

✉️  **Paul\_white** Highly Voted 7 months ago

YOU CAN ONLY ADD LOCATIONS AND EXTEND THE DURATION  
upvoted 13 times

✉️  **Testtest123** Most Recent 4 months, 3 weeks ago

**Selected Answer: AD**

When a preservation lock is implemented on a retention policy in Microsoft 365, it significantly restricts what can be done with that policy, especially in terms of reducing its retention capabilities. This is designed to ensure that the policy remains in compliance with regulations or internal governance requirements. Given the options, here's what can and cannot be done:

- A. Add locations to the policy.
  - D. Extend the duration of the policy.
- upvoted 3 times

✉️  **Testtest123** 4 months, 3 weeks ago

I Mean, it can be done with A and D.  
upvoted 1 times

✉️  **DiligentSam** 7 months ago

<https://www.examtopics.com/discussions/microsoft/view/67142-exam-ms-101-topic-3-question-36-discussion/>  
upvoted 1 times

✉️  **Milad666** 7 months 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 2 times

✉️  **Nail** 5 months, 4 weeks ago

which TWO actions...  
upvoted 1 times

✉️  **NrdAlert** 5 months, 3 weeks ago

You literally picked ALL the wrong answers here, lol. Preservation lock only allows you increase the scope and duration of policy, not reduce it. You have to call Microsoft, submit paperwork etc to have policy completely removed once it has been locked.  
upvoted 2 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

曰  **DiligentSam** 7 months ago

User 2 and User 3  
their type are member. so they are user insider your ORG.  
upvoted 4 times

曰  **Paul\_white** 7 months ago

B IS CORRECT

<https://www.examtopics.com/discussions/microsoft/view/48738-exam-ms-101-topic-3-question-32-discussion/>  
upvoted 2 times

店铺：学习小店66

店铺：学习小店66

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**

*Community vote distribution*

C (100%)

✉  **siulas**  8 months ago

**Selected Answer: C**

<https://www.examtopics.com/discussions/microsoft/view/94552-exam-ms-101-topic-3-question-148-discussion/>  
upvoted 13 times

✉  **TBGarner**  7 months, 1 week ago

**Selected Answer: C**

SecOps mailbox allows you to collect unfiltered messages.  
upvoted 7 times

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

**Selected Answer: C**

I agree with people here  
upvoted 1 times

✉  **Tomtom11** 1 month, 4 weeks ago

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

✉  **cricri** 4 months, 1 week ago

**Selected Answer: C**

Security Operations (SecOps) mailboxes: These are special mailboxes Admins setup to support the ability for end users to report malicious emails to SecOps teams. These are also used by security teams to collect and analyze unfiltered messages.  
upvoted 1 times

✉  **NrdAlert** 5 months, 3 weeks ago

**Selected Answer: C**

You need to use Advanced Delivery to set up a secops mailbox that allows all messages sent to that mailbox to bypass all messaging hygiene filtering in EOP.  
upvoted 2 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.

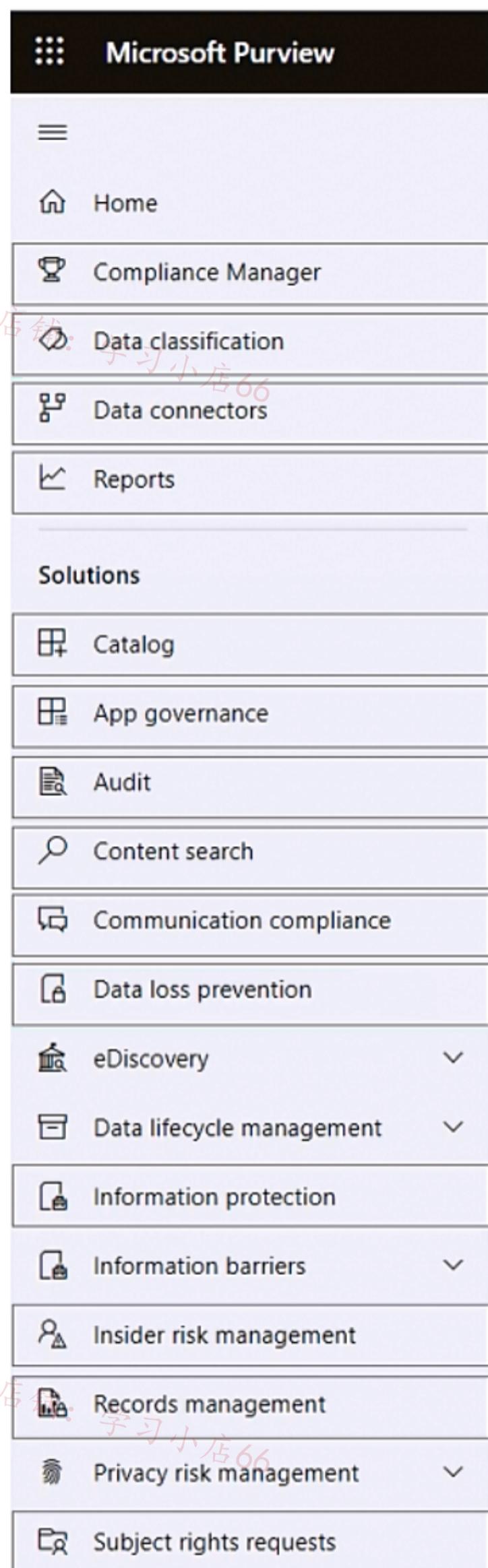
Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.

店铺: 学习小店66

店铺: 学习小店66

NOTE: Each correct selection is worth one point.

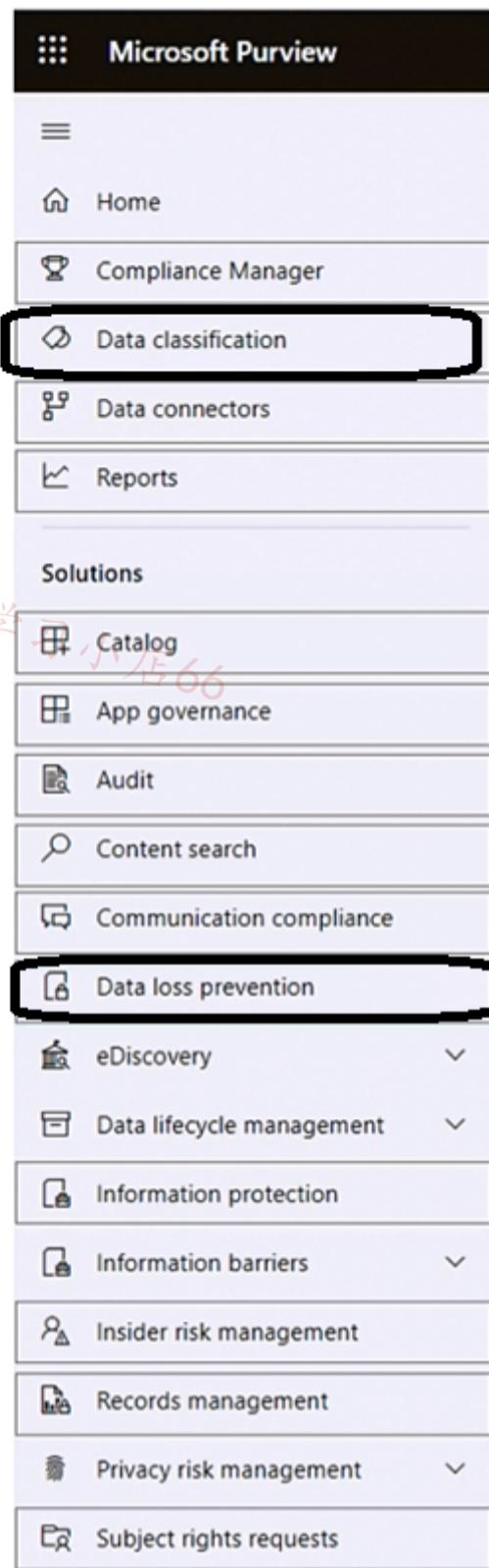
### Answer Area



店铺：学习小店66

店铺：学习小店66

Answer Area



Correct Answer:

④ **kavikumar** Highly Voted 7 months, 1 week 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 18 times

④ **1435b1b** 1 month, 3 weeks ago

kavikumar is correct. Tested in tenant.

Data Classification - Create sensitive info type classifier  
Information Protection - Create label with watermark  
upvoted 2 times

④ **Paul\_white** Most Recent 7 months ago

<https://www.examtopics.com/discussions/microsoft/view/110776-exam-ms-101-topic-3-question-169-discussion/>  
upvoted 1 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**

*Community vote distribution*

D (100%)

✉️  **jt2214** Highly Voted 7 months, 2 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 13 times

✉️  **Paul\_white** Highly Voted 7 months 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 7 times

✉️  **Tomtom11** Most Recent 1 month, 3 weeks ago

From the Purview

Conditions

Define the conditions that must be met for this policy to be applied. Include specific content, senders, and recipients that you want the rule to detect. For more complex rules, create groups to exclude or include items.

Use actions to protect content when the conditions are met.

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

upvoted 1 times

✉️  **Amir1909** 2 months, 4 weeks ago

C is correct

upvoted 1 times

✉️  **Sesbri** 3 months, 2 weeks ago

Agree with action and answer D. For reference see here: <https://www.examtopics.com/discussions/microsoft/view/94552-exam-ms-101-topic-3-question-148-discussion/>

upvoted 1 times

✉️  **Syn\_P** 5 months, 1 week ago

**Selected Answer: D**

Agree with everyone else, should be D.  
upvoted 1 times

曰 **Geri17** 6 months, 2 weeks ago

**Selected Answer: D**

D -> the policy rule actions.  
upvoted 2 times

曰 **VikC** 6 months, 2 weeks ago

**Selected Answer: D**

D. the policy rule actions.  
upvoted 2 times

曰 **GLL** 7 months ago

Should be D the action  
upvoted 2 times

曰 **JensV** 7 months, 3 weeks ago

Should be D the action.  
There you can choose to block everyone or only people outside your organization  
upvoted 4 times

店铺：学习小店66

Question #229

Topic 1

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**

曰 **Paul\_white** Highly Voted 7 months ago  
GIVEN ANSWER IS CORRECT A - ANTI -SPAM  
upvoted 6 times

曰 **Amir1909** Most Recent 2 months, 4 weeks ago

A is correct  
upvoted 2 times

店铺：学习小店66

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

*Community vote distribution*

E (100%)

✉ siulas Highly Voted 8 months ago

**Selected Answer:** E

<https://www.examtopics.com/discussions/microsoft/view/103242-exam-ms-101-topic-3-question-159-discussion/>  
upvoted 12 times

✉ Paul\_white Highly Voted 7 months 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 9 times

✉ Tomtom11 Most Recent 1 month, 3 weeks ago

<https://learn.microsoft.com/en-us/purview/data-classification-content-explorer?view=o365-worldwide>  
Access to content explorer is highly restricted because it lets you read the contents of scanned files  
upvoted 1 times

店铺：学习小店66

**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.

① 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.

① 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 Highly Voted 7 months 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 14 times

1435b1b Most Recent 1 month, 3 weeks ago

Sharepoint  
Onedrive

"Protecting sensitive information in documents. Suppose that someone attempts to share a document with guests in a Microsoft Teams channel or chat, and the document contains sensitive information. If you have a DLP policy defined to prevent this, the document won't open for those users. Your DLP policy must include SharePoint and OneDrive in order for protection to be in place."

<https://learn.microsoft.com/en-us/purview/dlp-microsoft-teams?view=o365-worldwide>  
upvoted 3 times

店铺：学习小店66

店铺：学习小店66

**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

店铺：学习小店66

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.

Content contains

Default1 Any of these

Sensitive info types

IP Address: High confidence (2 to Any)

Add Create group

Back Next Cancel

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"/>

Correct Answer:  
AlfaExamPro Highly Voted 7 months, 1 week ago  
correct

<https://www.examtopics.com/discussions/microsoft/view/56718-exam-ms-101-topic-3-question-95-discussion/>  
upvoted 9 times

1435b1b Most Recent 1 month, 3 weeks ago  
NNY - Sensitivity labels do not support .txt file types  
upvoted 2 times

Tomtom11 1 month, 3 weeks ago  
<https://learn.microsoft.com/en-us/purview/sensitivity-labels-sharepoint-onedrive-files>

Supported file types  
After you've enabled sensitivity labels for SharePoint and OneDrive, the following Office file types are supported for sensitivity labeling scenarios

Applying a sensitivity label in Office on the web or in SharePoint:

Word: .docx, .docm  
Excel: .xlsx, .xlsm, .xlsb  
PowerPoint: .pptx, .ppsx

Uploading a labeled document, and then extracting and displaying that sensitivity label:

Word: doc, .docx, .docm, .dot, .dotx, .dotm  
Excel: .xls, .xlt, .xla, .xlc, .xlm, .xlw, .xlsx, .xltx, .xlsm, .xltm, .xlam, .xlsb  
PowerPoint: .ppt, .pot, .pps, .ppa, .pptx, .ppsx, .ppsxm, .potx, .ppam, .pptm, .potm, .ppsm  
upvoted 1 times

Amir1909 2 months, 4 weeks ago  
Correct  
upvoted 1 times

benpatto 5 months, 1 week ago  
Correct, file types such as .txt are identified differently, these also include file types like jpg and .bmp files so doesn't apply here.  
<https://learn.microsoft.com/en-us/azure/information-protection/rms-client/clientv2-admin-guide-file-types>

upvoted 1 times

≡  **DiligentSam** 7 months ago

correct

upvoted 3 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

**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:

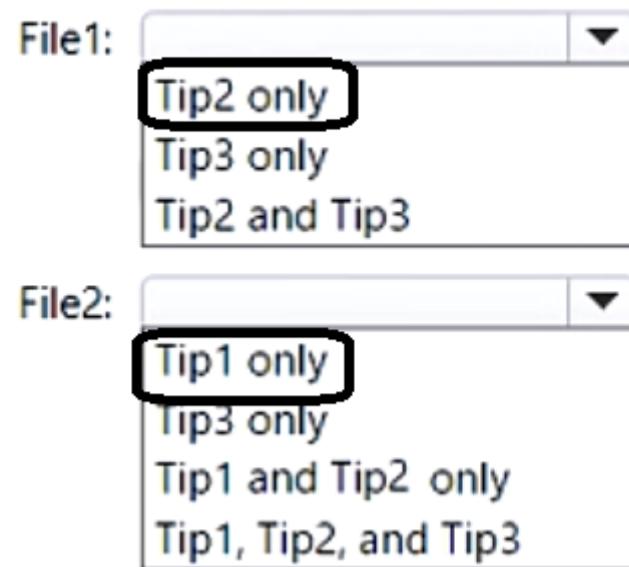
Tip1 only

Tip3 only

Tip1 and Tip2 only

Tip1, Tip2, and Tip3

## Answer Area



Correct Answer:

□ **Casticod** Highly Voted 8 months ago

Tip 1 is configuring to no Stop The rule, In the second option should be Tip 1 and 2  
upvoted 18 times

□ **Paul\_white** 7 months ago

WHICH MEANS

FILE1: TIP2

FILE2: TIP 1 & 3

upvoted 3 times

□ **Paul\_white** 7 months ago

SORRY FOR THE TYPO

FILE1: TIP2

FILE2: TIP1 & 2

upvoted 12 times

□ **mickey88** Most Recent 4 months, 2 weeks ago

I Think it is File 1: Tip 2 Only  
Where as for File 2: Tip 1 and Tip2 only. Because RULe one says if there is a match stop processing as NO.  
upvoted 2 times

□ **TP447** 5 months, 3 weeks ago

Initially i thought the answer was File1: Tip2 and File2: Tip1 & 2 but surely only Tip1 will appear for File2 because of the higher priority set (even with Stop Processing set to No)?  
upvoted 1 times

□ **Darekms0** 6 months, 2 weeks ago

Answer is correct . Please look on priority  
upvoted 4 times

□ **sergioandresiq** 6 months, 1 week ago

Only one policy tip will be showed, In this case we don't know what is the most restrictive, so, the policy tip to be showed will be based on DLP rule precedence.

<https://learn.microsoft.com/en-us/purview/dlp-policy-reference#the-priority-by-which-rules-are-evaluated-and-applied>  
upvoted 1 times

□ **Paul\_white** 7 months 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** 7 months ago

FILE1: TIP2 ONLY  
FILE2: TIP 2 & 3  
upvoted 1 times

□ **cb0900** 7 months ago

Similar question:

<https://www.examtopics.com/discussions/microsoft/view/82220-exam-ms-500-topic-3-question-32-discussion/>

## 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

*Community vote distribution*

A (100%)

imlearningstuffagain 6 months, 2 weeks ago

**Selected Answer: A**

If the recommended txt record is not supported, you may use a MX record to verify the ownership of the domain name. But be aware that this is not the MX record that can be used to receive mail. In this scenario the domain needs to be validated, therefore answer A <https://learn.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide#verify-with-an-mx-record>

upvoted 4 times

DiligentSam 7 months ago

the mailboxes of 100 users in the sales department will be moved to Microsoft 365

Mailbox = MX Record

upvoted 1 times

NrdAlert 5 months, 3 weeks ago

This is misleading. You're using a special MX record in lieu of a TXT record to verify domain ownership. MX is for SMTP mail flow, definitely not mailbox migration. Given project1 is a pilot, you would not modify mail flow until at least a full migration ready to kick off.

upvoted 1 times

✉  **cgmaxmax** 5 months, 2 weeks ago

This MX record's Priority must be the highest of all existing MX records for the domain. Otherwise, it can interfere with sending and receiving email. You should delete this records as soon as domain verification is complete.

<https://learn.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide#verify-with-an-mx-record>

upvoted 1 times

✉  **Greatone1** 7 months ago

Given answer is correct for this one

upvoted 1 times

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

店铺: 学习小店66

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**

*Community vote distribution*

B (100%)

✉️  **Tomtom11** 1 month, 3 weeks ago

**Selected Answer: B**

Teams Administrator

Users in this role can manage all aspects of the Microsoft Teams workload via the Microsoft Teams & Skype for Business admin center and the respective PowerShell modules. This includes, among other areas, all management tools related to telephony, messaging, meetings, and the teams themselves. This role additionally grants the ability to create and manage all Microsoft 365 groups, manage support tickets, and monitor service health.

upvoted 2 times

✉️  **Festus365** 4 months, 3 weeks ago

It should be Team, SharePoint and OneDrive online administrator roles not Team Admin only. B is correct!

upvoted 3 times

✉️  **GGLight** 5 months, 3 weeks ago

It should be Yes

<https://www.examtopics.com/discussions/microsoft/view/76446-exam-ms-101-topic-2-question-50-discussion/#:~:text=You%20need%20to%20ensure%20that,SecAdmin1%20the%20Security%20administrator%20role.>

upvoted 1 times

✉️  **ITCALegends** 5 months, 2 weeks ago

your link proves your wrong , learn to read

upvoted 3 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 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 店铺：学习小店66

Action:

- Enable app registrations.
- Enable password writeback.
- Enable password hash synchronization.
- Disable password hash synchronization.

Correct Answer:

Tool:

- Azure AD Connect
- Synchronization Rules Editor
- Microsoft Entra admin center

✉  **northgaterebel**  6 months, 2 weeks ago

Enable password writeback  
Azure AD Connect  
Password writeback must first be enabled in AD Connect. <https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr-writeback>  
upvoted 14 times

✉  **KerrAvon**  2 months, 1 week ago

The descriptive states that Self-service password reset (SSPR) is enabled - this is the part in Entra admin. So the writeback now needs to be enabled in Entra Connect (AADC)  
upvoted 1 times

✉  **MvdSpoel** 5 months, 3 weeks ago

Answers are Enable password writeback and Azure AD Connect. Please note that Azure AD Connect is also named Microsoft Entra Connect  
upvoted 3 times

✉  **Greatone1** 7 months ago

<https://www.examtopics.com/discussions/microsoft/view/107026-exam-ms-100-topic-13-question-1-discussion/>  
upvoted 2 times

✉  **Greatone1** 7 months ago

Correct answers are enable password write back and azure ad connect  
upvoted 4 times

✉  **jakke91** 7 months 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** 7 months 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

✉  **CheMetto** 6 months, 1 week ago

Nope!  
By default, Microsoft Entra ID enables self-service password reset for admins. They're required to use two authentication methods to reset their password. For more information, see Administrator reset policy differences.  
<https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr>

It's AADConnect the answer.

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="checkbox"/>	<input type="radio"/>
Users must use the Microsoft Authenticator app to complete MFA.	<input type="radio"/>	<input checked="" type="checkbox"/>
After registering, users must use MFA for every sign-in.	<input type="radio"/>	<input checked="" type="checkbox"/>

✉  Paul\_white Highly Voted 7 months 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 21 times

✉  60ed5c2 6 months ago

It doesn't have to be MS Auth - "or any app supporting OATH TOTP"

<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>

Yes, No, No is correct

upvoted 5 times

✉  sergioandresiq 6 months, 1 week ago

Thanks, I didn't remember that sentence which force MS Authenticator. I was thinking on the authentication methods where we can choose different options but security default change the answer for item 2.

Thanks,

upvoted 1 times

✉  Festus365 Most Recent 4 months, 3 weeks ago

Multi factor authentication every sign in requirement ==>>

After registering for Multi-Factor Authentication (MFA), a user will not necessarily need to use MFA for every sign-in. Generally, MFA is required the first time a user signs into a new app or device, or after they've changed their password

Microsoft authenticator app requirement for MFA ==>>

No, a user is not required to use the Microsoft Authenticator app to complete Multi-Factor Authentication (MFA). While the Microsoft Authenticator app is a commonly

used option, users can choose different methods for verification. These methods may include text messages, phone calls, or other authenticator apps.(Answers: Y/N/N)

upvoted 2 times

✉  Paul\_white 7 months ago

YES, NO, NO

<https://www.examtopics.com/discussions/microsoft/view/83963-exam-ms-100-topic-16-question-1-discussion/>

upvoted 2 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.

店铺：学习小店66

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**

Community vote distribution

B (100%)

店铺：学习小店66

 **MvdSpoel** 5 months, 3 weeks ago

**Selected Answer: B**

Answer is connect

<https://techcommunity.microsoft.com/t5/intune-customer-success/configuring-microsoft-intune-just-in-time-admin-access-with/ba-p/3843972>

upvoted 3 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 Administrator
- C. Service Administrator
- D. User Administrator

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉  **Paul\_white**  7 months ago

CORRECT B!!!

upvoted 5 times

✉  **Tomtom11**  1 month, 3 weeks ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection>

Required roles

Identity Protection requires users be a Security Reader, Security Operator, Security Administrator, Global Reader, or Global Administrator in order to access.

upvoted 3 times

✉  **king001** 2 months, 3 weeks ago

Require Role:

1 Global Admin

2 Security Admin

3 Security Reader

available choice and least privilege is Security Admin

upvoted 2 times

✉  **DiligentSam** 7 months ago

base on this question <https://www.examtopics.com/discussions/microsoft/view/49685-exam-ms-100-topic-3-question-29-discussion/>

upvoted 4 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**

✉  **Paul\_white**  7 months ago

SECURITY READER IS CORRECT!!!!

upvoted 5 times

✉  **king001**  2 months, 3 weeks ago

Require Role:

1 Global Admin

2 Security Admin

3 Security Reader

available choice and least privilege is Security Reader

upvoted 2 times

✉  **Amir1909** 2 months, 4 weeks ago

B is correct

upvoted 1 times

✉  **DiligentSam** 7 months ago

<https://www.examtopics.com/discussions/microsoft/view/49685-exam-ms-100-topic-3-question-29-discussion/>

upvoted 3 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

店铺：学习小店66

✉️  **Amir1909** 2 months, 4 weeks ago

D is correct

upvoted 1 times

✉️  **Greatone1** 6 months, 1 week ago

Answer is correct Exchange admin center

upvoted 2 times

✉️  **Paul\_white** 7 months 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

店铺：学习小店66

店铺：学习小店66

**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.

User2 can send a maximum of 50 email messages per day.

User3 can send a maximum of 100 email messages per day.

**Answer Area**

Statements	Yes	No
------------	-----	----

**Correct Answer:** User1 can send a maximum of 150 email messages per day.

User2 can send a maximum of 50 email messages per day.

User3 can send a maximum of 100 email messages per day.

✉ aleksdj Highly Voted 5 months ago

N User1 max 50 users per day because both Antispam policies apply for User1 but the least privilege counts, so 50.  
Y User2 is in Group1 and 2, so both Antispam policies apply but the least privilege counts, so 50  
N User3 is excluded from Antispam1 (Group2 excluded) and Antispam2 (User3 excluded)  
upvoted 6 times

✉ Paul\_white Highly Voted 7 months ago

NO, YES, NO AS VALIDATED BY BING GPT  
upvoted 6 times

✉ 9711d59 Most Recent 2 months, 3 weeks ago

Different conditions use AND logic (for example, <recipient1> and <member of group 1>). The recipient must satisfy all of the specified conditions, which is typically difficult or redundant.  
Nobody applies to this rule so YYY.  
upvoted 1 times

✉ Amir1909 3 months ago

- No  
- No  
- No  
upvoted 3 times

✉ itguys 4 months, 2 weeks ago

With Anti-spam, anti-phishing and anti-malware policies (also CA policies), exclusion takes precedence over inclusion

Answers are correct

FYI the opposite is true for safe-links and safe-attachment policies - inclusion takes precedence over exclusion  
upvoted 4 times

✉ timkuo1009 5 months ago

I think is N, Y, Y  
Once User3 is included to AntiSpam1, user 3 will not be applied to Antispam2 policy.

Refer to the following document

The priority order matters if you have the same recipient intentionally or unintentionally included in multiple policies, because only the first policy of that type (anti-spam, anti-malware, anti-phishing, etc.) is applied to that recipient, regardless of how many other policies that the recipient is included in. There's never a merging or combining of the settings in multiple policies for the recipient. The recipient is unaffected by the settings of the remaining policies of that type.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/how-policies-and-protections-are-combined?view=o365-worldwide>

upvoted 1 times

✉ timkuo1009 5 months ago

Sorry, my mistake, user3 is excluded from antispam1 (Group2 is excluded). user3 will be applied to antispam2. Answer is N, Y, N  
upvoted 3 times

✉ DiligentSam 6 months, 4 weeks ago

I think User 3 matches PolicyName:Anti-spam 1  
so the 3rd option is Yes  
upvoted 3 times

✉ DiligentSam 6 months, 4 weeks ago

I am sorry, policy 1 excludes group2, and user3 is a member of group 2  
upvoted 1 times

✉ 60ed5c2 6 months ago

Policy 1 includes user3 AND excludes group2 of which user 3 is a member. User3 is both included and excluded. Wouldn't the rule of more restrictive apply and therefore user3 would be included?

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:

Settings:

**Answer Area**

Administrators:

Correct Answer: Admin1 & Admin 2 - Anti Spam is the correct answer

Settings:

✉ **Acacio** 5 months, 4 weeks ago

Admin1 & Admin 2 - Anti Spam is the correct answer  
upvoted 8 times

✉ **Paul\_white** 7 months ago

ADMIN 1 & 2, - ANTI SPAM  
<https://www.examtopics.com/discussions/microsoft/view/94096-exam-ms-101-topic-2-question-122-discussion/>

upvoted 7 times

✉️  **Capital** Most Recent 2 months, 2 weeks ago

Tested this in lab environment - Exchange Administrator CAN unblock user from restricted entities.

upvoted 1 times

✉️  **Geri17** 6 months, 2 weeks ago

Admin2:

You need to be assigned permissions before you can do the procedures in this article. You have the following options:

Exchange Online permissions:

Remove user accounts from the Restricted entities page: Membership in the Organization Management or Security Administrator role groups.

Read-only access to the Restricted entities page: Membership in the Global Reader, Security Reader, or View-Only Organization Management role groups.

Microsoft Entra permissions: Membership in the Global Administrator, Security Administrator, Global Reader, or Security Reader roles gives users the required permissions and permissions for other features in Microsoft 365.

upvoted 3 times

✉️  **imlearningstuffagain** 6 months, 2 weeks ago

there is no exchange administrator in exchange online, and even if it was the case, it had not enough permissions:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam?view=o365-worldwide#what-do-you-need-to-know-before-you-begin>

Answer: admin2 and Anti-Spam

upvoted 2 times

✉️  **NrdAlert** 5 months, 3 weeks ago

Good catch. No such role exists in EXO named Exchange Administrator. Organization Management is the highest level role, however you would have permissions with this particular role to remove the user per your link.

upvoted 2 times

✉️  **NrdAlert** 5 months, 3 weeks ago

Just kidding, it does exist in the admin center. Unclear if it gives the Organization Management role when assigned, but I have found a few posts claiming it is which makes sense.

upvoted 1 times

✉️  **Greatone1** 7 months ago

Answer is Admin 1 & Admin 2 - Anti Spam

Exchange Admin do have permission to amend and set up Anti Spam policies.

upvoted 2 times

店铺：学习小店66

店铺：学习小店66

## 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 to the tenant for the project.

Which DNS record should you recommend?

- A. alias (CNAME)
- B. host information (HINFO)
- C. host (A)
- D. text (TXT)

#### Correct Answer: A

*Community vote distribution*

D (100%)

phlegmbot Highly Voted 6 months ago

**Selected Answer: D**

You can either add a TXT(preferred) or an MX record to validate the domain.

upvoted 5 times

Vaerox Most Recent 3 months, 1 week ago

**Selected Answer: D**

As part of adding the domain to your tenant, you will need to verify the domain first. Microsoft will provide you with a TXT record that usually looks like "MS=xxxxxxxx" and you will be asked to add the TXT record to your public DNS provider.

upvoted 1 times

Christianbrivio1991 5 months, 1 week ago

**Selected Answer: D**

Add to record TXT

upvoted 2 times

Acacio 5 months, 4 weeks ago

TXT is the correct answer.  
upvoted 4 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

You create a Conditional Access policy named Policy1 and assign Policy1 to all users.

You need to configure Policy1 to enforce multi-factor authentication (MFA) if the user risk level is high.

Which two settings should you configure in Policy1? 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 \*

 ✓**Assignments**

Users or workload identities ⓘ

[All users](#)

Cloud apps or actions ⓘ

[All cloud apps](#)

Conditions ⓘ

[0 conditions selected](#)**Access controls**

Grant ⓘ

[0 controls selected](#)

Session ⓘ

[0 controls selected](#)

店铺：学习小店66

店铺：学习小店66

## 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 \*

Policy1 ✓

#### Assignments

Correct Answer: [All users](#)

[Cloud apps or actions](#)

[Conditions](#)

0 conditions selected

#### Access controls

[Grant](#)

0 controls selected

[Session](#)

0 controls selected

店铺：学习小店66

**sergioandreslq** 6 months ago

The answers are correct, you need to configure in condition user-risk and in access control Grant enable MFA  
upvoted 5 times

**itguys** 4 months, 2 weeks ago

in addition - needs a session policy - sign-in everytime  
upvoted 2 times

**Bouncy** 2 months, 2 weeks ago

Yeah, no, why would you want to annoy all your users with this setting???  
upvoted 2 times

店铺：学习小店66

店铺：学习小店66

Your network contains an Active Directory domain.

You have an Azure AD tenant that has Security defaults disabled.

Azure AD Connect is configured for directory synchronization. Password hash synchronization and pass-through authentication are disabled.

You need to enable Azure AD Identity Protection to detect leaked credentials.

What should you do first?

- A. From Azure AD Connect, enable password hash synchronization.
- B. From the Microsoft Entra admin center, enable Security defaults.
- C. From the Microsoft Entra admin center, configure verifiable credentials.
- D. From Azure AD Connect, enable pass-through authentication.

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉  **apokavk** Highly Voted 6 months, 1 week ago

**Selected Answer: A**

<https://www.examtopics.com/discussions/microsoft/view/107560-exam-ms-100-topic-3-question-93-discussion/>  
upvoted 5 times

✉  **Motanel** Most Recent 2 weeks ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#leaked-credentials>

Leaked credentials are processed anytime Microsoft finds a new, publicly available batch. Because of the sensitive nature, the leaked credentials are deleted shortly after processing. Only new leaked credentials found after you enable password hash synchronization (PHS) will be processed against your tenant. Verifying against previously found credential pairs isn't done.

upvoted 1 times

## HOTSPOT

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

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1, Group2	Enabled
User3	Group2	Disabled

You configure a multi-factor authentication (MFA) registration policy that has the following settings:

- Assignments:
  - o Include: Group1
  - o Exclude: Group2
- Access controls: Require Azure MFA registration
- Enforce Policy: On

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

- Name: Policy 1
- Assignments:
  - o Include: Group2
  - o Exclude: Group1
- Access controls:
  - o Grant, Require multi-factor authentication
- 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 will be required to register for MFA on the next sign-in.	<input type="radio"/>	<input type="radio"/>
User2 will be required to register for MFA on the next sign-in.	<input type="radio"/>	<input type="radio"/>
User3 will be required to register for MFA on the next sign-in.	<input type="radio"/>	<input type="radio"/>

**Correct Answer:**

Statements	Yes	No
User1 will be required to register for MFA on the next sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User2 will be required to register for MFA on the next sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be required to register for MFA on the next sign-in.	<input checked="" type="radio"/>	<input type="radio"/>

 **Mr4D97** Highly Voted 5 months, 2 weeks ago

Statement 1 = Yes - User 1 is part of group 1 with MFA status disabled and, as per the MFA registration policy, will need to register for MFA.

Statement 2 = No - Although part of group one and two, they already have MFA enabled so will not need to register for it

Statement 3 = No - does not have MFA enabled already is part of group 2 so is excluded from registration policy, therefore will not need to

register.

Y, N, N

This are my thoughts but please comment if you think im wrong or have any further points to add :)

upvoted 12 times

□ **Vaerox** 3 months, 2 weeks ago

Statement 3 must be Yes. The user is indeed excluded from the MFA Campaign (policy) but is included in the CA policy, which enforces MFA.  
upvoted 7 times

□ **Kmkz83510** Highly Voted 4 months, 3 weeks ago

Have not tested, but I think YNY since the question is about registration.

U1 - User will be prompted because they are in Group1. They aren't currently registered and would be required to do so because of registration policy. Does not matter if they are excluded from CA. Remember register, not necessarily use for access.

U2 - Already registered.

U3 - User not registered. Even though they are excluded from the registration policy, they need MFA for CA, so they are forced to register anyway  
upvoted 12 times

□ **oopspruu** Most Recent 1 week, 3 days ago

When MFA is being pushed from MFA Registration policy, you are not required to setup MFA on the very next login. You have 14 days to complete it.

Given answers are correct.

upvoted 1 times

□ **Tomtom11** 1 month, 3 weeks ago

Microsoft Entra multifactor authentication user states

All users start out Disabled. When you enroll users in per-user Microsoft Entra multifactor authentication, their state changes to Enabled. When enabled users sign in and complete the registration process, their state changes to Enforced. Administrators may move users between states, including from Enforced to Enabled or Disabled.

upvoted 1 times

□ **Tomtom11** 1 month, 3 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-userstates>

upvoted 1 times

□ **Amir1909** 2 months, 4 weeks ago

No

Yes

Yes

upvoted 1 times

□ **AAlmani** 3 months ago

Yes No Yes

if you enable MFA via the MFA portal, you completely rub out the ability to utilize Conditional Access Policies. You must have the Azure MFA user state set to disabled, and a CA policy configured to require multi factor authentication for CA based settings to apply.

-user1 excluded from the CA but enforced to register MFA based on the first policy.(yes)

-user2 included in the CA (no already registered)

-user3 included in the CA but MFA not register yet (yes should register)

upvoted 3 times

□ **Vaerox** 3 months, 2 weeks ago

Y, N, Y

User 1 = Might be excluded from the CA policy but is still required to set-up MFA because of the MFA Campaign

User 2 = Excluded from the CA policy and has also already registered MFA.

User 3 = CA policy enforces the user to set-up MFA (we have this type of policy for over 100 customers. You can't skip the 14 day grace period).

upvoted 6 times

□ **aleksdj** 5 months ago

学习小店66

Exclude wins over include

User1 = Group1 = Excluded = no MFA required

User2 = Group1/Group2 = Should be Excluded because Group1 is excluded BUT MFA Auth Status is set to enabled so User2 must register for MF.

User3 = Group2 = included = MFA required

upvoted 2 times

□ **aleksdj** 5 months ago

Correction:

User2 has already MFA Enabled, so no need to register again, answer is NO.

The given answer is correct, NNY

upvoted 2 times

□ **jt2214** 5 months, 3 weeks ago

I'm confused, this question is about will they need to register with MFA, not authenticate. Wouldn't it be Y, Y, N?  
upvoted 1 times

✉ **MvdSpoel** 5 months, 3 weeks ago

Answers are correct  
<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy>  
<https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide>  
upvoted 2 times

✉ **MvdSpoel** 5 months, 1 week ago

Answers is correct  
User 1 -> No: - See <https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#require-all-users-to-register-for-microsoft-entra-multifactor-authentication> users have a 14 day grace period after which they require registration

User 2 -> No: because there are no MFA rules applicable. Because user is a member of Group 1 and Group 2 which are both used as include and exclude

User 3 -> Yes: The MFA policy used is require autentioncation, which overrule the grace period of 14 days  
upvoted 1 times

✉ **BSVIT** 5 months, 3 weeks ago

Yes, no, no? its about REGISTRATION for MFA, not prompting to login with it.  
upvoted 4 times

✉ **Cloudddd** 5 months, 4 weeks ago

Correct answer is: No, Yes, Yes

<https://www.examtopics.com/discussions/microsoft/view/58278-exam-ms-100-topic-4-question-69-discussion/>  
upvoted 4 times

✉ **sigvast** 5 months, 3 weeks ago

The question you linked is about "use MFA", this one ask "register for MFA". Not the same thing.  
upvoted 4 times

Your network contains an on-premises Active Directory domain.

You have a Microsoft 365 subscription.

You implement a directory synchronization solution that uses pass-through authentication.

You configure Azure AD smart lockout as shown in the following exhibit.

**Authentication methods | Password protection**

Custom smart lockout  
Lockout threshold: 5  
Lockout duration in seconds: 60

Custom banned passwords  
Enforce custom list: Yes  
Custom banned password list:  
password  
Pa\$\$w0rd  
Pa55w0rd  
Contoso

Password protection for Windows Server Active Directory  
Enable password protection on Windows Server Active Directory: Yes  
Mode: Audit

You discover that Active Directory users can use the passwords in the custom banned passwords list.

You need to ensure that banned passwords are banned for all users.

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 the Azure AD Password Protection Proxy.
- B. From Active Directory, modify the Default Domain Policy.
- C. From a domain controller, install the Azure AD Application Proxy connector.
- D. From all the domain controllers, install the Azure AD Password Protection DC Agent.
- E. From Password protection for Windows Server Active Directory, modify the Mode setting.
- F. From Custom banned passwords, modify the Enforce custom list setting.

**Correct Answer: ADE**

*Community vote distribution*

ADE (67%)

ADF (33%)

Rohgun 2 weeks, 6 days ago

**Selected Answer: ADE**

A,D,E - sure

upvoted 1 times

✉ **CharlesS76** 4 weeks ago

**Selected Answer: ADE**

<https://www.examtopics.com/discussions/microsoft/view/3694-exam-ms-100-topic-4-question-38-discussion/>

upvoted 1 times

✉ **Vaerox** 3 months, 2 weeks ago

**Selected Answer: ADF**

After reading through the MS documentation AND watching a YouTube video, I'm fairly confident that the answers are:

A

D

F

You need to set-up the proxy, install the DC Agent and eventually switch Audit to Enforced mode. Now I can't find anywhere that you have to do this on the on-prem environment so that's why I'm going for F.

upvoted 1 times

✉ **Vaerox** 3 months, 1 week ago

Sorry, it is ADE, not ADF.

upvoted 6 times

✉ **apokavk** 6 months, 1 week ago

correct

<https://www.examtopics.com/discussions/microsoft/view/3694-exam-ms-100-topic-4-question-38-discussion/>

upvoted 1 times

Your network contains an Active Directory domain and an Azure AD tenant.

The network uses a firewall that contains a list of allowed outbound domains.

You begin to implement directory synchronization.

You discover that the firewall configuration contains only the following domain names in the list of allowed domains:

- \*.microsoft.com
- \*.office.com

Directory synchronization fails.

店铺：学习小店66

You need to ensure that directory synchronization completes successfully.

What is the best approach to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

- A. From the firewall, modify the list of allowed outbound domains.
- B. From Azure AD Connect, modify the Customize synchronization options task.
- C. From the firewall, create a list of allowed inbound domains.
- D. Deploy an Azure AD Connect sync server in staging mode.
- E. From the firewall, allow the IP address range of the Azure data center for outbound communication.

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉️  **apokavk**  6 months, 1 week ago

**Selected Answer: A**

<https://www.examtopics.com/discussions/microsoft/view/53623-exam-ms-100-topic-3-question-40-discussion/>  
upvoted 6 times

店铺：学习小店66

店铺：学习小店66

You have a Microsoft 365 E5 subscription that contains users in the United States, Europe, and Asia.

You use Azure AD Identity Protection.

You have a virtual desktop infrastructure (VDI). All VDI servers are located in the United States.

Users connect to Microsoft 365 from laptops and the VDI.

Some VDI users report that they are blocked from signing in to Microsoft 365 due to a high sign-in risk.

You need to reduce the likelihood that the VDI users will be erroneously blocked from signing in to Microsoft 365. The solution must ensure that sign-ins from the VDI environment are protected by using Identity Protection.

What should you configure?

- A. ExpressRoute for Microsoft 365
- B. a trusted location
- C. a Satellite Geography location
- D. a Conditional Access policy

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉️  **Tomtom11** 1 month, 3 weeks ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-configure-risk-policies>  
upvoted 2 times

✉️  **Vaerox** 3 months, 1 week ago

**Selected Answer: B**

Seems correct.  
upvoted 2 times

✉️  **apokavk** 6 months, 1 week ago

**Selected Answer: B**

similar question  
<https://www.examtopics.com/discussions/microsoft/view/118344-exam-ms-102-topic-1-question-89-discussion/>  
upvoted 3 times

## HOTSPOT

You have a Microsoft 365 subscription.

From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

**Global Administrator | Role settings**

Privileged Identity Management | Azure AD roles

Edit

**Activation**

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

**Assignment**

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	15 day(s)
Allow permanent active assignment	Yes
Expire active assignments after	*
Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	No

You make a user named admin1@contoso.com eligible for the Global Administrator role.

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 use the Global Administrator role, admin1@contoso.com must provide [answer choice].

Azure Multi-Factor Authentication (MFA) and requires admin approval justification and Azure Multi-Factor Authentication (MFA) ticket information and justification ticket information and requires admin approval

To make a new user eligible for the Global Administrator role, a PIM administrator must configure [answer choice].

an assignment duration and justification  
Azure Multi-Factor Authentication (MFA) and an assignment duration  
Azure Multi-Factor Authentication (MFA) and justification  
justification and ticket information

**Answer Area**

To use the Global Administrator role, admin1@contoso.com must provide [answer choice].

Azure Multi-Factor Authentication (MFA) and requires admin approval justification and Azure Multi-Factor Authentication (MFA)

ticket information and requires admin approval

An assignment duration and justification

Azure Multi-Factor Authentication (MFA) and an assignment duration

Azure Multi-Factor Authentication (MFA) and justification

justification and ticket information

**Correct Answer:**

To make a new user eligible for the Global Administrator role, a PIM administrator must configure [answer choice].

An assignment duration and justification

Azure Multi-Factor Authentication (MFA) and an assignment duration

Azure Multi-Factor Authentication (MFA) and justification

justification and ticket information

sergioandreslq Highly Voted 6 months ago

I believe the answers are correct.  
upvoted 6 times

Tomtom1 Most Recent 1 month, 3 weeks ago

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure>  
upvoted 1 times

Tomtom1 1 month, 3 weeks ago

<https://learn.microsoft.com/en-ie/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings>  
upvoted 1 times

Amir1909 2 months, 4 weeks ago

Correct  
upvoted 1 times

Vaerox 3 months, 1 week ago

Joining sergio on this one, answers seem correct.  
upvoted 1 times

**Question #252****Topic 1**

You have a Microsoft 365 subscription that contains more than 2,000 guest users.

You need to ensure that when guest users are added to Microsoft 365 groups in the subscription, their membership is validated by the group owner every 30 days.

What should you configure?

- A. group expiration policies
- B. retention policies
- C. access reviews
- D. Conditional Access policies

**Correct Answer: C**

Amir1909 2 months, 4 weeks ago

C is correct  
upvoted 3 times

sergioandreslq 6 months ago

C: Correct:  
Access review policy can request the owner to check the membership for guest every 30 days.  
upvoted 4 times

**HOTSPOT**

You have a Microsoft 365 subscription that uses a domain name of adatum.com.

In Azure AD, you set Guest invite restrictions to Only users assigned to specific admin roles can invite guest users.

A user named user1@adatum.com reports that they can no longer invite external users from a domain named contoso.com to collaborate in Microsoft Teams.

You need to modify the Azure AD configuration to meet the following requirements:

- Ensure that User1 can invite the contoso.com users to Teams.
- Ensure that only the contoso.com users can be invited as guests to the Azure AD tenant.
- Follow the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Ensure that User1 can invite the contoso.com users to Teams:

- Assign the Guest Inviter role to User1.
- Assign the User Administrator role to User1.
- Assign the Teams Administrator role to User1.
- Add User1 as a group owner to each team in Teams.

Ensure that only the contoso.com users can be invited as guests to the Azure AD tenant:

- From the Cross-tenant access settings, edit the Outbound access settings.
- From the External collaboration settings, edit the Collaboration restrictions settings.
- From the External collaboration settings, edit the Guest user access restrictions settings.

**Answer Area**

Ensure that User1 can invite the contoso.com users to Teams:

- Assign the Guest Inviter role to User1.
- Assign the User Administrator role to User1.
- Assign the Teams Administrator role to User1.
- Add User1 as a group owner to each team in Teams.

**Correct Answer:**

Ensure that only the contoso.com users can be invited as guests to the Azure AD tenant:

- From the Cross-tenant access settings, edit the Outbound access settings.
- From the External collaboration settings, edit the Collaboration restrictions settings.
- From the External collaboration settings, edit the Guest user access restrictions settings.

✉  **Amir1909** 2 months, 4 weeks ago

Correct

upvoted 2 times

✉  **MvdSpoel** 5 months, 3 weeks ago

Correct

<https://learn.microsoft.com/en-us/microsoft-365/solutions/collaborate-in-site?view=o365-worldwide>

upvoted 1 times

✉  **sergioandreslq** 6 months ago

Box1: Correct

Only users assigned to specific admin roles can invite guest users:

To allow only those users with administrator roles to invite guests, select this radio button.

- The administrator roles include
- Global Administrator
- User Administrator
- Guest Inviter

Box 2: Correct

Under Collaboration restrictions, you can choose whether to allow or deny invitations to the domains you specify and enter specific domain names in the text boxes.

<https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure#configure-settings-in-the-portal>  
upvoted 2 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

## HOTSPOT

Your network contains an on-premises Active Directory domain that is synced to Azure AD as shown in the following exhibit.

The screenshot shows the Microsoft Azure Active Directory Connect interface. On the left, there's a sidebar with 'Welcome', 'Tasks', and 'Review your solution' buttons. The 'Review your solution' button is highlighted in blue. The main area is titled 'Synchronized Directories' and shows 'DIRECTORY' set to 'Adatum.com' and 'ACCOUNT' set to 'ADATUM.COM\MSOL\_e785c048abcc'. Below this, under 'Synchronization Settings', various sync options are listed:

Setting	Value
SOURCE ANCHOR	mS-DS-ConsistencyGuid
SYNC CRITERIA	AlwaysProvision
AZURE AD APP AND ATTRIBUTE FILTERING	Disabled
DIRECTORY EXTENSION ATTRIBUTE SYNC	Disabled
GROUP WRITEBACK	Disabled
PASSWORD WRITEBACK	Disabled
AUTO UPGRADE	Enabled
SQL SERVER NAME	(localdb)
ACCOUNT	ADATUM.COM\MSOL_e785c048abcc
USER PRINCIPAL NAME	userPrincipalName
FILTER OBJECTS TO SYNCHRONIZE BY GROUP	Disabled
DEVICE WRITEBACK	Disabled
EXCHANGE HYBRID DEPLOYMENT	Disabled
PASSWORD HASH SYNCHRONIZATION	Enabled
USER WRITEBACK	Disabled
EXCHANGE MAIL PUBLIC FOLDERS	Disabled
SQL SERVER INSTANCE NAME	.\ADSync

At the bottom right are 'Previous' and 'Exit' buttons.

An on-premises Active Directory user account named Allan Yoo is synchronized to Azure AD. You view Allan's account from Microsoft 365 and notice that his username is set to Allan@adatum.onmicrosoft.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
From the Azure portal, you can reset the password of Allan Yoo.	<input checked="" type="radio"/>	<input type="radio"/>
From the Azure portal, you can configure the job title of Allan Yoo.	<input type="radio"/>	<input checked="" type="radio"/>
From the Azure portal, you can configure the usage location of Allan Yoo.	<input type="radio"/>	<input checked="" type="radio"/>

**Answer Area****Correct Answer:**

Statements	Yes	No
From the Azure portal, you can reset the password of Allan Yoo.	<input type="radio"/>	<input checked="" type="checkbox"/>
From the Azure portal, you can configure the job title of Allan Yoo.	<input type="radio"/>	<input checked="" type="checkbox"/>
From the Azure portal, you can configure the usage location of Allan Yoo.	<input checked="" type="checkbox"/>	<input type="radio"/>

✉  **coyoteee**  5 months, 1 week ago

NNY

Allan Yoo's user account is synchronized from the on-premise Active Directory. This means that most user account settings have to be configured in the on-premise Active Directory.

In the exhibit, Password Writeback is disabled. Therefore, you cannot reset the password of Allan Yoo from the Azure portal.

You also cannot change Allan Yoo's job title in the Azure portal because his account is synchronized from the on-premise Active Directory.

One setting that you can configure for synchronized user accounts is the usage location. The usage location must be configured on a user account before you can assign licenses to the user.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback>

upvoted 5 times

✉  **kgri**  5 months ago

Is Allan Yoo synced from AD? Doesn't the @adatum.onmicrosoft.com indicate that this is a cloud user?

upvoted 2 times

✉  **apokavk** 6 months, 1 week ago

<https://www.examtopics.com/discussions/microsoft/view/50305-exam-ms-100-topic-3-question-42-discussion/>

upvoted 3 times

店铺：学习小店66

店铺：学习小店66

Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 10.

You purchase a Microsoft 365 subscription.

You implement password hash synchronization and Azure AD Seamless Single Sign-On (Seamless SSO).

You need to ensure that users can use Seamless SSO from the Windows 10 computers.

What should you do?

- A. Join the computers to Azure AD.
- B. Create a conditional access policy in Azure AD.
- C. Modify the Intranet zone settings by using Group Policy.
- D. Deploy an Azure AD Connect staging server.

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉️  **sergioandreslq** 6 months ago

C: Correct:

- a. Open the Group Policy Management Editor tool.
- b. Edit the group policy that's applied to some or all your users. This example uses Default Domain Policy.
- c. Go to User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page. Select Site to Zone Assignment List.

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-sso-quick-start#group-policy-detailed-steps>  
upvoted 2 times

✉️  **apokavk** 6 months, 1 week ago

**Selected Answer: C**

<https://www.examtopics.com/discussions/microsoft/view/41985-exam-ms-100-topic-4-question-47-discussion/>  
upvoted 2 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 Azure Cloud Shell, run the Get-MsolUser and Set-MsolUser cmdlets.
- B. From Windows PowerShell on a domain controller, run the Get-MgUser and Update-MgUser cmdlets.
- C. From Active Directory Administrative Center, select the Active Directory users, and then modify the Properties settings.
- D. From Azure Cloud Shell, run the Get-MgUser and Update-MgUser cmdlets.

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉️  **Christianbrivio1991** 5 months, 1 week ago

**Selected Answer: C**

C is correct

upvoted 2 times

✉️  **apokavk** 6 months, 1 week ago

**Selected Answer: C**

<https://www.examtopics.com/discussions/microsoft/view/16976-exam-ms-100-topic-3-question-49-discussion/>

upvoted 3 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 the Azure portal, select all the Azure AD users, and then use the User settings blade.

**Correct Answer:** A

✉️  **sergioandreslq** 6 months ago

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.

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 4 times

**HOTSPOT**

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

You need to identify the settings that are configured less secure than the Standard protection profile settings in the preset security policies.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Portal:

- Microsoft 365 admin center
- Microsoft 365 Defender portal
- Microsoft Purview compliance portal

Feature:

- Configuration analyzer
- Preset security policies
- Threat tracker

**Answer Area**

Correct Answer:

Portal:

- Microsoft 365 admin center
- Microsoft 365 Defender portal**
- Microsoft Purview compliance portal

Feature:

- Configuration analyzer**
- Preset security policies
- Threat tracker

CBZ57 5 months, 1 week ago

yep it's right

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/configuration-analyzer-for-security-policies?view=o365-worldwide>  
upvoted 2 times

apokavk 6 months, 1 week ago

seems correct

<https://www.examtopics.com/discussions/microsoft/view/93899-exam-ms-101-topic-1-question-96-discussion/>  
upvoted 4 times

## HOTSPOT

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

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

All the devices are onboarded to Microsoft Defender for Endpoint.

You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:

- Detect operating system vulnerabilities.
- Perform a configuration assessment of the operating system.

Which devices support each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Detect operating system vulnerabilities:

Device1 only  
Device1 and Device2 only  
Device1, Device2, and Device3 only  
Device1, Device2, and Device4 only  
Device1, Device2, Device3, and Device4

Perform a configuration assessment of the operating system:

Device1 only  
Device1 and Device2 only  
Device1, Device2, and Device3 only  
Device1, Device2, and Device4 only  
Device1, Device2, Device3, and Device4

## Answer Area

Detect operating system vulnerabilities:

Device1 only  
Device1 and Device2 only  
Device1, Device2, and Device3 only  
Device1, Device2, and Device4 only  
Device1, Device2, Device3, and Device4

## Correct Answer:

Perform a configuration assessment of the operating system:

Device1 only  
Device1 and Device2 only  
Device1, Device2, and Device3 only  
Device1, Device2, and Device4 only  
Device1, Device2, Device3, and Device4

sergioandreslq 6 months ago

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/tvm-supported-os?view=o365-worldwide#capabilities-per-supported-operating-systems-os-and-platforms>  
upvoted 4 times

apokavk 6 months, 1 week ago

correct  
<https://www.examtopics.com/discussions/microsoft/view/102907-exam-ms-101-topic-2-question-128-discussion/>  
upvoted 3 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

You have a Microsoft 365 E5 tenant.

The Microsoft Secure Score for the tenant is shown in the following exhibit.

## Microsoft Secure Score

Overview Improvement actions History Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export

12 items

Search

Filter

Group by

Applied filters:

Rank	Improvement action	Score impact	Points achieved
1	Require MFA for administrative roles	+16.95%	0/10
2	Ensure all users can complete multi-factor authentication for ...	+15.25%	0/9
3	Enable policy to block legacy authentication	+13.56%	0/8
4	Turn on user risk policy	+11.86%	0/7
5	Turn on sign-in risk policy	+11.86%	0/7
6	Do not allow users to grant consent to unmanaged applicatio...	+6.78%	0/4
7	Enable self-service password reset	+1.69%	0/1
8	Turn on customer lockbox feature	+1.69%	0/1
9	Use limited administrative roles	+1.69%	0/1
10	Designate more than one global admin	+1.69%	0/1

You plan to enable Security defaults for Azure AD.

Which three improvement actions will this affect?

NOTE: Each correct selection is worth one point.

- A. Require MFA for administrative roles
- B. Ensure all users can complete multi-factor authentication for secure access
- C. Enable policy to block legacy authentication
- D. Enable self-service password reset
- E. Use limited administrative roles

**Correct Answer: ABC**

*Community vote distribution*

ABC (100%)

**1428901** 3 weeks, 4 days ago

How?? Administrators are MFA enable by default? MFA data is now used for SSPR. So for It's BCD.  
upvoted 1 times

**Vaerox** 3 months, 1 week ago

**Selected Answer: ABC**

This question is asked multiple times throughout this course. Wish it would be on the actual exam!

upvoted 3 times

✉️ **sergioandreslq** 6 months ago

ABC: Correct

These basic controls include:

- Requiring all users to register for multifactor authentication
- Requiring administrators to do multifactor authentication
- Requiring users to do multifactor authentication when necessary
- Blocking legacy authentication protocols
- Protecting privileged activities like access to the Azure portal

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

upvoted 2 times

✉️ **apokavk** 6 months, 1 week ago

**Selected Answer: ABC**

<https://www.examtopics.com/discussions/microsoft/view/67759-exam-ms-101-topic-2-question-90-discussion/>

upvoted 3 times

店铺：学习小店66

Question #261

Topic 1

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Intune.

Devices are enrolled to Microsoft Intune and 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. an endpoint detection and response policy
- C. a device compliance policy

**Correct Answer: C**

✉️ **sergioandreslq** 6 months ago

C: Correct

Configure a Device compliance policy that takes into consideration the Defender for endpoint to define if device is compliant or not compliant

<https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows#microsoft-defender-for-endpoint-rules>

upvoted 2 times

店铺：学习小店66

店铺：学习小店66

You have a Microsoft 365 subscription.

You create a retention label named Retention1 as shown in the following exhibit.

## Create retention label

- Name
- Label Settings
- Period
- Finish

### Review and finish

Name  
Retention1  
[Edit](#)

### Retention settings

Retention period	Retention action
6 months	<a href="#">Retain and Delete</a>
<a href="#">Edit</a>	<a href="#">Edit</a>

### Based on

Based on when it was created  
[Edit](#)

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

Amir1909 3 months ago

B is correct  
upvoted 3 times

sergioandresiq 6 months ago

B: Correct  
retain the item for 6 months using the date reference when it was created.  
the file1 was created on Jan 01, 2020, this file1 will be deleted automatically after 6 months in Jul 01, 2020.  
upvoted 4 times

feperezv 4 months, 2 weeks ago

Could you respond to questions 186 187 197 201 205 238 248 263-267 please?  
upvoted 1 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

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. Global Administrator
- B. Service Administrator
- C. Security Administrator
- D. Reports Reader

**Correct Answer: D**

*Community vote distribution*

C (92%) 8%

✉  **solderboy**  3 months, 3 weeks ago

**Selected Answer: C**

The risky sign-ins reports are available to users in the following roles:

- Security Administrator
- Global Administrator
- Security Reader

There are several versions of this question in the exam. The question has three possible correct answers:

1. Security Reader
2. Security Administrator
3. Global Administrator

Other incorrect answer options you may see on the exam include the following:

1. Service Administrator.
  2. Reports Reader
  3. Compliance Administrator
- upvoted 9 times

✉  **darcone23**  23 hours, 47 minutes ago

**Selected Answer: D**

Security Reader  
upvoted 1 times

✉  **SBGM** 2 months, 4 weeks ago

**Selected Answer: C**

Solder is correct in my opinion  
upvoted 2 times

✉  **SBGM** 2 months, 4 weeks ago

<https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection#required-roles>

"Identity Protection requires users be a Security Reader, Security Operator, Security Administrator, Global Reader, or Global Administrator in order to access."

upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 E5 tenant.

You have a sensitivity label configured as shown in the Sensitivity label exhibit.

**Review your settings and finish**

**Name**  
Sensitivity1  
  
**Display name**  
Sensitivity1  
  
**Description for users**  
Sensitivity1  
  
**Scope**  
File,Email  
  
**Encryption**  
  
**Content marking**  
Watermark: Watermark  
Header: Header  
  
**Auto-labeling**  
  
**Group settings**  
  
**Site settings**  
  
**Auto-labeling for database columns**  
None

You have an auto-labeling policy as shown in the Auto-labeling policy exhibit.

**Auto-labeling policy**

 Edit policy  Delete policy

**Policy name**  
Auto-labeling policy

**Description**

**Label in simulation**  
Sensitivity1

**Info to label**  
IP Address

**Apply to content in these locations**  
Exchange email All

**Rules for auto-applying this label**  
Exchange email 1 rule

**Mode**  
On

**Comment**

A user sends an email that contains the components shown in the following table.

Type	File	Includes IP address
Mail body	<i>Not applicable</i>	No
Attachment	File1.docx	Yes
Attachment	File2.xml	Yes

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 the email.	<input type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input type="radio"/>

店铺：学习小店66

店铺：学习小店66

## Answer Area

	Statements	Yes	No
Correct Answer:	Sensitivity1 is applied to the email.	<input checked="" type="checkbox"/>	<input type="radio"/>
	A watermark is added to File1.docx.	<input type="radio"/>	<input checked="" type="checkbox"/>
	A header is added to File2.xml.	<input type="radio"/>	<input checked="" type="checkbox"/>

Tomtom11 1 month, 3 weeks ago

<https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically?view=o365-worldwide>

Specific to auto-labeling for Exchange:

PDF attachments and Office attachments are scanned for the conditions you specify in your auto-labeling policy. When there's a match, the email is labeled but not the attachment.

upvoted 1 times

solderboy 3 months, 3 weeks ago

Answers are correct

<https://www.examtopics.com/discussions/microsoft/view/65201-exam-ms-101-topic-3-question-100-discussion/>

upvoted 1 times

店铺：学习小店66

店铺：学习小店66

You have a Microsoft 365 subscription.

You need to implement a passwordless authentication solution that supports the following device types:

- Windows
- Android
- iOS

The solution must use the same authentication method for all devices.

Which authentication method should you use?

- A. the Microsoft Authentication app
- B. FIDO2-compliant security keys
- C. multi-factor authentication (MFA)
- D. Windows Hello for Business

**Correct Answer: B**

*Community vote distribution*

A (55%)      B (45%)

✉ **solderboy** Highly Voted 3 months, 3 weeks ago

**Selected Answer: A**

<https://www.examtopics.com/discussions/microsoft/view/81291-exam-ms-100-topic-5-question-73-discussion/>  
upvoted 6 times

✉ **Sesbri** 3 months, 2 weeks ago

I agree to use Answer A. For the named platforms it must be authenticator app.  
upvoted 1 times

✉ **Vaerox** 3 months, 2 weeks ago

But you can't use the Authenticator app on Windows. The question states that all devices must be supported. You can use a FIDO2 USB device you want to log in on all the devices in an Office app (such as Outlook Mobile).  
upvoted 2 times

✉ **Wuhao** Most Recent 6 days, 17 hours ago

**Selected Answer: B**

no Authenticator on Windows  
upvoted 1 times

✉ **Jeeda8998** 1 month, 2 weeks ago

**Selected Answer: B**

Chat gpt says b  
upvoted 1 times

✉ **Tomtom11** 1 month, 3 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless#fido2-security-keys>  
upvoted 1 times

✉ **Bouncy** 2 months, 2 weeks ago

**Selected Answer: B**

As stated by others, no Authenticator on Windows, hence B  
upvoted 1 times

✉ **SBGM** 3 months, 1 week ago

**Selected Answer: B**

I think B is correct since there is no Authenticator app for Windows and the question states that the same method must be used on all platforms.  
upvoted 2 times

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

店铺：学习小店66

**HOTSPOT**

You have a Microsoft 365 subscription.

You need to configure an auto-apply policy for sensitivity labels that will protect corporate data. The solution must meet the following requirements:

- Documents containing content that matches a custom regular expression must be classified automatically.
- Contract documents in a standard format must be classified automatically.

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**

Documents containing content that matches a custom regular expression must be classified automatically:

- A sensitive info type
- A trainable classifier
- An exact data match (EDM) schema

Contract documents in a standard format must be classified automatically:

- A data connector
- A trainable classifier
- An exact data match (EDM) schema

**Answer Area**

Documents containing content that matches a custom regular expression must be classified automatically:

- A sensitive info type
- A trainable classifier
- An exact data match (EDM) schema

Correct Answer:

Contract documents in a standard format must be classified automatically:

- A data connector
- A trainable classifier
- An exact data match (EDM) schema

✉  **darcone23** 23 hours, 39 minutes ago

1. EDM
2. Trainable classifier

upvoted 1 times

✉  **dilmah** 1 month, 2 weeks ago

1 is EDM To automatically classify documents based on customer-defined regular expressions, you can leverage the power of Exact Data Match (EDM)

and 2. SIt is needed but close enough is trainable classifier.

upvoted 1 times

✉  **SBGM** 3 months ago

Second is definitely a Trainable Classifier, as it has the ability recognize an item based on a template: <https://learn.microsoft.com/en-us/purview/classifier-learn-about#automated-pattern-matching>

upvoted 2 times

✉  **sgoncharuk** 3 months, 2 weeks ago

1. Trainable classifier
2. EDM

upvoted 2 times

✉  **TonyTe0** 3 months, 3 weeks ago

The second should be Trainable classifiers.

When you publish the classifier, it sorts through items in locations like SharePoint Online, Exchange, and OneDrive, and classifies the content. After you publish the classifier, you can continue to train it using a feedback process that is similar to the initial training process.

For example you could create trainable classifiers for:

Legal documents - such as attorney client privilege, closing sets, statement of work

Strategic business documents - like press releases, merger and acquisition, deals, business or marketing plans, intellectual property, patents, design docs

Pricing information - like invoices, price quotes, work orders, bidding documents

Financial information - such as organizational investments, quarterly or annual results

<https://learn.microsoft.com/en-us/purview/classifier-learn-about>

upvoted 4 times

曰  **Sesbri** 3 months, 2 weeks ago

I agree, the 2nd one is trainable classifier.

upvoted 2 times

曰  **TonyTe0** 3 months, 3 weeks ago

Looks correct

<https://learn.microsoft.com/en-us/purview/sensitive-information-type-learn-about#sensitive-information-types-are-used-in-sites>

<https://learn.microsoft.com/en-us/purview/sit-learn-about-exact-data-match-based-sits>

upvoted 1 times

## HOTSPOT

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

Name	Membership type	Membership rule
Group1	Assigned	<i>Not applicable</i>
Group2	Dynamic	(user.department -eq "Finance")
Group3	Dynamic	(user.department -eq "R&D")

The subscription contains the users shown in the following table.

Name	Department	Assigned group membership
User1	Finance	Group1
User2	Technical	<i>None</i>
User3	R&D	Group1

You have a Conditional Access policy that has the following settings:

- Assignments
  - Users
    - Include: Group1
    - Exclude: Group2, Group3
  - Target resources
    - Cloud apps
      - App1
    - Access controls
      - Grant
      - Block access

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 App1.	<input type="radio"/>	<input type="radio"/>
User2 can sign in to App1.	<input type="radio"/>	<input type="radio"/>
User3 can sign in to App1.	<input type="radio"/>	<input type="radio"/>

## Answer Area

Statements	Yes	No
Correct Answer: User1 can sign in to App1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in to App1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can sign in to App1.	<input checked="" type="radio"/>	<input type="radio"/>

曰 **TONYTeO** Highly Voted 3 months, 3 weeks ago

Should be YYY  
User2 is not applied the CA  
upvoted 11 times

店铺：学习小店66

曰 **TONYTeO** Highly Voted 3 months, 3 weeks ago

CA is not applied, so not blocked. So can sign in the app1. (YYY)

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-policy-unknown-unsupported-device>  
upvoted 5 times

曰 **TonyManero** Most Recent 1 day, 21 hours ago

I think NYN because:  
In Azure, within a Conditional Access policy, when a user belongs to multiple groups with contrasting configurations, precedence follows the rule of least privilege.  
upvoted 1 times

曰 **JMB7448** 3 weeks, 3 days ago

I believe it is NYN

Here is why:  
User 1 is in group1 and group 2  
User 2 is not in a group  
User 3 is in group1 and group 3

User 1 = N -> Block always wins (because of membership group1)  
User 2 = y -> policy does not apply  
User 3 = N -> Block always wins (because of membership group1)  
upvoted 2 times

曰 **solderboy** 3 months, 3 weeks ago

NNN

User1 is in Group1 (static assigned) and Group2 (dynamic assigned). CA includes Group1 but excludes Group2. Since exclusion takes precedence over inclusion, CA is not applied to User1. So, User1 cannot sign in to App1.

User2 is not in any group hence CA is not applied. So, User2 cannot sign in to App1.

User3 is in Group1 (static assigned) and Group3 (dynamic assigned). CA includes Group1 but excludes Group2. Since exclusion takes precedence over inclusion, CA is not applied to User3. So, User3 cannot sign in to App1.

Please correct if I am wrong!  
upvoted 3 times

曰 **SBGM** 3 months ago

I think TONYTeO is right, both of the members in group 1 (Users 1 & 3) are also in dynamic groups 2 & 3, thus excluded. The policy blocks access. Since it won't be applied to all 3 users and users without a CA policy applied can freely access they will all be able to access the app.  
upvoted 4 times

Your company has a Microsoft Entra tenant named contoso.com and a Microsoft 365 subscription.

All users use Windows 10 devices to access Microsoft Office 365 apps.

All the devices are in a workgroup.

You plan to implement password less sign-in to contoso.com.

You need to recommend changes to the infrastructure for the planned implementation.

What should you include in the recommendation?

- A. Join all the devices to contoso.com.
- B. Deploy Microsoft Entra Application Proxy.
- C. Deploy X.509.3 certificates to all the users.
- D. Deploy the Microsoft Authenticator app.

**Correct Answer:** D

*Community vote distribution*

A (100%)

✉️  **TonyManero** 1 day, 20 hours ago

**Selected Answer: A**

The best recommendation to implement passwordless sign-in for your scenario is:

- A. Join all the devices to contoso.com

Here's why the other options are not ideal:

- B. Deploy Microsoft Entra Application Proxy: This is not necessary for passwordless sign-in. Application Proxy publishes on-premises applications to Azure Active Directory (Azure AD) but doesn't directly affect passwordless login functionality.
- C. Deploy X.509.3 certificates to all the users: While certificates can be used for passwordless authentication, it's a more complex solution compared to Azure AD joined devices.
- D. Deploy the Microsoft Authenticator app: While the Microsoft Authenticator app can be used for multi-factor authentication (MFA) which can be part of a passwordless solution, it requires Azure AD joined devices to leverage Windows Hello for passwordless sign-in.

Since your users are already using Windows 10 devices and you want passwordless sign-in, joining the devices to the Azure AD domain (contoso.com) allows them to leverage Windows Hello for passwordless login with features like fingerprint or facial recognition. This is a simpler and more efficient approach for your scenario.

upvoted 1 times

✉️  **arsh807** 3 weeks, 1 day ago

**Selected Answer: A**

How do you plan to use Authenticator without joining the devices to the domain?

upvoted 1 times

✉️  **TonyTe0** 3 months, 3 weeks ago

Correct: D

<https://www.examtopics.com/discussions/microsoft/view/75062-exam-ms-100-topic-4-question-1-discussion/>

upvoted 3 times

**HOTSPOT**

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

You need to enable multi-factor authentication (MFA) for the members of Group1 and Group2. The solution must meet the following requirements:

- The Group1 members must be prompted for MFA only when authenticating to Microsoft Entra ID from Android devices.
- The Group2 members must be prompted for MFA only when accessing Microsoft Exchange Online from outside the corporate network.
- Administrative effort must be minimized.

What should you configure for each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Group1:

- Microsoft Entra Identity Protection
- Microsoft Entra Privileged Identity Management (PIM)
- Conditional Access
- Per-user MFA
- Microsoft Entra Security defaults

Group2:

- Microsoft Entra Identity Protection
- Microsoft Entra Privileged Identity Management (PIM)
- Conditional Access
- Per-user MFA
- Microsoft Entra Security defaults

**Answer Area**

Group1:

- Microsoft Entra Identity Protection
- Microsoft Entra Privileged Identity Management (PIM)
- Conditional Access
- Per-user MFA
- Microsoft Entra Security defaults

Correct Answer:

Group2:

- Microsoft Entra Identity Protection
- Microsoft Entra Privileged Identity Management (PIM)
- Conditional Access
- Per-user MFA
- Microsoft Entra Security defaults

✉  **TonyTeo**  3 months, 3 weeks ago

Wrong answer

Correct

Group1 : CA

Group2: CA

upvoted 16 times

✉  **Sesbri** 3 months, 2 weeks ago

For me too. Must be CA for both.

upvoted 1 times

✉  **oopspruu** Most Recent 1 week, 3 days ago

Security Defaults and CAPs cannot co-exist. Answer is CAP for both.

upvoted 1 times

✉  **examcrammer** 2 weeks ago

You cannot use both Security Defaults and CA in the same Entra tenancy.

upvoted 1 times

Question #270

Topic 1

You have a Microsoft 365 E5 subscription.

店铺：学习小店66

You need to create a mail-enabled contact.

店铺：学习小店66

Which portal should you use?

- A. the Microsoft 365 admin center
- B. the Microsoft Teams admin center
- C. the Intune admin center
- D. the Microsoft Purview compliance portal

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉  **TonyManero** 1 day, 18 hours ago

Selected Answer: A

365 Admin center o Exchange Admin center only.

upvoted 1 times

✉  **arsh807** 3 weeks, 1 day ago

Selected Answer: A

It can be created in Microsoft 365 admin center or Exchange admin center. All other given options are clearly incorrect.

<https://learn.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-mail-contacts>

upvoted 2 times

✉  **swoam** 3 months, 3 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/microsoft/view/120633-exam-ms-102-topic-1-question-170-discussion/>

upvoted 2 times

✉  **TomBoy25** 3 months, 3 weeks ago

Can also be Exchange Administration portal

upvoted 2 times

店铺：学习小店66

## HOTSPOT

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

Name	Role	Role assignment type
User1	Global Administrator	Eligible
User2	Global Administrator	Assigned
User3 <sup>店铺: 学习小店66</sup>	Global Administrator	Eligible

The Global Administrator role has the Privileged Identity Management (PIM) settings shown in the following table.

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
Expire eligible assignments after	15 Days

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 must provide justification to activate the Global Administrator role.	<input type="radio"/>	<input type="radio"/>
User2 must perform multifactor authentication (MFA) to activate the Global Administrator role.	<input type="radio"/>	<input type="radio"/>
After eight hours, User3 will no longer be able to activate the Global Administrator role.	<input type="radio"/>	<input type="radio"/>

## Answer Area

	Statements	Yes	No
Correct Answer:	User1 must provide justification to activate the Global Administrator role.	<input checked="" type="radio"/>	<input type="radio"/>
	User2 must perform multifactor authentication (MFA) to activate the Global Administrator role.	<input checked="" type="radio"/>	<input type="radio"/>
	After eight hours, User3 will no longer be able to activate the Global Administrator role.	<input type="radio"/>	<input checked="" type="radio"/>

✉️  **TonyTe0** Highly Voted 3 months, 3 weeks ago

Y

N: Because user2 was assigned  
N: After 8 hours, User3 can activate again

upvoted 12 times

✉️  **Tomtom11** Most Recent 1 month, 3 weeks ago

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings>  
upvoted 1 times

✉️  **Tomtom11** 1 month, 3 weeks ago

Eligible assignments require the member of the role to perform an action to use the role. Actions might include activation, or requesting approval from designated approvers.  
Active assignments don't require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role.

upvoted 1 times

✉️  **Tomtom11** 1 month, 3 weeks ago

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure>

Term or concept Role assignment category Description

eligible Type A role assignment that requires a user to perform one or more actions to use the role. If a user has been made eligible for a role, that means they can activate the role when they need to perform privileged tasks. There's no difference in the access given to someone with a permanent versus an eligible role assignment. The only difference is that some people don't need that access all the time.  
active Type A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role.

upvoted 1 times

✉️  **solderboy** 3 months, 3 weeks ago

YNY

YES, User1 must provide justification as per the PIM setting.  
NO, User2 is already assigned. No need activation again.  
YES, User3 will no longer be able to activate after 8 hours as per the PIM setting.

upvoted 1 times

✉️  **ITCALegends** 3 months, 2 weeks ago

i think you are correct for user 3, If PIM is configured with an activation duration, such as 8 hours in your example, it means that the elevated privileges granted to a user through PIM will expire after that period. After the specified duration, the user will lose the Global Admin role assigned through PIM until they request and activate it again.

upvoted 1 times

✉️  **SBGM** 3 months ago

I work with PIM configured similarly in my production environment and when the activation expires you can immediately re-activate. After the 15 day eligibility expires the role can not be activated unless requested again. I therefore think the answer is no, like Tony stated above after 8 hours User 3 can activate again immediately.

upvoted 3 times

## DRAG DROP

You have an Azure subscription that is linked to a hybrid Microsoft Entra tenant.

All users sync from Active Directory Domain Services (AD DS) to the tenant by using Express Settings in Microsoft Entra Connect.

You plan to implement self-service password reset (SSPR).

You need to ensure that when a user resets or changes a password, the password syncs with AD DS.

Which actions should you perform in sequence? To answer, drag the appropriate actions to the correct order. Each action 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.

**Actions**

From the Microsoft Entra admin center, configure on-premises integration password writeback.

From the Microsoft Entra admin center, configure the authentication methods for SSPR.

From the Microsoft Entra admin center, configure the registration settings for SSPR.

Select Group writeback in Microsoft Entra Connect.

Select Password writeback in Microsoft Entra Connect.

**Answer Area**

Step 1:

Step 2:

Step 3:

**Answer Area**

Step 1: From the Microsoft Entra admin center, configure the registration settings for SSPR.

**Correct Answer:** Step 2: Select Password writeback in Microsoft Entra Connect.

Step 3: From the Microsoft Entra admin center, configure on-premises integration password writeback.

✉️  **oopsruu** 1 week, 3 days ago

The express settings don't have password writeback. So the very first thing you need to enable is password writeback feature form AAD Connect on-premise. Then you can come back and define SSPR registration and authentication methods.

upvoted 2 times

✉️  **Rohgun** 2 weeks, 5 days ago

1. Configure on-premises integration password writeback
2. Configure authentication methods for SSPR.
3. Configure registration methods for SSPR.

i don't think you need the last step Select Password writeback because this one ist in step 1 - Configure on-premises integration password writeback. But you need authetication and registration for SSPR

upvoted 2 times

✉️  **arsh807** 3 weeks, 1 day ago

1. Configure on-premises integration password writeback.
2. Configure authentication methods for SSPR.
3. Select password writeback in Entra Connect.

upvoted 1 times

✉️  **sgoncharuk** 3 months, 3 weeks ago

I think the first step is to configure authentication methods, not the registration settings

upvoted 4 times

✉️  **TonyTe0** 3 months, 3 weeks ago

Correct answer

<https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-cloud-sync-sspr-writeback>

<https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr>

upvoted 4 times

Question #273

Topic 1

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

You need to compare your company's security configurations to Microsoft best practices and review improvement actions to increase the security posture.

What should you use?

- A. Microsoft Secure Score
- B. Cloud discovery
- C. Exposure distribution
- D. Threat tracker
- E. Exposure score

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉️  **arsh807** 3 weeks, 1 day ago

**Selected Answer: A**

Easy.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide>  
upvoted 1 times

✉️  **SBGM** 3 months, 1 week ago

**Selected Answer: A**

Correct

upvoted 2 times

✉️  **TonyTe0** 3 months, 3 weeks ago

Correct

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide>  
upvoted 1 times

**HOTSPOT**

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

You need to automate Attack simulation training for users when a phishing campaign is detected in real-time.

Which type of automation should you use, and which condition should you configure for the Attack simulation training? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Automation type:

- Fixed simulation automation
- Payload automation
- Randomized simulation automation

Condition:

- Credential Harvest
- How-to Guide
- Malware Attachment

**Answer Area**

Automation type:

- Fixed simulation automation
- Payload automation**
- Randomized simulation automation

Condition:

- Credential Harvest**
- How-to Guide
- Malware Attachment

✉  arsh807 3 weeks, 1 day ago

Automation Type - Payload automation

Condition - Any of the three should be okay really

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-payload-automations?view=o365-worldwide>

upvoted 1 times

✉  TonyTe0 3 months, 3 weeks ago

Correct answer

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-payload-automations?view=o365-worldwide>

upvoted 1 times

You have two Microsoft 365 tenants. Users have accounts in both tenants.

You plan to deploy a single device to each user. Each device will contain the Microsoft Authenticator app.

You need to ensure that the users can use their device to authenticate to both tenants by using passwordless authentication.

Which platform should you provide?

- A. iOS
- B. Android
- C. Windows
- D. macOS

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉️  **Wuhao** 6 days, 16 hours ago

You can enable passwordless phone sign-in for multiple accounts in Microsoft Authenticator on any supported iOS device. Consultants, students, and others with multiple accounts in Microsoft Entra ID can add each account to Microsoft Authenticator and use passwordless phone sign-in for all of them from the same iOS device.

upvoted 1 times

✉️  **Charlie33** 1 week, 5 days ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-passwordless-phone>

upvoted 1 times

✉️  **Motanel** 1 week, 6 days ago

**Selected Answer: A**

Answer correct

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-passwordless-phone>

upvoted 2 times

Your network contains an Active Directory domain named adatum.com that is synced to a Microsoft Entra tenant.

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-MgUser and Update-MgUser cmdlets.
- C. From the Microsoft Entra admin center, select all the Microsoft Entra users, and then use the User settings blade.
- D. From the Microsoft 365 admin center, select the users, and then use the Bulk actions option.

**Correct Answer: A**

*Community vote distribution*

✉️  **TonyManero** 1 day, 17 hours ago

**Selected Answer: A**

Sync from onprem, so you have to modify from onprem.  
upvoted 1 times

✉️  **examcrammer** 1 week, 5 days ago

**Selected Answer: A**

Correct  
upvoted 2 times

**HOTSPOT**

You have a Microsoft 365 subscription.

You need to identify all users that have an Enterprise Mobility + Security plan, and then provide a list of the users in the CSV format.

Which settings should you use in the Microsoft 365 admin center, and which option should you select? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Settings:

- Billing accounts
- Bills & payments
- Licenses
- Your products

Option:

- Export users
- Show history list
- View apps and services with this subscription

**Correct Answer:**

Answer Area

Settings:

- Billing accounts
- Bills & payments
- Licenses**
- Your products

Option:

- Export users**
- Show history list
- View apps and services with this subscription

✉  **examcrammer** 1 week, 5 days ago

Correct

upvoted 1 times

✉  **Motanel** 1 week, 6 days ago

Answer is correct, just tested in my lab.

In Licenses, select the License and export the users.

upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 subscription that contains two administrative units named AU1 and AU2.

The subscription contains the users shown in the following table.

Name	Administrative unit	Role	Scope
User1	<i>None</i>	User Administrator	AU1
User2	AU1	Global Administrator	<i>None</i>
User3	<i>None</i>	<i>None</i>	Organization

The subscription contains the groups shown in the following table.

Name	Members	Administrative unit
Group1	User3	AU2
Group2	User2 User3	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 User2.	<input type="radio"/>	<input type="radio"/>
User2 can modify the membership of Group1.	<input type="radio"/>	<input type="radio"/>
User1 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>

**Answer Area**

Statements	Yes	No
Correct Answer: User1 can reset the password of User2.	<input checked="" type="checkbox"/>	<input type="radio"/>
User2 can modify the membership of Group1.	<input checked="" type="checkbox"/>	<input type="radio"/>
User1 can reset the password of User3.	<input type="radio"/>	<input checked="" type="checkbox"/>

✉  **oopspruu** 1 week, 3 days ago

NYN

A user admin can never reset the password of a Global Admin, AU or not. That's a huge security risk if you use common sense.  
upvoted 2 times

✉  **Motanel** 1 week, 6 days ago

No - The User Admin can not reset the password for the Global Admin, User2 is not in direct scope.

Yes The Global Admin he can manage all aspects of Entra ID

No User3 is not in the same scope as User1

upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 subscription.

You plan to update the EmployeeType attribute for all the users in a group named Contractors. You retrieve the GroupId value of the Contractors group.

You need to use Microsoft Graph PowerShell to retrieve all the Contractors group users and set their EmployeeType attribute to Part-time.

How should you complete the PowerShell script? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

```
foreach ($person in $(  
    Get-AzureADUser  
    Get-MgGroupMember  
    Get-MgUser  
))  
  
{  
    $person.ObjectId -EmployeeType "Part-time"}  
  
Set-AzureADUser  
Set-MsolUser  
Update-MgUser  
-DisplayName  
-ObjectId  
-UserId
```

**Answer Area**

```
foreach ($person in $(  
    Get-AzureADUser  
    Get-MgGroupMember  
    Get-MgUser  
))  
    $person.ObjectId -EmployeeType "Part-time"
```

**Correct Answer:**

```
{  
    Set-AzureADUser  
    Set-MsolUser  
    Update-MgUser  
    -DisplayName  
    -ObjectId  
    -UserId
```

✉ **Motanel** 1 week, 5 days ago

answer is correct

<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/update-mguser?view=graph-powershell-1.0>  
upvoted 2 times

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

You need to configure Privileged Identity Management (PIM) for the User Administrator role in Microsoft Entra. Eligible users must meet the following requirements:

- Always be able to request the User Administrator role
- Must provide a reason when requesting the User Administrator role
- Must require multi-factor authentication (MFA) when activating the User Administrator role

The solution must minimize administrative effort.

How should you configure the Role settings for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Always be able to request the User Administrator role:

Select Require approval to activate.  
Set Allow permanent active assignment to yes.  
Set Allow permanent eligible assignment to yes.

Must provide a reason when requesting the User Administrator role:

Select Require justification on activation.  
Select Require ticket information on activation.  
Select Require justification on active assignment to Yes.

Must require MFA when activating the User Administrator role:

Select On activation require to Azure MFA.  
Select On activation require to Microsoft Entra Conditional Access authentication context.  
Select Require Azure Multi-Factor Authentication on active assignment to Yes.

**Answer Area**

Always be able to request the User Administrator role:

Select Require approval to activate.  
Set Allow permanent active assignment to yes.  
Set Allow permanent eligible assignment to yes.

Must provide a reason when requesting the User Administrator role:

Select Require justification on activation.  
Select Require ticket information on activation.  
Select Require justification on active assignment to Yes.

**Correct Answer:**

Must require MFA when activating the User Administrator role:

Select On activation require to Azure MFA.  
Select On activation require to Microsoft Entra Conditional Access authentication context.  
Select Require Azure Multi-Factor Authentication on active assignment to Yes.

✉  **oopspruu** 1 week, 3 days ago

The answer for last one is option 3.

upvoted 1 times

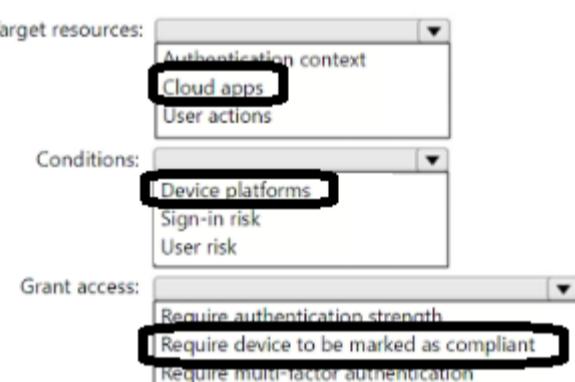
**HOTSPOT**

You have a Microsoft 365 E5 subscription.

You need to create a Conditional Access policy that will require the use of FIDO2 security keys only when users join their Windows devices to Microsoft Entra ID.

How should you configure the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area****Correct Answer:****Answer Area**

✉️ **Motanel** Highly Voted 1 week, 5 days ago

User Actions - here you choose the policy to apply when the user joins the device.

Device Platform - because it is a Windows device

Require authentication strength - to require FIDO2 Key

upvoted 5 times

✉️ **TonyManero** Most Recent 1 day, 16 hours ago

<https://cloudbrothers.info/en/fido2-security-keys-are-important/>

For the user action "Register or join devices" there is only the "Require multi-factor authentication" option available.

upvoted 1 times

✉️ **oopspruu** 1 week, 3 days ago

1. User Actions

2. Device Platform

3. You can only use "Require MFA" with the Join or Register device user action. Tested in lab.

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. name server (NS)
- B. host information (HINFO)
- C. text (TXT)
- D. pointer (PTR)

**Correct Answer: C**

You have a Microsoft 365 E5 subscription.

From the Microsoft 365 Defender portal, you review your company's Microsoft Secure Score.

You discover a large number of recommended actions.

You need to ensure that the actions can be filtered based on specific department names.

What should you create first?

- A. a dynamic security group
- B. a tag
- C. an administrative unit
- D. a custom detection rule

**Correct Answer: A**

*Community vote distribution*

B (83%) C (17%)

✉️  **examcrammer** 1 week, 5 days ago

**Selected Answer: B**

tested, create a tag on 1 recommendation, refresh the Defender portal, and the tag name shows up for filtering.  
upvoted 4 times

✉️  **Name\_** 1 week, 5 days ago

**Selected Answer: B**

<https://security.microsoft.com/securescore>  
The only option for filtering from these answers is TAG  
upvoted 1 times

✉️  **egman18** 1 week, 5 days ago

**Selected Answer: C**

C. an administrative unit

The reasoning behind this answer is that an administrative unit in Microsoft 365 allows for the organization of users based on different departments or other criteria, such as geographical location or job function. Once these users are organized into administrative units, various settings and policies, including those related to security, can be applied specifically to these units. In the context of Microsoft Secure Score, being able to filter recommendations based on specific departments will require that these departments are first organized in a way that they can be individually addressed, which is facilitated by creating administrative units. This allows for a more targeted and efficient management of the recommendations based on the particular needs and characteristics of each department.

upvoted 1 times