



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

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)

Suggested Answer: C

Community vote distribution

C (100%)

 **oszvkwpcfxfobqjby** Highly Voted 1 year, 4 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 12 times

 **AvoKikinha** Highly Voted 3 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 5 times

 **meeeert** Most Recent 2 months, 1 week ago

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 1 times

 **iamchoy** 6 months, 3 weeks ago

Selected Answer: C

C for domain verification

upvoted 1 times

 **abul8223** 7 months, 2 weeks ago

Selected Answer: C

C is the correct answer.

upvoted 1 times

 **AvoKikinha** 1 year, 1 month 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

 **miki** 1 year, 3 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** 1 year, 4 months 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.

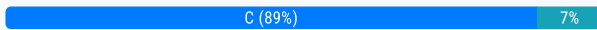
Which authentication strategy should you implement for the pilot projects?

- A. pass-through authentication

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

Suggested Answer: C

Community vote distribution



osxvkwpcfxfobqjby Highly Voted 1 year, 4 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 25 times

Kock Most Recent 3 days, 5 hours ago

Selected Answer: A

<https://learn.microsoft.com/pt-br/microsoft-365/enterprise/deploy-identity-solution-identity-model?view=o365-worldwide>

upvoted 1 times

Kock 1 week ago

Resposta |A

identidade somente na nuvem

autenticação federada

autenticação de passagem (PTA)

Esta resposta está correta.

sincronização de hash de senha (PHS)

Essa resposta está incorreta.

A autenticação de passagem (PTA) e a autenticação federada dão suporte ao uso de domínios locais do Active Directory para autenticação.

A sincronização de hash de senha e a identidade somente na nuvem são usadas para garantir que o Microsoft Entra ID forneça autenticação.

<https://learn.microsoft.com/pt-br/microsoft-365/enterprise/deploy-identity-solution-identity-model?view=o365-worldwide>

upvoted 1 times

Kock 1 month ago

Selected Answer: D

AD FS is a Microsoft service that provides single sign-on (SSO) and identity federation capabilities. AD FS allows users to authenticate using their on-premises Active Directory credentials and access resources in cloud or partner environments without the need for separate identities or credentials.

<https://learn.microsoft.com/pt-br/training/modules/explore-identity-synchronization/3-examine-authentication-options>

upvoted 1 times

TristanForest 4 months, 1 week ago

Selected Answer: D

Technical Requirements -

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

Seamless Single Sign-On (Seamless SSO): This method allows users to automatically sign in when they are on the corporate network. However, it still relies on the on-premises AD for authentication. If the on-premises AD is unavailable, users will not be able to authenticate

upvoted 2 times

🗨️ 👤 **Charard** 11 months, 3 weeks ago

Selected Answer: C

C is the correct answer as explanations below.

upvoted 2 times

🗨️ 👤 **Saj_316** 1 year ago

Selected Answer: C

Hash Sync and SSO

upvoted 1 times

🗨️ 👤 **AvoKikinha** 1 year, 1 month 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** 1 year, 1 month ago

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

upvoted 3 times

🗨️ 👤 **rfree** 1 year, 2 months 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 3 times

🗨️ 👤 **Kock** 1 week ago

identidade somente na nuvem

autenticação federada

autenticação de passagem (PTA)

Esta resposta está correta.

sincronização de hash de senha (PHS)

Essa resposta está incorreta.

A autenticação de passagem (PTA) e a autenticação federada dão suporte ao uso de domínios locais do Active Directory para autenticação.

A sincronização de hash de senha e a identidade somente na nuvem são usadas para garantir que o Microsoft Entra ID forneça autenticação.

<https://learn.microsoft.com/pt-br/microsoft-365/enterprise/deploy-identity-solution-identity-model?view=o365-worldwide>

upvoted 1 times

🗨️ 👤 **letters1234** 1 year, 4 months ago

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

upvoted 1 times

Overview -

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

Existing Environment -

Active Directory Environment -

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

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com. Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

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

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

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

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

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

Requirements -

Planned Changes -

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

Fabrikam plans to implement two pilot projects:

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

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

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

Technical Requirements -

Fabrikam identifies the following technical requirements:

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

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

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

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

Disruptions to email access must be minimized.

Application Requirements -

Fabrikam identifies the following application requirements:

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

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

Security Requirements -

Fabrikam identifies the following security requirements:

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

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

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

The principle of least privilege must be used.

Which role should you assign to User1?

A. Hygiene Management

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

Suggested Answer: B

Community vote distribution

B (100%)

 **Nilz76** Highly Voted 1 year, 3 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 9 times

 **oszvkwpcfxobqjby** Highly Voted 1 year, 4 months ago

Selected Answer: B

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


upvoted 8 times

 **MR_Eliot** Most Recent 4 months, 1 week ago

Selected Answer: B

B is correct.

upvoted 1 times

 **iamchoy** 6 months, 3 weeks ago

Selected Answer: B

OBVIOUSLY B

upvoted 1 times


 **Kaybee2022** 9 months, 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/purview-compliance-portal-permissions>

upvoted 2 times

 **Charard** 11 months, 3 weeks ago

Selected Answer: B


Security reader is the correct answer.

upvoted 1 times

 **AvoKikinha** 1 year, 1 month 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 3 times

 **Nocho** 1 year, 1 month 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 4 times

 **dede321** 1 year, 1 month 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** 1 year, 2 months 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

Enabled

Last Sync

Less than 1 hour ago

Password Hash Sync

Enabled



USER SIGN-IN



Federation

Disabled

0 domains

Seamless single sign-on

Disabled

0 domains

Pass-through authentication

Disabled

0 agents

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

NOTE: Each correct selection is worth one point.

Answer Area

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

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

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

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

Answer Area

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

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

Suggested 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

oszvkwpcfxobqjby Highly Voted 1 year, 4 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 33 times

 **Jonnaz** Highly Voted 3 months, 1 week 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 applications¹. 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 resources². 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 Project1, as well as minimizing disruptions to email access.

upvoted 6 times

 **Moazzamfarooqiiii** 10 months, 2 weeks ago

i dont think thats correct

upvoted 2 times

 **aleper85** 1 year 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 5 times

 **668cffd** 12 months ago

Seamless SSO ist not enabled, but thats not the question, so SSO is possible

upvoted 2 times

 **Perycles** 11 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** 11 months, 3 weeks ago

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

upvoted 2 times

 **Kock** Most Recent 1 month, 2 weeks ago

A vantagem dessa abordagem é que os usuários podem usar o SSO (logon único) para acessar recursos locais e baseados em nuvem.

<https://learn.microsoft.com/pt-br/training/modules/manage-users-and-groups-in-aad/3-users>

upvoted 1 times

 **DasChi_cken** 4 months ago

1) on-prem only: sso for the on-prem Environment was already preconfigured (stated in the first paragrah) but ist still disabled on the could (visable from the screenshot)

2) cloud Apps only: pass-throu Authentication is disabled, therefore authentication for cloud Apps will not be passed to on-prem Domain Controller to validate the password

upvoted 1 times


 **MR_Eliot** 4 months, 1 week ago

The answers seems to be correct.

For SSO in Cloud you will need to enable Seamless-SignOn in EntraID Connect.

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-ss0>

upvoted 1 times

 **jarattdavis** 4 months, 2 weeks ago

Answer: both on-premises and cloud-based

Answer: in the cloud only

Explanation:

Project1: The goal of Project1 is to migrate 100 sales department mailboxes to Microsoft 365. With password hash synchronization and seamless SSO enabled, users can access both on-premises and cloud-based applications using a single sign-on.

Active Directory unavailability: In this scenario, cloud-based resources like Microsoft 365 will still be accessible as they rely on Azure AD for authentication. However, on-premises resources dependent on Active Directory will be inaccessible.

upvoted 2 times

🗨️ 👤 **Lerato22** 3 months, 3 weeks ago

during project 1 , meaning the migration is not yet done . at the stage the sales can only access on-prem but after sales can access both

upvoted 1 times

🗨️ 👤 **Razuli** 6 months ago

The top question makes no sense to me, if everything is working why cant they use on prem and cloud? the second question I understand

upvoted 1 times

🗨️ 👤 **Charard** 11 months, 3 weeks ago

Explanations below, but answer given is correct.

upvoted 3 times

🗨️ 👤 **CBZ57** 1 year, 2 months ago

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

upvoted 2 times

🗨️ 👤 **CheMetto** 1 year, 2 months ago

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

upvoted 1 times

🗨️ 👤 **CheMetto** 1 year, 2 months 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** 1 year, 4 months 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

Suggested Answer: D

Community vote distribution

C (100%)


 **oszvkwpcfxobqjby** Highly Voted 1 year, 4 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 27 times


 **Greatone1** Highly Voted 1 year, 4 months 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 8 times

 **justITtopics** Most Recent 1 month, 1 week ago

Selected Answer: C

Even though I would choose the D option (based on the link I provide), there are no reports in M365 Admin Center yet (november 2024), that give you a view of assignment licenses by group.

<https://learn.microsoft.com/en-us/entra/fundamentals/concept-group-based-licensing> (article updated on 08/02/2024)

"Starting September 1st, the Microsoft Entra ID Admin Center and the Microsoft Azure portal will no longer support license assignment through their user interfaces. To manage license assignments for users and groups, administrators must use the Microsoft 365 Admin Center."

The correct answer to this question (when it was made) is C.

upvoted 1 times

 **justITtopics** 1 month, 1 week ago

Even though I would choose the D option (based on the link I provide), there are no reports in M365 Admin Center yet (nomvember 2024), that give you a view of assignment licenses by group.

<https://learn.microsoft.com/en-us/entra/fundamentals/concept-group-based-licensing> (article updated on 08/02/2024)

"Starting September 1st, the Microsoft Entra ID Admin Center and the Microsoft Azure portal will no longer support license assignment through their user interfaces. To manage license assignments for users and groups, administrators must use the Microsoft 365 Admin Center."

The correct answer to this question (when it was made) is C.

upvoted 1 times

 **rcristiano** 1 month, 3 weeks ago

Resporta D => Relatorios no centro de administração do Microsoft 365

upvoted 1 times

 **mido3100** 2 months ago

Selected Answer: A

This feature is moved to Microsoft Admin Center
upvoted 3 times

MR_Eliot 4 months, 1 week ago

Selected Answer: C

C is correct. Option A could also be true, but then it doesn't show if the user has been activated using a group membership.
upvoted 1 times

roses2021 5 months, 2 weeks ago

Selected Answer: C

Tested in Azure Entra ID
upvoted 1 times

fatso_567 5 months, 4 weeks ago

To identify all users in your Microsoft 365 subscription who are licensed for Office 365 through a group membership and include the name of the group used to assign the license, you should use:

****C. the Licenses blade in the Microsoft Entra admin center****

The Licenses blade in the Microsoft Entra admin center provides detailed information on how licenses are assigned to users, including whether the assignment was done through a group membership and the name of the group responsible for the license assignment. This allows administrators to track and manage license assignments effectively.

upvoted 1 times

Hamouda1 6 months ago

Correct answer C
upvoted 1 times

Jaqueplakzaque 6 months ago

Selected Answer: C

There is no license report in Reports in the 365 admin center.
C is correct.
upvoted 1 times

Carl191 7 months, 2 weeks ago

Selected Answer: C

Answer is C
upvoted 1 times

samet5 8 months ago

Selected Answer: C

C is correct
upvoted 1 times

HelloItsSam 9 months, 1 week ago

Selected Answer: C

Answer is C
upvoted 1 times

Charard 11 months, 3 weeks ago

Selected Answer: C

C is the correct answer. Explanations given below.
upvoted 1 times

AvoKinha 1 year, 1 month 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

NrdAlrt 1 year, 1 month 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

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

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

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

Suggested Answer:

(user.userType) and (user.department)

Percycles Highly Voted 1 year, 4 months ago

Correct answers

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

Be carrefull : Case Sensitive

upvoted 14 times

Blixa 1 year, 1 month ago

Nope, not case sensitive

upvoted 3 times

MR_Eliot Most Recent 4 months, 1 week ago

The provided answers are correct. However, in second box, Match could also be a solution, but since we don't need any advanced matching, the best solution would be using Contains.

upvoted 1 times

Tomtom11 6 months, 3 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership>

Operator Syntax

Not Equals -ne

Equals -eq

Not Starts With -notStartsWith

Starts With -startsWith

Not Contains -notContains

Contains -contains

Not Match -notMatch

Match -match

In -in

Not In -notIn

upvoted 2 times

Jslei 1 year, 3 months ago

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

upvoted 2 times

🗨️ 👤 **imlearningstuffagain** 1 year, 2 months 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 3 times

🗨️ 👤 **MR_Eliot** 4 months, 1 week ago

Microsoft also recommends to minimize the use of contains in favor of -eq and -startswith

upvoted 1 times

🗨️ 👤 **gomezmax** 1 year, 3 months ago

Correct

upvoted 2 times

🗨️ 👤 **vinch** 1 year, 3 months ago

Good answer is -eq -match

upvoted 1 times

🗨️ 👤 **imlearningstuffagain** 1 year, 2 months 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

🗨️ 👤 **nenge** 1 year, 4 months 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

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


Suggested Answer:

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

 **Perycles** Highly Voted 1 year, 4 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 22 times

 **Hamouda1** Most Recent 1 week, 4 days ago

box 1 - CSV


box 2 - UserName and Display name

upvoted 1 times

 **MR_Eliot** 4 months, 1 week ago

Answers are correct!

upvoted 2 times

 **examcrammer** 8 months, 1 week 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** 11 months ago

Correct

upvoted 1 times

🗨️ 👤 **Blixa** 1 year, 1 month 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 3 times

🗨️ 👤 **gomezmax** 1 year, 3 months ago

Correct

upvoted 1 times

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

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

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

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

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

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

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

What is the minimum number of deployment groups required?

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

Suggested Answer: C

Community vote distribution

C (100%)

 **Percycles** Highly Voted 1 year, 4 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 34 times

 **letters1234** Highly Voted 1 year, 4 months ago

Selected Answer: C

All users and the two deparments, three groups

upvoted 8 times

 **MR_Eliot** Most Recent 4 months, 1 week ago

Selected Answer: C

3 groups is the most logical answer.

upvoted 1 times

 **mikl** 7 months, 4 weeks ago

Selected Answer: C

3 Groups gets my vote!

upvoted 2 times

 **bleeding** 1 year, 2 months ago

Selected Answer: C

All, Research, and Marketing. 3 groups.

upvoted 4 times

You have a Microsoft 365 subscription.




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

Service health

October 18, 2022 4:20 PM

Overview Issue history Reported issues

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






 Report an issue  Customize 

Active issues

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

Microsoft service health

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

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

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

Which role should you assign to User1?

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

Suggested Answer: C

Community vote distribution

C (100%)

letters1234 Highly Voted 1 year, 4 months 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 13 times

MR_Eliot Most Recent 3 months, 1 week ago

Selected Answer: C

C is the correct answer:

Message Center Reader:

Can read messages and updates for their organization in Office 365 Message Center only.

Can read service health information and manage support tickets:

Can read service health information and manage support tickets.

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference>

upvoted 1 times

mikl 3 months, 1 week ago

Selected Answer: C

To ensure that User1 can view the advisories and investigate service health issues, you should assign them the role that grants access to the service health dashboard in the Microsoft 365 admin center. According to the information available, Service Support Administrator is a role that allows viewing of service health¹. Therefore, the correct role to assign to User1 would be:

C. Service Support Administrator

upvoted 2 times

Nilz76 3 months, 1 week 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

CharlesS76 8 months, 4 weeks 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 10 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

🗨️ 👤 **rfree** 1 year, 4 months ago

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

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

upvoted 1 times

🗨️ 👤 **stai** 1 year, 4 months ago

Answer A is correct.

Message Center Reader

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

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

upvoted 1 times

🗨️ 👤 **Casticod** 1 year, 4 months ago

Message center it's not the same of service health

upvoted 2 times

🗨️ 👤 **Casticod** 1 year, 4 months ago

Selected Answer: C

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

upvoted 3 times

🗨️ 👤 **Venusaur** 1 year, 4 months ago

Answer C is correct.

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

upvoted 4 times

HOTSPOT -

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

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:

Scope type: Directory -

Selected members: Group1 -

Assignment type: Active -

Assignment starts: Mar 15, 2023 -

Assignment ends: Aug 15, 2023 -

You add the following assignment for the Exchange Administrator role:

Scope type: Directory -

Selected members: Group2 -

Assignment type: Eligible -

Assignment starts: Jun 15, 2023 -

Assignment ends: Oct 15, 2023 -

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

NOTE: Each correct selection is worth one point.

Answer Area

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

Answer Area

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

Suggested Answer:

Casticod Highly Voted 1 year, 4 months ago

Yes, Yes, Yes ??

upvoted 35 times

Bobalo 7 months, 1 week ago

YNY, Exchange Admin status is eligible, an admin still needs to request it first. the user admin assignment status is active.

upvoted 9 times

🗨️ 👤 **MondherBB** Highly Voted 1 year, 2 months 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 24 times

🗨️ 👤 **mashk19** Most Recent 3 months, 4 weeks ago

question doesn't say that PIM is enabled. So surely it's YYY?

upvoted 1 times

🗨️ 👤 **MR_Eliot** 4 months, 1 week ago

For me the answer is correct. Admin 2 has to activate their role to be able to manage the Exchange online. Since it is not mentioned, I go with no.

upvoted 1 times

🗨️ 👤 **FireBeast** 9 months ago

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

upvoted 3 times

🗨️ 👤 **Davito** 10 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 6 times

🗨️ 👤 **Razuli** 7 months, 1 week ago

Microsoft get me so mad. Why include these buggy related questions but thanks for the explanation

upvoted 2 times

🗨️ 👤 **solderboy** 1 year 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 7 times

🗨️ 👤 **TP447** 1 year, 1 month 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 10 times

🗨️ 👤 **GLLimaBR** 10 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 6 times

🗨️ 👤 **miki** 8 months, 3 weeks 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 3 times

🗨️ 👤 **CheMetto** 1 year, 2 months ago

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

upvoted 3 times

  **Darekms0** 1 year, 2 months ago

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



upvoted 1 times

  **imlearningstuffagain** 1 year, 2 months 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** 1 year, 2 months ago

Here are my thoughts and explanations:

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 8 times

  **amurp35** 1 year, 3 months ago

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

upvoted 3 times

  **mpetlk** 1 year, 3 months ago

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

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

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

Important

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

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

upvoted 4 times

  **vercracked_007** 1 year, 3 months ago

YNY

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

upvoted 2 times

  **AMDf** 1 year, 4 months ago

Yes

?? - It depends

Yes

upvoted 2 times

  **miki** 7 months, 4 weeks ago

Just need to activate the role - then it can be done.

Surely its a Y Y Y here.

upvoted 1 times

  **Tedd_TS** 1 year, 4 months ago

Yes, Yes, Yes i think too

upvoted 3 times

  **Venusaur** 1 year, 4 months 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

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

Suggested Answer: B

Community vote distribution

B (76%)

D (24%)

 **gbartumeu** Highly Voted 1 year, 3 months 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 50 times

 **Xbmc66** 1 year ago

But user1 is listed if you look in to 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 3 times

 **Xbmc66** 1 year ago

User 1 Only is the only correct answer
upvoted 1 times

 **Xbmc66** 1 year ago

Please moderator remove my previous messages, it is wrong! Correct answer is User 2 only :)
upvoted 5 times

ae88d96 **Highly Voted** 1 year, 4 months 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 received a notification as well.

User3 is Service Support Administrator so he won't received 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 15 times

Ody 1 year, 1 month 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 1 year, 2 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

jedboy88 **Most Recent** 1 month ago

Selected Answer: B

If the tenant experiences a data breach, Microsoft will contact the Global Administrator. In this case, that would be User2 (Option B) because the Global Administrator is the primary contact for such notifications

upvoted 1 times

MR_Eliot 4 months, 1 week 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 Microsoft Entra services. If there's no person listed here, Microsoft contacts your Global Administrators

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

upvoted 2 times

roses2021 4 months, 1 week ago

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 Microsoft Entra services. If there's no person listed here, Microsoft contacts your Global Administrators. Please refer to the article below:

<https://learn.microsoft.com/en-us/entra/fundamentals/properties-area#to-access-the-properties-area-and-add-your-privacy-information>

upvoted 1 times

Atos 5 months, 2 weeks ago

"Global privacy contact" is user that is contacted in a data breach. As we can see, it is empty, therefore the Global Admin is notified. So B
upvoted 1 times

🗨️ 👤 **[Removed]** 6 months, 1 week ago

Was in Exam 27-6-24

upvoted 3 times

🗨️ 👤 **RikyLorenz** 6 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

🗨️ 👤 **rus123** 7 months, 1 week ago

Option E.

upvoted 1 times

🗨️ 👤 **abul8223** 7 months, 2 weeks ago

Selected Answer: B

I will go for B

upvoted 1 times

🗨️ 👤 **JeSuisCertif** 8 months, 3 weeks ago

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

upvoted 1 times

🗨️ 👤 **ismaelo** 8 months, 3 weeks 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** 9 months ago

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

upvoted 1 times

🗨️ 👤 **JManuel** 9 months, 1 week ago

Selected Answer: D

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

upvoted 1 times

🗨️ 👤 **JManuel** 9 months, 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** 10 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** 11 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** 11 months, 3 weeks ago

Selected Answer: B

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

upvoted 3 times

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

You purchase a Microsoft 365 subscription.

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

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

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

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

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Greatone1** Highly Voted 👍 1 year, 4 months ago

Selected Answer: D

Given answer is correct

upvoted 10 times

🗳️ 👤 **Nilz76** Highly Voted 👍 1 year, 2 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 6 times

🗳️ 👤 **CheMetto** 1 year, 2 months 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 3 times

🗳️ 👤 **Nocho** 1 year, 1 month 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

🗳️ 👤 **ronin201** 7 months, 2 weeks ago

no, you can go with tenant .onmicrosoft.com

upvoted 2 times

🗳️ 👤 **MR_Eliot** 3 months, 3 weeks ago

you can, but it will not be really professional. Best option is to purchase the domain and then add it to DNS-suffix list.

upvoted 2 times

🗳️ 👤 **FemiA55** Most Recent 🕒 1 month, 3 weeks ago

D. Purchase a custom domain name.

upvoted 1 times



🗳️ 👤 **jsmthy** 2 months, 1 week ago

Selected Answer: D

The answer is D.

It took some research, but although Entra ID doesn't support .local/non-routable domains, it can accept users and put them in as (tenant).onmicrosoft.com users. Therefore the next best action is to buy a custom domain that can be implemented on the on-prem AD afterwards if so desired.

upvoted 1 times

  **RFULL** 4 months, 1 week ago

Selected Answer: D



<https://learn.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide>

upvoted 1 times

  **LakesWizard** 6 months, 2 weeks ago

I'd say C and D. Because if you have yours users as .local in their UPN they'll sync as .onmicrosoft.com. You can start from the beggining by doing it right and purchase a .com and updating your users UPN from local to .com

upvoted 1 times

  **AndrewsF** 10 months, 4 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 3 times

You have a Microsoft 365 subscription.

You configure a new Azure AD enterprise application named App1. App1 requires that a user be assigned the Reports Reader role. Which type of group should you use to assign the Reports Reader role and to access App1?

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

Suggested Answer: C

Community vote distribution

C (100%)

 **osxvkwpcfxobqjby** Highly Voted 1 year, 4 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 22 times

 **mikl** 7 months, 4 weeks ago

Correct!

upvoted 1 times

 **sherifhamed** Highly Voted 1 year, 3 months 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 7 times

 **FemiA55** Most Recent 1 month, 3 weeks ago

C. a security group that has assigned membership
upvoted 1 times

 **MR_Eliot** 4 months, 1 week ago

Selected Answer: C

I fully agree with C

upvoted 1 times

 **mikl** 7 months, 4 weeks ago

Selected Answer: C

C. a security group that has assigned membership
upvoted 1 times

 **Amir1909** 11 months ago


C is correct

upvoted 1 times

 **Kmkz83510** 1 year ago

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

upvoted 4 times

 **Nilz76** 1 year, 2 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.

Suggested Answer: A

Community vote distribution

A (88%) 12%

🗳️ 👤 **Nilz76** Highly Voted 👍 1 year, 2 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 14 times

🗳️ 👤 **anonavia** Highly Voted 👍 1 year, 4 months 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 6 times

🗳️ 👤 **FemiA55** Most Recent 🕒 1 month, 3 weeks ago

A. Enable auditing.

upvoted 1 times

🗳️ 👤 **MR_Eliot** 4 months, 1 week ago

Selected Answer: A

Only A makes senses, but is is also enabled by default!

upvoted 1 times

🗳️ 👤 **[Removed]** 6 months, 1 week ago

Was in Exam 27-6-24

upvoted 4 times

🗳️ 👤 **norbe01** 4 months ago

By any chances, you mentioned in all comments which ones was at the exam? :)

upvoted 1 times

🗳️ 👤 **rus123** 7 months, 1 week ago

Option C

upvoted 1 times

🗳️ 👤 **mikl** 7 months, 4 weeks ago

Selected Answer: A

To enable an alert policy in a new Microsoft 365 E5 tenant that will be triggered by the elevation of Microsoft Exchange Online administrative privileges, the first step you should take is:

A. Enable auditing.

Auditing must be enabled to track and record actions within the tenant, which allows for the creation of alert policies based on those audit logs. Once auditing is enabled, you can create alert policies in the Microsoft Purview compliance portal or the Microsoft Defender portal to monitor activities such as assigning admin privileges in Exchange Online

upvoted 1 times

🗨️ 👤 **SecAz0365** 11 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 4 times

🗨️ 👤 **SecAz0365** 11 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** 1 year, 1 month 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

🗨️ 👤 **osxvkwpcfxobqjby** 1 year, 4 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 3 times

🗨️ 👤 **GLLimaBR** 10 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>

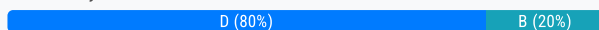
upvoted 3 times

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

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

Suggested Answer: B

Community vote distribution



Nilz76 Highly Voted 1 year, 2 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 16 times

sherifhamed Highly Voted 1 year, 3 months 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

mertak Most Recent 3 days, 5 hours ago

Selected Answer: A

To store Microsoft Defender for Endpoint data in Europe, the first step you should take is to delete the existing workspace (Option A). This is necessary because the data storage location is determined during the initial setup of the workspace, and it cannot be changed afterward¹².

After deleting the current workspace, you can create a new workspace and specify Europe as the data storage location during the setup process.

Would you like more details on how to delete and recreate the workspace?

1: Microsoft Defender for Endpoint data storage and privacy 2: Defender for Endpoint - Data Storage Location integrity question (GDPR/EU)

upvoted 1 times

rcristiano 1 month, 3 weeks ago

Resporta B => Crie uma espaço de trabalho

upvoted 1 times

FemiA55 1 month, 3 weeks ago

D. Offboard the test devices.

upvoted 1 times

MR_Eliot 4 months, 1 week ago

Selected Answer: D

I go with D. Cannot find any confirmation, but it seems right.
upvoted 1 times

HelloitsSam 4 months, 3 weeks ago

Selected Answer: D

1- Offboard the test devices
2- Delete the workspace
3- Create a new workspace, So the Answer is D
upvoted 1 times

[Removed] 6 months, 1 week ago

Was in Exam 27-6-24
upvoted 2 times

Bobalo 7 months, 1 week ago

Selected Answer: D

Old question carries over from previous exam, D is correct answer.
upvoted 1 times

rus123 7 months, 1 week ago

Option D
upvoted 1 times

miki 7 months, 4 weeks ago

Selected Answer: D

I guess you could do either B or D first - it shouldn't really matter that much, should it?

I mean, create the workspace - and then offboard, and onboard to the new workspace, otherwise just offboard the devices and then create a workspace afterwards - and onboard them to EU location.

Anyway - I would go for D if I had to choose.
upvoted 1 times

dvmhike 7 months, 4 weeks ago

The answer is B. Create a workspace is the correct action to store Microsoft Defender for Endpoint data in Europe. Deleting the workspace or onboarding/offboarding devices won't directly address the data storage location.
upvoted 1 times

Omta 9 months, 1 week ago

Selected Answer: D

the pint is data storage location configured during the onboarding process so we need to offboard device first then do onboarding again
upvoted 2 times

neken123 12 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 5 times

pantcm 1 year, 4 months ago

D is the correct answer
upvoted 1 times

gomezmax 1 year, 4 months ago

(D) Offboard the test devices. from here to the Moon
upvoted 1 times

Greatone1 1 year, 4 months ago

D is the correct answer from MS 101
upvoted 3 times

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

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

Suggested Answer: D

Community vote distribution

D (100%)

 **Dtriminio** Highly Voted 1 year, 4 months 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 14 times


 **sherifhamed** Highly Voted 1 year, 3 months 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

 **FemiA55** Most Recent 1 month, 3 weeks ago

A. the Exchange admin center
upvoted 1 times

 **MR_Eliot** 4 months, 1 week ago

Selected Answer: D

D is correct. Had to do this multiple times with our scanner account.
upvoted 1 times

 **[Removed]** 6 months, 1 week ago

Was in Exam 27-6-24
upvoted 4 times

 **LakesWizard** 6 months, 2 weeks ago

Selected Answer: D

MSFT Defender Portal > Restricted Entities
upvoted 1 times

 **mikl** 7 months, 4 weeks ago

Selected Answer: D

Copilot says D.

To remove User1 from the Restricted entities list in a Microsoft 365 E5 subscription, you should use:

D. the Microsoft 365 Defender portal

In the Microsoft 365 Defender portal, you can remove a user from the Restricted entities page. This action is typically necessary when a user is restricted from sending email because they have exceeded the outbound sending limits¹.

upvoted 1 times

🗨️ 👤 **Tomtom11** 11 months 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** 11 months ago

D is correct

upvoted 1 times

🗨️ 👤 **Charard** 11 months, 3 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** 1 year, 1 month 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** 1 year, 3 months 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** 1 year, 3 months ago

D is correct

upvoted 1 times

🗨️ 👤 **RAG** 1 year, 4 months 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

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.

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Nilz76** Highly Voted 👍 1 year, 2 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 15 times

🗳️ 👤 **MR_Eliot** Most Recent 🕒 4 months, 1 week ago

Selected Answer: D

Agree with D

upvoted 1 times

🗳️ 👤 **[Removed]** 6 months, 1 week ago

Was in Exam 27-6-24

upvoted 3 times

🗳️ 👤 **mikl** 7 months, 4 weeks ago

Selected Answer: D

Copilot says :

To prevent the research department users from accessing potentially unsafe websites through hyperlinks in email messages and documents, while not restricting other departments, you should:

D. Create a new safe links policy.

Safe Links is a feature in Microsoft Defender for Office 365 that provides URL scanning and time-of-click verification of URLs in email messages, Teams, and supported Office apps¹. You can create Safe Links policies that apply to specific users, groups, or domains, which allows you to tailor the protection to the needs of different departments within your organization

upvoted 2 times

🗳️ 👤 **Charard** 11 months, 3 weeks ago

Selected Answer: D

See Nilz explanation, correct answer.

upvoted 2 times

🗳️ 👤 **Ruhansen** 1 year, 3 months ago

D - and assigned to different groups

upvoted 1 times

  **Greatone1** 1 year, 4 months ago

D is the correct answer

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

HOTSPOT -

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

Name	Member of
User1	Group1
User2	Group2
User3	Group3

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes

No

User1 can run an antivirus scan on Device2.

User2 can collect an investigation package from Device2.

User3 can isolate Device1.

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.

Suggested Answer:

Nilz76 Highly Voted 1 year, 2 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 32 times

  **sigvast** 1 year, 1 month ago

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

upvoted 5 times

  **Greatone1**  1 year, 4 months 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

  **MR_Eliot**  3 months, 1 week ago

Given answers are correct.


<https://learn.microsoft.com/en-us/defender-endpoint/user-roles#permission-options>

upvoted 1 times

  **Charard** 11 months, 3 weeks ago

Given answer is correct.

upvoted 1 times



  **m2L** 1 year 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 4 times

  **mhmyz** 1 year, 4 months ago

No,No,No

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

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



upvoted 4 times

  **hogegehoge** 1 year, 4 months ago

Box3: No?

Because Defferent Group In User and Device.

upvoted 2 times

  **rinzler1** 1 year, 4 months ago

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

upvoted 10 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

Suggested Answer:


Role:

- Quarantine Administrator
- Security Administrator
- Organization Management
- Communication Compliance Administrators

 **oszvkwpcfxfobqjby** Highly Voted 1 year, 4 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 47 times

 **sigvast** 1 year, 1 month 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** 1 year, 1 month ago

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


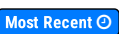
upvoted 14 times

  **letters1234**  1 year, 4 months 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 11 times

  **MR_Eliot**  3 months, 3 weeks ago

Second one is Security Administrator:

Role group name

Security Administrator

Role group description

-

Roles in the role group

Audit Logs

Compliance Manager Administration

Device Management

DLP Compliance Management

IB Compliance Management

Manage Alerts

Quarantine

Security Administrator

Sensitivity Label Administrator

Tag Contributor

Tag Manager

Tag Reader

View-Only Audit Logs

View-Only Device Management

View-Only DLP Compliance Management

View-Only IB Compliance Management

View-Only Manage Alerts

upvoted 1 times

  **LakesWizard** 6 months, 2 weeks ago

Using least privileged won't be organization management.

upvoted 1 times

🗨️ 👤 **9326359** 8 months ago

-Alert

-Security administrator

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

upvoted 1 times

🗨️ 👤 **neken123** 12 months ago

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

upvoted 1 times

🗨️ 👤 **Jonnaz** 1 year 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** 1 year, 1 month ago

sigvast you are right the given answer is correct

upvoted 1 times

🗨️ 👤 **TonyManero** 1 year, 1 month ago

Alert and Security Admin.

Please update the answers.

upvoted 6 times

🗨️ 👤 **lolern123** 1 year, 2 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** 1 year, 1 month ago

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

upvoted 1 times

🗨️ 👤 **Clinson** 1 year, 1 month ago

Yep, but per your same link communication compliance administrator can create policies, and has less privileges that Org Management

upvoted 2 times

🗨️ 👤 **Alecks** 1 year, 2 months 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%20set>
upvoted 1 times

🗨️ 👤 **sergioandreslq** 1 year, 2 months ago

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

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

🗨️ 👤 **Paul_white** 1 year, 2 months ago

CORRECT!!!

<https://www.examttopics.com/discussions/microsoft/view/110911-exam-ms-101-topic-2-question-139-discussion/>
upvoted 1 times

🗨️ 👤 **MarkusSan** 1 year, 2 months ago

not correct, by link provided ;)

upvoted 3 times

🗨️ 👤 **Nilz76** 1 year, 2 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** 1 year, 3 months ago

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

Communication Compliance Administrators Administrators of communication compliance that can create/edit policies and define global settings.
upvoted 1 times

🗨️ 👤 **vercracked_007** 1 year, 3 months ago

Alert and Security Admin

Organisation Management is not a Purview role indeed.

upvoted 2 times

🗨️ 👤 **Blixa** 1 year 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** 1 year, 4 months ago

I think security administrator.

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

upvoted 1 times

You have a Microsoft 365 E5 subscription.

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


What should you use?

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

Suggested Answer: C

Community vote distribution

D (100%)

 **certma2023** Highly Voted 1 year, 4 months ago


Selected Answer: D

It should be answer D.

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

There is 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 21 times

 **MR_Eliot** 3 months, 3 weeks ago

The following types of policies are analyzed by the configuration analyzer:

Exchange Online Protection (EOP) policies: Includes Microsoft 365 organizations with Exchange Online mailboxes and standalone EOP organizations without Exchange Online mailboxes:

Anti-spam policies.

Anti-malware policies.

EOP anti-phishing policies.

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 1 times

 **JunetGoyal** Most Recent 1 month, 1 week ago

D is right

upvoted 1 times

 **MR_Eliot** 3 months, 3 weeks ago

Selected Answer: D

Configuration Analyser is correct:

<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 1 times

  **mikl** 7 months, 4 weeks ago

Selected Answer: D

Copilot says :

To compare the current Safe Links configuration to the Microsoft recommended configurations in your Microsoft 365 E5 subscription, you should use the Configuration Analyzer in Microsoft Defender for Office 365. This tool helps you find and fix security policies that are less secure than the recommended settings by comparing your current configurations with Microsoft's best practices¹.

upvoted 3 times

  **dvmhike** 7 months, 4 weeks ago

Answer should be B.


Microsoft Secure Score provides insights into your organization's security posture and helps you identify areas for improvement. It evaluates various security settings, including Safe Links, and provides recommendations based on best practices.

Configuration analyzer doesn't specifically focus on Safe Links.

While it can identify discrepancies and misconfigurations, it doesn't provide tailored recommendations for Safe Links settings.

For Safe Links, you need a solution that specifically evaluates its configuration against best practices.

upvoted 1 times

  **Tomtom11** 9 months, 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** 11 months ago

D is correct



upvoted 1 times

  **TonyManero** 1 year, 1 month ago

Selected Answer: D

agree with D. Please update the solution.

upvoted 4 times

  **Nilz76** 1 year, 2 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 4 times

  **ae88d96** 1 year, 4 months 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

  **gomezmax** 1 year, 4 months ago

It should be D

upvoted 1 times

  **Greatone1** 1 year, 4 months ago

Selected Answer: D

Correct answer is D

upvoted 1 times

  **Takanami** 1 year, 4 months ago

Configuration Analyzer is correct, direct link:

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

upvoted 1 times

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

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



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

Which Microsoft Defender for Endpoint setting should you modify?

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

Suggested Answer: E

Community vote distribution

E (100%)

Dtriminio Highly Voted 10 months, 3 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 14 times

RAG Highly Voted 10 months, 3 weeks ago

Selected Answer: E

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

upvoted 6 times

miki Most Recent 1 month, 3 weeks ago

Selected Answer: E

Copilot says Incidcators.

To enable user access to the partner company's portal and resolve the issue of the website being blocked, you should modify the Indicators setting in Microsoft Defender for Endpoint. Indicators are used to define URLs, IPs, and files that you've determined to be safe or malicious. By adjusting the indicators, you can allow access to a URL that was previously blocked1.

upvoted 1 times

letters1234 10 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:

Credential harvest
Link to malware
Malware attachment

Training experience:

Identity Theft
Mass Market Phishing
Web Phishing

Answer Area

Social engineering technique:

Credential harvest
Link to malware
Malware attachment

Suggested Answer:

Training experience:

Identity Theft
Mass Market Phishing
Web Phishing

 **imlearningstuffagain** Highly Voted 1 year, 2 months 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 16 times

 **Murad01** Most Recent 5 months, 3 weeks ago

Given answers are correct
upvoted 1 times

 **miki** 7 months, 4 weeks ago

With a Microsoft 365 E3 subscription, you have access to a limited "trial" version of the Attack simulation training feature. The available social engineering technique in this trial version is credential harvesting¹. As for the training experience, it includes the "ISA Phishing and Mass Market Phishing" training experiences².

Therefore, the options available for you to select in the answer area would be:

Social Engineering Technique: Credential Harvesting
Training Experience: ISA Phishing and Mass Market Phishing
upvoted 4 times

🗨️ 👤 **Amir1909** 11 months ago

Answer is correct
upvoted 2 times

🗨️ 👤 **krzysztofbr** 1 year, 1 month ago

answers are corect
Credential Harvest
Mass Market Phishing
upvoted 1 times

🗨️ 👤 **Nilz76** 1 year, 2 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** 1 year, 2 months ago

this is the announcement for the public preview and almost 3 years old.
upvoted 1 times

🗨️ 👤 **faem** 1 year, 3 months 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** 1 year, 4 months 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

🗨️ 👤 **osxvkwpcfxfobqjby** 1 year, 4 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** 1 year, 4 months 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

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

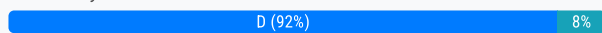
You need to ensure that users are prevented from opening or downloading malicious files from Microsoft Teams, OneDrive, or SharePoint Online.

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.

Suggested Answer: D

Community vote distribution



Nilz76 Highly Voted 1 year, 2 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 11 times

LakesWizard Most Recent 6 months, 2 weeks ago

Selected Answer: D

D - Safe Attachments

upvoted 1 times

Tomtom11 6 months, 3 weeks ago

Anti-malware policy

Anti-malware policies allow you to configure how Microsoft 365 protects your organization from malware transmitted through email messages. By default, existing policies will already provide adequate protection against threats of this type. If necessary, you can create a custom anti-malware policy by performing the following steps:

upvoted 1 times

mikl 7 months, 4 weeks ago

Selected Answer: D

To ensure that users are prevented from opening or downloading malicious files from Microsoft Teams, OneDrive, or SharePoint Online, you should:

D. Configure the Safe Attachments global settings.

Safe Attachments for SharePoint, OneDrive, and Microsoft Teams provides an additional layer of protection against malware by scanning files in a virtual environment. It can be configured to prevent users from opening or downloading malicious files1.

upvoted 1 times

andrewtb 1 year, 3 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 1 year, 4 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** 1 year, 4 months ago

Selected Answer: D

D is the correct answer
upvoted 2 times

🗄️ 👤 **mshkoshbgosh** 1 year, 4 months ago

Selected Answer: D

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

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

Global settings

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

Protect files in SharePoint, OneDrive, and Microsoft Teams

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

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

upvoted 3 times

🗄️ 👤 **Dtriminio** 1 year, 4 months 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

🗄️ 👤 **NrdAlrt** 1 year, 1 month ago

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

upvoted 2 times

🗄️ 👤 **alecrobertburns** 1 year, 4 months 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** 1 year, 4 months 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

🗄️ 👤 **osxvkwpcfxfobqjby** 1 year, 4 months ago

Selected Answer: B

Safe attachments is only for mail so the answer is B

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

upvoted 1 times

🗄️ 👤 **cgmaxmax** 1 year, 2 months ago

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

upvoted 4 times

HOTSPOT -

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

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

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

Settings > Endpoints > computer1



computer1

Device summary

Risk level ⓘ

None

Device details

Domain

adatum.com

OS

Windows 10 64-bit

Version 21H2

Build 19044.2130

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

NOTE: Each correct selection is worth one point.

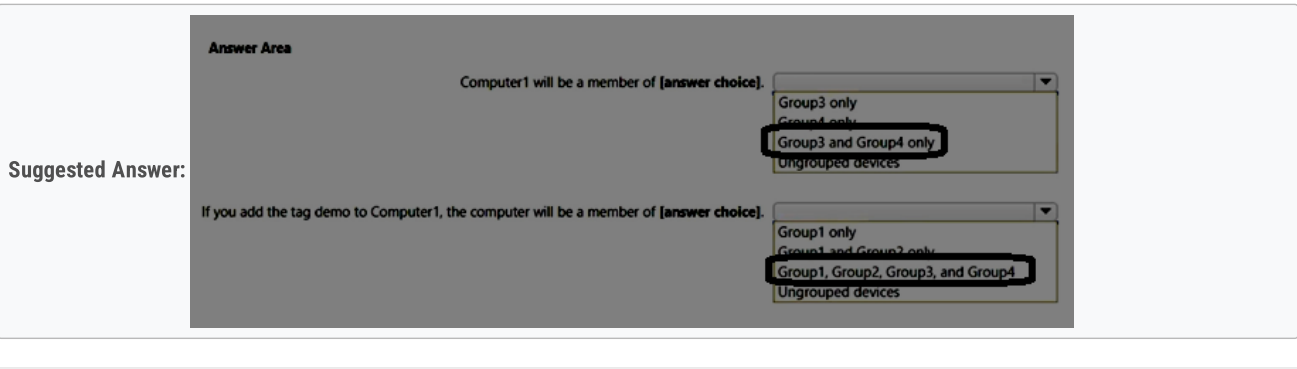
Answer Area

Computer1 will be a member of [answer choice].

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped devices

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

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



Nalle Highly Voted 1 year, 4 months 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 85 times

APK1 6 months, 1 week ago

I agree with you
upvoted 2 times

Sesbri 11 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 4 times

RVerzijl Highly Voted 1 year, 3 months ago

Group 3 only
Group 1 only
upvoted 12 times

RVerzijl 1 year, 3 months 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 3 times

miki Most Recent 7 months, 4 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

Wojer 8 months, 2 weeks ago

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

cpaljchc4 11 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

[Removed] 1 year 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 1 year, 1 month ago

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

sh123df 1 year ago

Because it is due to Rank. Upper rank in list have priority. If that match so that will be set.

upvoted 1 times

  **cpaljhc4** 11 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** 1 year, 1 month ago

Group 3 and Group 4 only

Group 1 and Group 2 only for Tag Demo



upvoted 1 times

  **NrdAlrt** 1 year, 1 month 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** 1 year, 4 months ago

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

upvoted 1 times

  **Greatone1** 1 year, 4 months ago

Group 3 and Group 1

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

upvoted 2 times

  **Casticod** 1 year, 4 months ago

Group 3 only

Group 1 Only

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

upvoted 4 times

HOTSPOT -

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.

You need to identify the following information:

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

To identify the number of emails quarantined by ZAP:

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

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

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

Suggested Answer:

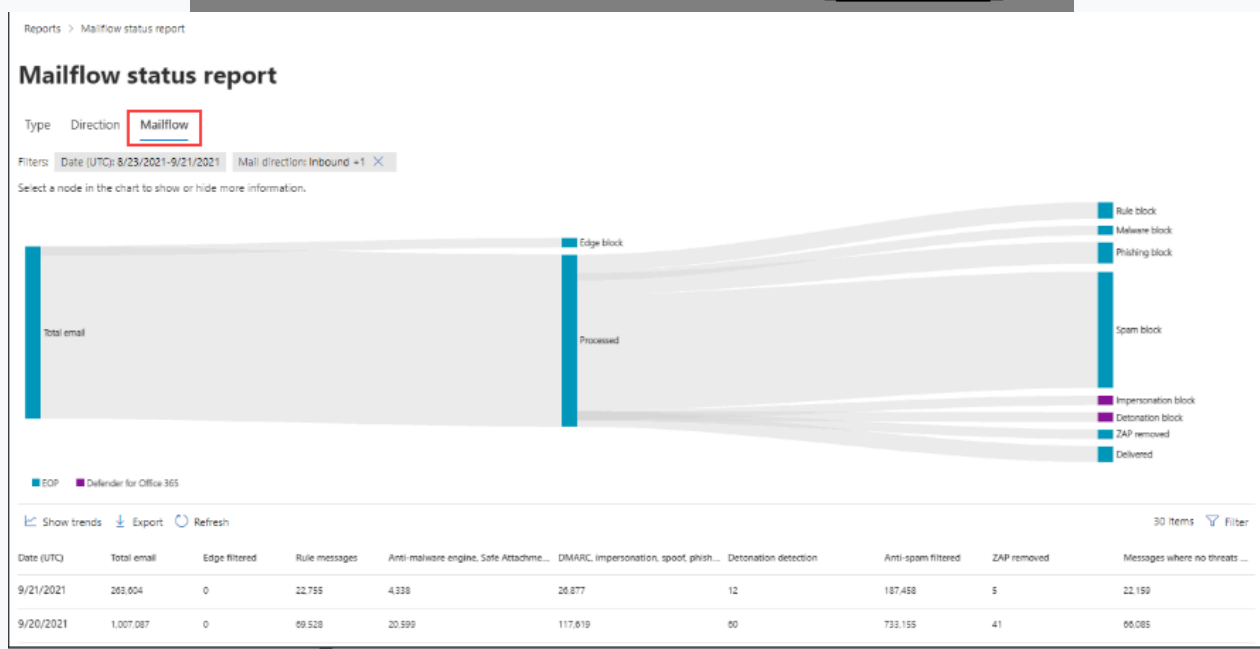
Answer Area

To identify the number of emails quarantined by ZAP:

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

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

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



Mailflow Status Report

2) URL Protection

upvoted 15 times

  **oszvkwpcfxfobqjby** Highly Voted 1 year, 4 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 8 times

  **bobrimal** Most Recent 4 months, 2 weeks ago



right answer: <https://learn.microsoft.com/en-us/defender-office-365/zero-hour-auto-purge?view=o365-worldwide>

upvoted 1 times

  **Nuance** 6 months, 2 weeks ago



<https://learn.microsoft.com/en-us/defender-office-365/reports-email-security#threat-protection-status-report> First one should be Threat Protection Status

upvoted 2 times

  **MR_Eliot** 3 months, 3 weeks ago

I can only find the ZAP-count in mailflow status rapport. Threat Protection Status doesn't contain any information.

upvoted 1 times

  **Motanel** 8 months, 4 weeks ago

Here it says that Threat Protection status shouldd be for first.

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

upvoted 3 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

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **Shloeb** Highly Voted 1 year, 3 months ago

What kind of questions are these? How does this help in getting certified? Microsoft has lost their mind
upvoted 26 times

🗨️ 👤 **NrdAirt** 1 year, 1 month ago

I keep thinking this. Such obscure specific trivia for such a massive platform. Guess that prevents too many people from passing anyway.
upvoted 4 times

🗨️ 👤 **GenPatton** Highly Voted 1 year, 3 months 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 16 times

🗨️ 👤 **Ody** Most Recent 1 month, 2 weeks ago

Selected Answer: D

On the Incidents page, you can filter for Service Source

The options are:

Defender for Cloud Apps

Defender for Endpoint

Defender XDR

Defender for Office 365

App Governance

AAD Identity Protection

Data Loss Prevention

upvoted 1 times

🗨️ 👤 **wakh** 5 months ago

M365 defender now called XDR consists of Defender for identity, office apps, endpoints etc. Sentinel, defender for cloud, azure arc are in Azure Cloud so totally different from M365 defender(XDR). So answer is D.

upvoted 1 times

🗨️ 👤 **Blixa** 1 year 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** 8 months, 3 weeks ago

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

upvoted 1 times

🗨️ 👤 **gomezmax** 1 year, 3 months ago

C. Azure Arc

Right Answer

upvoted 1 times

🗨️ 👤 **Casticod** 1 year, 3 months ago

Real Question in exam

upvoted 4 times

🗨️ 👤 **cb0900** 1 year, 4 months 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 4 times

🗨️ 👤 **Greatone1** 1 year, 4 months ago

Selected Answer: D

D is correct

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

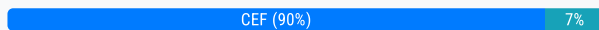
upvoted 3 times

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.

Suggested Answer: ABE

Community vote distribution



certma2023 Highly Voted 1 year, 4 months ago

Selected Answer: CEF

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

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

Then comes the Azure AD Connect deployment & the PTA configuration.
upvoted 31 times

GLLimaBR 8 months, 3 weeks 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 2 times

WORKTRAIN 1 year, 2 months ago

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

upvoted 4 times

Casticod Highly Voted 1 year, 3 months ago

Real Question in exam

upvoted 7 times

Cryptosuri 8 months, 2 weeks ago

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

upvoted 4 times

Kock Most Recent 3 days, 16 hours ago

Selected Answer: ABE

- A. From a domain controller, install an Authentication Agent.
- B. From the Microsoft Entra admin center, configure an authentication method.
- E. From the Microsoft Entra admin center, add a custom domain name

<https://learn.microsoft.com/pt-br/entra/identity/hybrid/connect/how-to-connect-pta-quick-start>
<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta-quick-start>
upvoted 1 times

🗨️ **Frank9020** 1 month, 2 weeks ago

Selected Answer: ACE

the three most essential actions:

- A. From a domain controller, install an Authentication Agent.
- C. From Active Directory Domains and Trusts, add a UPN suffix.
- E. From the Microsoft Entra admin center, add a custom domain name.

upvoted 2 times

🗨️ **MR_Eliot** 3 months, 3 weeks ago

Selected Answer: CEF

CEF. You should not install Authentication Agent on a domain controller. You can, but you really should not.

upvoted 3 times

🗨️ **The_W_Man21** 4 months, 1 week ago

To prepare your environment for implementing pass-through authentication with Azure AD Connect, you should perform the following actions:

From a domain controller, install an Authentication Agent (Option A). This agent is necessary for pass-through authentication to work.

From Active Directory Domains and Trusts, add a UPN suffix (Option C). This ensures that user principal names (UPNs) in your on-premises AD match the domain name in Azure AD.

From the Microsoft Entra admin center, add a custom domain name (Option E). This allows users to sign in with their custom domain rather than the default onmicrosoft.com domain.

These steps will help you set up the necessary components for pass-through authentication

upvoted 2 times

🗨️ **certifexams** 5 months, 1 week ago

Copilot answer ABE :

To prepare the environment for implementing pass-through authentication, follow these steps:

1. Install an Authentication Agent:

From a domain controller, install the Azure AD Connect Authentication Agent (also known as Microsoft Entra Connect) on a member server. This agent facilitates pass-through authentication by validating user passwords directly against the on-premises Active Directory1.

Ensure that the server running the Authentication Agent is running Windows Server 2016 or later and has TLS 1.2 enabled.

2. Configure an Authentication Method:

In the Microsoft Entra admin center, configure pass-through authentication as the authentication method for your Azure AD tenant. This allows users to sign in to both on-premises and cloud-based applications using the same passwords1.

Specify the on-premises account for connectivity during the configuration process.

3. Add a Custom Domain Name:

In the Microsoft Entra admin center, add one or more custom domain names to your Azure AD tenant. Users can sign in using these domain names1.

upvoted 2 times

🗨️ **dvmhike** 7 months, 4 weeks ago

Option C (adding a UPN suffix) is not necessary for implementing pass-through authentication.

upvoted 1 times

🗨️ **Scotte2023** 8 months, 1 week 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 2 times

🗨️ **GLLimaBR** 8 months, 2 weeks 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** 8 months, 4 weeks 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** 8 months, 4 weeks 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** 11 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** 11 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** 11 months, 4 weeks ago

Selected Answer: CEF

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

upvoted 2 times

🗨️ **Xbmc66** 1 year 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** 1 year 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 3 times

🗨️ **Percycles** 11 months, 3 weeks ago

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

upvoted 2 times

HOTSPOT -

You have a new Microsoft 365 E5 tenant.

Enable Security defaults is set to Yes.

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

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

NOTE: Each correct selection is worth one point.

Answer Area

MFA method:

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

Number of days:

- 7
- 14
- 30
- 60

Suggested 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

 **osxvkwpcfxfobqjby** Highly Voted 10 months, 4 weeks ago

- Notification to Microsoft Authenticator app
- 14 days

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/security-defaults#authentication-methods>
upvoted 16 times

 **sherifhamed** Highly Voted 9 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-in1
upvoted 8 times

 **northgaterebel** 8 months, 1 week 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 3 times

  **nils241** 6 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 2 times

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

Copilot says :



With Enable Security defaults set to Yes in a new Microsoft 365 E5 tenant, when a user signs in for the first time, they can use the Microsoft Authenticator app as their multi-factor authentication (MFA) method¹. The user has 14 days to register for MFA from the first time they sign in after security defaults have been enabled². After the 14-day period, if the user has not completed the MFA registration, they will not be able to sign in until the registration is completed

upvoted 2 times

  **benpato** 7 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's recommendation and automatically defaulted in every tenant unless specified otherwise.

upvoted 1 times

  **Alecks** 8 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

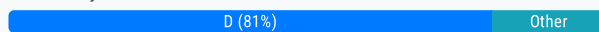
You configure Azure AD Connect to sync contoso.com to Azure AD.

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

Suggested Answer: D

Community vote distribution



Haso Highly Voted 1 year, 4 months ago

Selected Answer: D

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

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

upvoted 22 times

Kock Most Recent 3 days, 15 hours ago

Selected Answer: D

<https://learn.microsoft.com/pt-br/training/modules/manage-synchronized/1-introduction>

upvoted 1 times

Ody 1 month, 2 weeks ago

Selected Answer: D

Disabled Accounts sync.

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

upvoted 2 times

mikl 7 months, 4 weeks ago

Selected Answer: D

Its D.

Yes, disabled accounts do get synchronized via Azure AD Connect to Azure AD. By default, Azure AD Connect will sync all objects, including those that are disabled in your on-premises Active Directory, unless they are filtered out by configuration settings

upvoted 1 times

JamesWilliams 9 months, 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** 1 year, 1 month 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** 1 year, 1 month 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** 1 year, 1 month ago

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

upvoted 1 times

🗨️ **mikl** 7 months, 4 weeks ago

Explain please.

upvoted 1 times

🗨️ **Ruhansen** 1 year, 3 months ago

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

The answer is D

upvoted 1 times

🗨️ **Casticod** 1 year, 3 months ago

Real Question in exam

upvoted 2 times

🗨️ **Tisi** 1 year, 3 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** 1 year, 4 months ago

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

upvoted 2 times

🗨️ **mikl** 7 months, 4 weeks ago

Wrong.

Yes, disabled accounts do get synchronized via Azure AD Connect to Azure AD. By default, Azure AD Connect will sync all objects, including those that are disabled in your on-premises Active Directory, unless they are filtered out by configuration settings

upvoted 1 times

🗨️ **Mr4D97** 1 year, 4 months ago

Selected Answer: D

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

ANSWER IS D

upvoted 3 times

🗨️ **Casticod** 1 year, 4 months ago

Selected Answer: B

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

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

upvoted 1 times

🗨️ 👤 **moshkosbgosh** 1 year, 4 months 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

🗨️ 👤 **moshkosbgosh** 1 year, 4 months ago

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

upvoted 4 times

🗨️ 👤 **certma2023** 1 year, 4 months 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** 1 year, 4 months ago

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

ANSWER IS D

upvoted 1 times

🗨️ 👤 **mrac** 1 year, 4 months 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 4 times

🗨️ 👤 **mikl** 7 months, 4 weeks ago

Wrong.

Yes, disabled accounts do get synchronized via Azure AD Connect to Azure AD. By default, Azure AD Connect will sync all objects, including those that are disabled in your on-premises Active Directory, unless they are filtered out by configuration settings

upvoted 1 times

🗨️ 👤 **certma2023** 1 year, 4 months ago

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

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

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

upvoted 2 times

  **NrdAirt** 1 year, 1 month ago

Resource and shared mailboxes are attached to disabled user accounts, so that makes sense.
upvoted 1 times

You have a Microsoft 365 E5 subscription.

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

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

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

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

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

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

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


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

Suggested Answer: B

Community vote distribution

B (80%)

A (20%)

 **certma2023** Highly Voted 1 year, 4 months ago

Selected Answer: B


I would go for B answer.

4 rules configured like that :

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

For me, it should meet the goals.

upvoted 29 times

 **golijat** 1 year, 1 month 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** 1 year 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 triggers access will be blocked . Having a rule that lets you in will not allow you to log in from a blocked rule .

upvoted 4 times

🗄️ 👤 **Xbmc66** Highly Voted 1 year 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 9 times

🗄️ 👤 **FemiA55** Most Recent 1 month, 2 weeks ago

I go for B. I don't think there is a need for conditional access management for App1. The security requirement for App1 can be taken care of by granting access to a security group with members from finance team only.

upvoted 1 times

🗄️ 👤 **Frank9020** 1 month, 2 weeks ago

Selected Answer: A

Policy 1: Combine MFA, compliant devices, and geographic restrictions.

Conditions: Sign-in from outside the corporate network.

Controls: Require MFA, require compliant devices, block sign-ins from outside the United States and Canada.

Policy 2: Block R&D department users from signing in from Android and iOS devices.

Conditions: Users in the R&D department.

Controls: Block access from Android and iOS devices.

Policy 3: Restrict access to App1 to only finance department users.

Conditions: Users in the finance department.

Controls: Allow access to App1, block all other users.

upvoted 1 times

🗄️ 👤 **Ody** 1 month, 2 weeks ago

Selected Answer: B

The first two options are both requirements for being outside the corporate network.

upvoted 1 times

🗄️ 👤 **9326359** 8 months ago

The answer is 3, i am able to configure named locations in the new "network" section within Conditional access. This question may be outdated as this feature says "new" next to it

upvoted 2 times

🗄️ 👤 **Moazzamfarooqiiii** 10 months, 2 weeks ago

Chat GPT is saying C = 5

upvoted 5 times

🗄️ 👤 **Amir1909** 11 months ago

B is correct

upvoted 1 times

🗄️ 👤 **Master_Tx** 1 year, 4 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** 1 year, 4 months ago

answer is correct

B

upvoted 2 times

HOTSPOT -

Your network contains an on-premises Active Directory domain.

You have a Microsoft 365 E5 subscription.

You plan to implement directory synchronization.

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Tool:

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

Required group membership:

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

Suggested Answer:

Answer Area

Tool:

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

Required group membership:

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

 **osxzvkwpcfxfobqjby** Highly Voted 1 year, 4 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 35 times

 **mikl** 8 months ago

Agree - keyword here is identify!

upvoted 2 times

 **Casticod** Highly Voted 1 year, 4 months ago

IdFix

Domain Users

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

upvoted 6 times

🗨️ 👤 **Tomtom11** Most Recent 10 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 2 times

🗨️ 👤 **Amir1909** 11 months ago

- IdFix

- Domain Users

upvoted 1 times

🗨️ 👤 **azagroth** 1 year 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** 1 year ago

lare confuser

upvoted 2 times

🗨️ 👤 **KTM_999** 2 months ago

bathong nikhona

upvoted 1 times

🗨️ 👤 **benpatto** 1 year, 1 month 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** 1 year, 1 month ago

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

upvoted 1 times

🗨️ 👤 **vercracked_007** 1 year, 3 months ago

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

upvoted 3 times

🗨️ 👤 **rfree** 1 year, 4 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"/>

Suggested Answer:

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

Haso Highly Voted 1 year, 4 months ago

Y: User is in trusted location from CA policy

Y: User is in trusted location from CA policy

N: Trusted IPs in the MFA settings contains a list of IPs that MFA can be skipped from.

<https://c7solutions.com/2022/07/what-is-multifactor-authentication-trusted-ips>

upvoted 26 times

iamchoy 1 week, 2 days ago

User 2 MFA is enforced, so he will always be required to use MFA anywhere.

upvoted 1 times

365cm 1 year 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** 12 months ago

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

upvoted 2 times

  **osxzkwpfcfxobqjby** Highly Voted 1 year, 4 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 13 times

  **sergioandreslq** 1 year, 2 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 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 9 times

  **grimrodd** 4 months, 1 week ago

This is the correct answer, not because they are in an IP within a trusted location, but because if you're coming from a trusted location or not the CA policy is set to enforce MFA.

upvoted 2 times

  **certma2023** 1 year, 4 months ago

No it should be YYN.

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



upvoted 13 times

  **lali11** 12 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

  **justITtopics** Most Recent 1 month, 2 weeks ago

I vote for Y,Y,Y

In this link say that we can consider a trusted networks and locations: All locations marked as trusted locations (it applies to CA Ips:

131.107.20.0/24 and 131.107.50.0/24) and Multifactor authentication trusted IPs, if configured (it applies to the IP 131.107.5.0/24 marked as trusted in the MFA).

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-assignment-network>

All trusted networks and locations

This option applies to:

All locations marked as trusted locations.

Multifactor authentication trusted IPs, if configured.

upvoted 1 times

  **Frank9020** 1 month, 2 weeks ago

YES: User1 will be required to complete MFA when signing in from a trusted location because the Conditional Access policy requires MFA for all users.

YES: User2 from trusted location: MFA required due to the Conditional Access policy (trusted locations do not bypass MFA in this setup).

YES: User2 from non-trusted location: MFA required as per the policy settings.

upvoted 1 times

🗨️ 👤 **Xive** 2 months, 3 weeks ago

YYY. Refer to <https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-assignment-network#all-trusted-networks-and-locations>

CA Trusted Location INCLUDE Trusted IP in MFA. So it CANNOT be skip!

upvoted 2 times

🗨️ 👤 **MR_Eliot** 3 months, 2 weeks ago

1: YES

- User Matched

- IP is trusted

- User is accessing App1

2: Yes

- User Matched

- IP is trusted

- User is accessing App1

3: YES

- User matched

- Ip not machted, however Multi-factor auth is enforced. This will require user to use MFA for anything. This is tricky, but I can confirm this since I have thested this in my own lab.

upvoted 3 times

🗨️ 👤 **APK1** 4 months, 1 week ago

My thought is

User1 MFA is disabled, so he cannot be authenticated even if with "grant with MFA" policy assigned. MFA must be enabled or Enforced to him.

Answer should be NYN

upvoted 1 times

🗨️ 👤 **DasChi_cken** 4 months, 1 week ago

User1 can access to the app because he is in the trusted IP range, he needs to set up MFA because its currently disabled, but after setup and authenticating he cann access the app

User 2 is in the trusted range and has MFA already set up so only needs to authenticate the request and can access the app as well

User2 is now not in the trusted IP range, access to the app is block completly and therefore not MFA authentication is prompt at all

YYN is the answer in my opinion

upvoted 2 times

🗨️ 👤 **Atos** 5 months, 2 weeks ago

Given answer looks correct YYN. (User MFA Status is irrelevant in this case)

CA Policy hits first 2

Last one is in trusted ip range. To elaborate, when users are enabled individually, they perform multifactor authentication each time they sign in (with some exceptions, such as when they sign in from trusted IP addresses or when the remember MFA on trusted devices feature is turned on).

upvoted 1 times

🗨️ 👤 **Tomtom11** 6 months, 2 weeks ago

<https://learn.microsoft.com/en-ie/entra/identity/authentication/concept-mfa-howitworks>

upvoted 1 times

🗨️ 👤 **Scott2023** 8 months 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 2 times

  **[Removed]** 8 months, 2 weeks 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 2 times

  **Tomtom11** 9 months, 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** 11 months, 1 week ago

I also believe it's Y Y Y:

<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

  **Navin_83** 1 year 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** 1 year, 1 month ago

Agree with Y Y N (This is markes as a trusted location so MFA can be skipped)

upvoted 2 times

  **365cm** 1 year, 1 month ago

Y

Y

N

Trusted IPs you can set it to where it bypasses MFA.

upvoted 2 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.

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **sherifhamed** Highly Voted 9 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 7 times

🗨️ **Amir1909** Most Recent 5 months ago

Correct

upvoted 1 times

🗨️ **SBGM** 5 months ago

Selected Answer: A

Given answer is correct

upvoted 1 times

🗨️ **GLL** 10 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** 5 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:

- 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

Suggested Answer:**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**

 **RAG** Highly Voted 1 year, 4 months ago

Looks correct - <https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa>
upvoted 15 times

 **certma2023** 1 year, 4 months ago

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

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

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

upvoted 5 times

 **NrdAlrt** 1 year, 1 month ago

Thanks for sharing new way!

upvoted 1 times

 **amurp35** 1 year, 3 months ago

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

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

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

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

upvoted 1 times

  **Nandokun01** 1 year, 4 months 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

  **digats** Most Recent 2 months, 3 weeks ago

correct: Just in User risc you have the option to change the password

<https://learn.microsoft.com/de-de/entra/id-protection/concept-identity-protection-policies>

upvoted 1 times

  **Tomtom11** 6 months, 2 weeks ago

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



User risk detections might flag a legitimate user account as at risk, when a potential threat actor gains access to an account by compromising their credentials or when they detect some type of anomalous user activity. Sign-in risk detections represent the probability that a given authentication request isn't the authorized owner of the account. Having the ability to identify risk at the user and sign-in level is critical for customers to be empowered to secure their tenant.

upvoted 1 times

  **Tomtom11** 9 months, 2 weeks ago

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

upvoted 1 times

  **Tomtom11** 9 months, 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** 1 year, 1 month 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

upvoted 1 times

  **365cm** 1 year, 1 month 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** 1 year, 1 month 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** 1 year, 2 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** 1 year, 2 months 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.

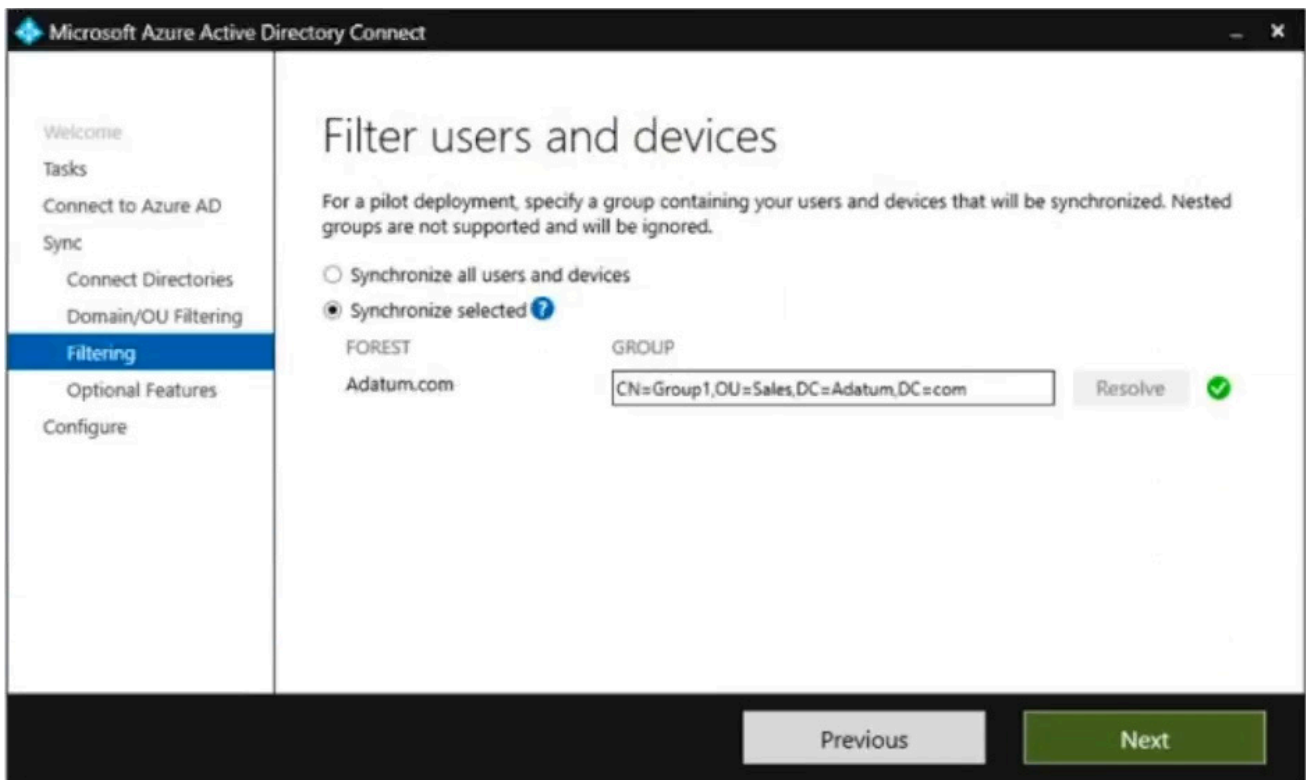
Name	Member of	In OU
Group1	None	Sales
Group2	Group1	OU1

You are deploying Azure AD Connect.

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

The screenshot shows the Microsoft Azure Active Directory Connect console. The main window is titled "Domain and OU filtering". Below the title, there is a note: "If you change the OU-filtering configuration for a given directory, the next sync cycle will automatically perform full import on the directory." The "Directory:" dropdown is set to "Adatum.com", and there is a "Refresh Domains" button. Two radio buttons are present: "Sync all domains and OUs" (unselected) and "Sync selected domains and OUs" (selected). Below this, a tree view shows the directory structure for "Adatum.com" with checkboxes for various OUs. The "OU1" checkbox is checked. At the bottom of the console, there are "Previous" and "Next" buttons.

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



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"/>

Suggested Answer:

Answer Area

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

Casticod Highly Voted 1 year, 4 months ago

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

When using OU-based filtering in conjunction with group-based filtering, the OU(s) where the group and its members are located must be included. (<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#group-based-filtering>)

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

upvoted 30 times

  **WORKTRAIN** 1 year, 2 months 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 10 times

  **mhmyz**  1 year, 3 months 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 8 times

  **APK1**  4 months, 1 week ago

NNN is correct

Sales OU is already included in filter but no member assigned to Sales OU

upvoted 1 times

  **arielreyes2712** 4 months, 2 weeks ago

N

N

N

The answer is here: <https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-configure-filtering#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.

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 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.

Enable and Target Configure

Enable

Include Exclude

Target All users Select groups

Add groups

Name	Type	Registration	Authentication mode
Group1	Group	Optional	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

User1 will be prompted for passwordless authentication once User1 sets up phone sign-in in the Microsoft Authenticator app.

Yes

No

User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.

User3 can use passwordless authentication without further action.

Suggested Answer:

Answer Area

Statements


User1 will be prompted for passwordless authentication once User1 sets up phone sign-in in the Microsoft Authenticator app.

Yes

No

User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.

User3 can use passwordless authentication without further action.

 certma2023 Highly Voted 1 year, 4 months ago

Answer is correct. YNN.

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

User2 is registred 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 20 times

 GLLimaBR 8 months, 2 weeks 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 2 times

  **gomezmax** Highly Voted  1 year, 4 months ago

Yes Correct YNN

upvoted 5 times

  **Tomtom11** Most Recent  6 months, 2 weeks ago

<https://learn.microsoft.com/en-ie/entra/identity/authentication/concept-authentication-authenticator-app>

upvoted 1 times

You have a Microsoft 365 E5 subscription.

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

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

Report on shared documents that contain PII.

What should you create?

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

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **Wazery** 4 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** 8 months, 2 weeks ago

Selected Answer: A

Also in ms-101 Qs:

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

upvoted 4 times

🗨️ 👤 **KT_Paradise75** 9 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

Suggested Answer: E

Community vote distribution


E (94%) 6%

 **Dtriminio** Highly Voted 1 year, 4 months ago

Selected Answer: E

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

upvoted 8 times

 **Manoj2y** 1 month, 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 I <https://learn.microsoft.com/en-us/purview/sensitivity-labels>

upvoted 1 times

 **omnomsnom** Highly Voted 1 year ago

Sensitivity labels cannot be assigned to distribution groups, tho?


upvoted 7 times

 **ankitata28** 11 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>

upvoted 1 times

 **radamelca** 3 months, 1 week ago

"Can be PUBLISHED to any specific user or email-enabled security group, distribution group, or Microsoft 365 group". I have not seen any docume

upvoted 2 times

 **OHMSS** Most Recent 2 weeks, 3 days ago

Selected Answer: C

I go for C only.

Sensitivity label can only be assigned to files and platforms like Email, Sharepoint and Onedrive.

upvoted 1 times

 **Frank9020** 1 month, 2 weeks ago

Selected Answer: E

365 Group (Group1): Sensitivity labels can be applied to Microsoft 365 Groups, including the associated resources such as Outlook mailboxes, SharePoint sites, and Teams.

Distribution Group (Group2): Sensitivity labels can also be applied to distribution groups, although there might be some limitations depending on

the type of distribution group (security or mail-enabled).

SharePoint Site (Site1): Sensitivity labels can be applied to SharePoint sites, which allows for protection of the data within the site, including documents and list items.

upvoted 2 times

🗨️ 👤 **bobg** 2 months, 4 weeks ago

i would think its group 1 and site 1 only but thats not an option. labels can only be applied to microsoft 365 groups not distribution groups.

<https://learn.microsoft.com/en-us/purview/sensitivity-labels-teams-groups-sites#how-to-configure-groups-and-site-settings>

upvoted 1 times

🗨️ 👤 **bobg** 2 months, 4 weeks ago

also here under troubleshooting it says the group has to be a m365 group <https://learn.microsoft.com/en-us/entra/identity/users/groups-assign-sensitivity-labels?tabs=microsoft#sensitivity-labels-arent-available-for-assignment-on-a-group>

upvoted 1 times

🗨️ 👤 **dearlover87** 3 months, 1 week ago

i thought only policies can apply on group or sites

upvoted 1 times

🗨️ 👤 **It2673** 4 months, 2 weeks ago

Selected Answer: C

All of this is wrong, a label cannot be applied to a group. The documentation from previous comment only indicates that a label POLICY can be applied to a group of users. That means WHO can apply a label, NOT ON WHAT.

upvoted 4 times

🗨️ 👤 **arielreyes2712** 4 months, 2 weeks ago

Selected Answer: E

Answer is E

upvoted 1 times

🗨️ 👤 **BurtSmart** 6 months, 3 weeks ago

READ THE QUESTION - states APPLY label1, not SEE Label1. Distribution groups can SEE the labels, but the labels cannot be applied to them! From this reference: <https://learn.microsoft.com/en-us/purview/sensitivity-labels> This is what is stated: 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. It clearly states SEE labels! This is the reference that explains it: <https://learn.microsoft.com/en-us/purview/sensitivity-labels-teams-groups-sites>

upvoted 3 times

🗨️ 👤 **mikl** 7 months, 4 weeks ago

Selected Answer: E

I agree - should be E here.

upvoted 1 times

🗨️ 👤 **Amir1909** 11 months ago

Correct

upvoted 1 times

🗨️ 👤 **Hasa** 11 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 5 times

🗨️ 👤 **ankitata28** 11 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 Micro

<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%2>

upvoted 2 times

🗨️ 👤 **gomezmax** 1 year, 2 months ago

D. Group1 and Group2 only

upvoted 1 times

🗨️ 👤 **Martham** 1 year, 2 months ago

Given Answer is correct

upvoted 2 times

🗨️ 👤 **RAG** 1 year, 4 months ago

Selected Answer: E

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

upvoted 6 times

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You need to meet the following requirements:

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

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









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

NOTE: Each correct selection is worth one point.

Answer Area

Solutions	
	Catalog
	Audit
	Content search
	Communication compliance
	Data loss prevention
	eDiscovery ▼
	Data lifecycle management
	Information protection
	Information barriers ▼
	Insider risk management
	Records management
	Priva Privacy Risk Managem... ▼
	Priva Subject Rights Requests
	Settings

Suggested Answer:

Answer Area	
Solutions	
	Catalog
	Audit
	Content search
	Communication compliance
	Data loss prevention
	eDiscovery ▼
	Data lifecycle management
	Information protection
	Information barriers ▼
	Insider risk management
	Records management
	Priva Privacy Risk Managem... ▼
	Priva Subject Rights Requests
	Settings

AMDf **Highly Voted** 1 year, 4 months ago

Correct:

<https://www.examttopics.com/discussions/microsoft/view/94672-exam-ms-101-topic-3-question-153-discussion/>
upvoted 9 times

Dtriminio **Highly Voted** 1 year, 4 months 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 7 times

Besxp 1 month, 2 weeks ago

I think you forgot to answer the question here, let me correct you:

1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
 2. From the navigation pane, select "Information protection" then "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 2 times

jarattdavis **Most Recent** 4 months, 2 weeks ago

Information protection: This setting allows you to define sensitivity labels, which can be applied to documents to classify and protect them based on their sensitivity level. You can configure encryption settings within sensitivity labels to automatically encrypt documents stored in OneDrive and SharePoint.

Data loss prevention (DLP): While DLP policies primarily focus on preventing data loss, they can also be configured to work in conjunction with sensitivity labels to enable co-authoring for encrypted documents. DLP policies can define specific conditions for allowing collaboration on sensitive information, ensuring that only authorized users can co-author encrypted documents.

upvoted 1 times

Shloeb 12 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 3 times

JazyStahh 8 months, 3 weeks 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 3 times

You have a Microsoft 365 E5 subscription.

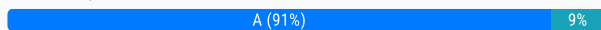
You plan to create a data loss prevention (DLP) policy that will be applied to all available locations.

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

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

Suggested Answer: C

Community vote distribution



🗳️ 👤 **Alecks** Highly Voted 👍 1 year, 2 months 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 13 times

🗳️ 👤 **SheryID** Highly Voted 👍 1 year, 4 months 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 5 times

🗳️ 👤 **radamelca** Most Recent 🕒 3 months, 1 week ago

Selected Answer: A

Sensitive Info Types is the only option.

upvoted 1 times

🗳️ 👤 **jarattdavis** 4 months, 2 weeks ago

Selected Answer: A

A. Sensitive info types

DLP policies use sensitive information types (SITs) as a primary method to identify and protect sensitive data across various Microsoft 365 locations. SITs are predefined patterns that match common types of sensitive information, such as credit card numbers, social security numbers, or bank account numbers.

upvoted 1 times

🗳️ 👤 **Sayulis** 1 year ago

You can add Sensitive info types or Trainable classifiers

upvoted 2 times

🗳️ 👤 **Armins** 1 year, 1 month ago

A 100% confirmed with my honor.

upvoted 3 times

🗳️ 👤 **sherifhamed** 1 year, 3 months 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 on1. 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 numbers2.

B, C, and D are incorrect because they are not valid conditions for DLP rules in Office
upvoted 4 times

  **sergioandreslq** 1 year, 2 months 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** 1 year, 3 months ago

Selected Answer: A

Vote for A
upvoted 1 times

  **gomezmax** 1 year, 4 months ago

Should be A
upvoted 1 times

  **Greatone1** 1 year, 4 months ago

Selected Answer: A

A should be the correct answer
<https://www.examttopics.com/discussions/microsoft/view/94556-exam-ms-101-topic-3-question-154-discussion/>
upvoted 1 times

  **moshkoshgosh** 1 year, 4 months ago

Selected Answer: A

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

The reason I'm suggesting A is that this needs to apply to all locations, but sensitivity labels can't be applied to Teams Chat and Channel Messages. I know this is being fussy about the wording, but it would be a way to reduce the choice to one valid option.
<https://learn.microsoft.com/en-us/purview/dlp-policy-reference#location-support-for-how-content-can-be-defined>
upvoted 5 times

  **certma2023** 1 year, 4 months ago

I would go for answer A too. When you select all locations inside the policy configuration (Exchange, Sharepoint, OneDrive, MS Defender for Cloud, Endpoint...), the only options you have on the custom rule is "sensitive info types".
upvoted 2 times



  **moshkoshgosh** 1 year, 4 months ago

Selected Answer: D

The reason I'm suggesting D is that this needs to apply to all locations, but sensitivity labels can't be applied to Teams Chat and Channel Messages. I know this is being fussy about the wording, but it would be a way to reduce the choice to one valid option.
<https://learn.microsoft.com/en-us/purview/dlp-policy-reference#location-support-for-how-content-can-be-defined>
upvoted 1 times

  **moshkoshgosh** 1 year, 4 months ago

please delete, it should have said A as per the link.
upvoted 1 times

  **Dtriminio** 1 year, 4 months ago

Selected Answer: D

A+D are correct
upvoted 2 times

  **osxvkwpcfcxobjby** 1 year, 4 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

You have a Microsoft 365 E5 tenant.
Users store data in the following locations:

Microsoft Teams -

Microsoft OneDrive -

Microsoft Exchange Online -

Microsoft SharePoint -

You need to retain Microsoft 365 data for two years.

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


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

Suggested Answer: C

Community vote distribution

C (85%)

B (15%)

 **moshkosbgosh** Highly Voted 1 year, 4 months 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 40 times

 **ATHOOS** 1 year, 1 month ago

Tested and Approved ! well done
upvoted 4 times

 **Witnz** 11 months, 1 week ago

not specified
upvoted 1 times

 **Turlin** Most Recent 5 months, 3 weeks ago

Selected Answer: C

I just checked in my tenant

1. Exchange mailboxes and OneDrive accounts can be turned on together.
2. Teams Channel Messages and Teams Chats and Copilot interactions can be turned on together.
3. Teams private channel can only be on by itself.

If you try different combinations the others get turned off. So, the least amount it can be done in is 3.
upvoted 1 times

 **rus123** 7 months, 1 week ago

Answer A
upvoted 1 times

 **NrdAirt** 1 year, 1 month ago

Selected Answer: C

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

upvoted 3 times

🗨️ 👤 **jay209328032038** 1 year, 2 months 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** 1 year, 3 months ago

Selected Answer: B

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

upvoted 1 times

🗨️ 👤 **mhmyz** 1 year, 3 months 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** 1 year, 4 months ago

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

upvoted 2 times

🗨️ 👤 **Greatone1** 1 year, 4 months ago

Selected Answer: C

3 is the correct answer from previous test

upvoted 1 times

🗨️ 👤 **nublitt** 1 year, 4 months ago

Selected Answer: B

In my opinion the correct answer is B.

1 Retention policy for Exchange, OneDrive and SharePoint

1 Retention policy for Teams channels and chat.

upvoted 2 times

🗨️ 👤 **mrac** 1 year, 4 months 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

🗨️ 👤 **osxvkwpcfxfobqjby** 1 year, 4 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 4 times

HOTSPOT -

You have a Microsoft 365 tenant.

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

Information governance > Create retention policy

- ✓ Name
- ✓ Locations
- ✓ Retention settings
- Finish**

Review and finish

It might take up to one day to apply this policy to the locations you selected.

Policy name
contoso
[Edit](#)

Description
[Edit](#)

Locations to apply the policy
Exchange email (All Recipients)
SharePoint sites (All Sites)
OneDrive accounts (All Accounts)
Microsoft 365 Groups (All Groups)
[Edit](#)

Retention settings
Delete items at end of retention period
Delete items that are older than 7 years based on when they were created
[Edit](#)

⚠ Items that are currently older than 7 years will be deleted after you turn on this policy. This is especially important to note for locations scoped to 'All' sources (for example, 'All Teams chats') because all matching items in those locations across your organization will be permanently deleted.

[Back](#)
[Submit](#)
[Cancel](#)

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

Suggested Answer:

Answer Area

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

recovered 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 1 year, 4 months ago

Deleted 7 years after they were created = Correct

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

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

upvoted 71 times

cpaljchc4 1 year 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** 9 months, 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** Highly Voted  1 year, 4 months 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

  **JunetGoyal** Most Recent  1 month, 1 week ago

I will go with B and A

upvoted 1 times



  **Khanbaba43** 4 months, 2 weeks ago

1. Deleted after 7 years of creation

2. Some data may be deleted immediately



<https://www.examttopics.com/discussions/microsoft/view/49390-exam-ms-101-topic-3-question-63-discussion/>

upvoted 1 times

  **hagosm** 8 months, 2 weeks ago

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

upvoted 1 times

  **Armins** 1 year, 1 month ago

Deleted 7 years after they were created

and

Some data will be deleted immediately

upvoted 7 times

You have a Microsoft 365 subscription.

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

Defines sensitive data based on existing data samples

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

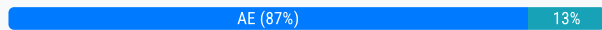
Which two components should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Suggested Answer: AE

Community vote distribution



Hard1k Highly Voted 1 year, 4 months 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 24 times

mikl 7 months, 4 weeks ago

<https://copilot.microsoft.com/> approves that A and E is correct.

upvoted 1 times

Vince_MCT Most Recent 1 month, 3 weeks ago

A, E

A. a trainable classifier:

A trainable classifier allows you to define sensitive information based on existing data samples. It can be used to train Microsoft 365 to recognize patterns in data that are indicative of sensitive content (e.g., financial data, personal information, or intellectual property). Once the classifier is trained, it can be used to identify and classify sensitive information in your environment.

E. a data loss prevention (DLP) policy:

A DLP policy is specifically designed to prevent the sharing of sensitive data outside of your organization. Once sensitive information is identified (either through a trainable classifier or predefined sensitive info types), a DLP policy can be applied to restrict actions such as sharing that data externally via SharePoint, Outlook email, or other communication channels.

upvoted 1 times

Tomtom11 6 months ago

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 item for application of Office sensitivity labels, Communications compliance policies, and retention label policies.

Sensitive information types (SITs) are pattern-based classifiers. They detect sensitive information like social security, credit card, or bank account numbers to identify sensitive items,

upvoted 2 times

🗨️ **miki** 7 months, 4 weeks ago

Selected Answer: AE

To configure a compliance solution that defines sensitive data based on existing data samples and automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages, you should configure the following two components:

A. a trainable classifier: Trainable classifiers in Microsoft 365 allow you to define sensitive data by providing examples of the data you're interested in. This machine learning tool can learn from the samples you provide and then identify similar content across your organization's data1.

E. a data loss prevention (DLP) policy: A DLP policy can use the trainable classifier to identify sensitive information and enforce rules that prevent the sharing of this data externally through SharePoint or email messages23.

These components work together to ensure that sensitive data, as defined by your provided samples, is protected from unauthorized external sharing.

upvoted 2 times

🗨️ **hagosm** 8 months, 2 weeks ago

The correct answers are A and E.

upvoted 1 times

🗨️ **GLlimaBR** 10 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** 1 year, 3 months 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** 1 year, 3 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 item for application of Office sensitivity labels, Communications compliance policies, and retention label policies.

<https://learn.microsoft.com/en-us/purview/classifier-get-started-with>

upvoted 1 times

🗨️ **RJTW070** 1 year, 3 months ago

Selected Answer: BE

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

See this

upvoted 1 times

🗨️ **Nandokun01** 1 year, 4 months 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** 1 year, 4 months ago

Agree Should be, BE

upvoted 1 times

🗨️ **Greatone1** 1 year, 4 months ago

Selected Answer: BE

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

upvoted 3 times

  **Nandokun01** 1 year, 4 months ago

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

upvoted 5 times

HOTSPOT -

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

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

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


Name	Role
User1	Owner
User2	Visitor


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

Edit rule




Conditions

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


Content contains 

Default Any of these 

Sensitive info types

IP Address  Instance count to  

Add

 Create group

+ Add condition


Exceptions

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

+ Add exception


Actions


Use actions to protect content when the conditions are met.


Restrict access or encrypt the content in Microsoft 365 locations 

Restrict access or encrypt the content in Microsoft 365 locations

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

Block everyone. 

Block only people outside your organization. 

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

How many files will be visible to User1 and User2 after Policy1 is applied to Site1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:

- 1
- 2
- 3
- 4
- 5

User2:

- 1
- 2
- 3
- 4
- 5

Answer Area

Suggested Answer:

User1:

- 1
- 2
- 3
- 4
- 5

User2:

- 1
- 2
- 3
- 4
- 5

 **mhmyz** Highly Voted 1 year, 3 months ago

File types supported for scanning


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

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

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

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

upvoted 8 times

 **examcrammer** Most Recent 7 months, 4 weeks ago

User 1 = 5, that's because the user is a site admin and they can access anything blocked by DLP. User 2 = 3 because .txt and .bmp files are not scanned in SharepointOnline and file1 only has 1 IP address so it doesn't match for the dlp rule.

upvoted 4 times

 **basak** 7 months, 3 weeks ago

user 2 should open 2 files (File1 - not in rule, and BMP file -cant scan)

upvoted 2 times

 **jarattdavis** 4 months, 2 weeks ago

User = 2.

Your explanation is valid

upvoted 1 times

🗨️ 👤 **hogegehoge** 1 year, 4 months ago

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

upvoted 4 times

🗨️ 👤 **osxvkwpcfxobjby** 1 year, 4 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** 1 year, 4 months ago

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

upvoted 17 times

🗨️ 👤 **sergioandreslq** 1 year, 2 months ago

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

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

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

User2: can open files with less than 2 ips and the format is not supported by data classification

User 2 can see: file1.docx, file4.bmp,

however,

the file2.txt-filex.xlsx and file5.doc are supported for data classification and the content has more than 2 ips.

upvoted 14 times

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

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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

USER SIGN-IN



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

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

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

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

Does this meet the goal?

- A. Yes
- B. No

Suggested Answer: B

Community vote distribution

B (100%)

mhmyz Highly Voted 1 year, 3 months ago

B.No

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

upvoted 12 times

NrdAlrt Highly Voted 1 year, 1 month 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 8 times

TopGun_1023 2 months ago

That's Microsoft for you.

upvoted 1 times

Greatone1 Most Recent 1 year, 4 months ago

Selected Answer: B

Should be no
upvoted 6 times

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

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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

USER SIGN-IN



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

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

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

Solution: From the 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

Suggested Answer: A

Community vote distribution

A (63%) B (38%)

Greatone1 Highly Voted 10 months, 2 weeks ago

Selected Answer: A

Correct answer is A
upvoted 9 times

TonyManero Most Recent 2 months, 1 week 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

Vukosir 4 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

🗨️ 👤 **AAlmani** 5 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 4 times

🗨️ 👤 **RJTW070** 5 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 2 times

🗨️ 👤 **bipsta** 5 months ago

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

upvoted 7 times

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

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

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

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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

USER SIGN-IN



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

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

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

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

Does this meet the goal?

- A. Yes
- B. No

Suggested Answer: A

Community vote distribution

A (67%) B (33%)

Greatone1 Highly Voted 1 year, 4 months ago

Selected Answer: A

the answer is A.

upvoted 13 times

sherifhamed Highly Voted 1 year, 3 months 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.examtactics.com/discussions/microsoft/view/50100-exam-ms-100-topic-2-question-56-discussion/>

upvoted 8 times


Crille Most Recent 1 month, 2 weeks ago

The answer is B

you need to sync fabric domain to azure ad with Azure ad connect

add fabric in domain and trust after that you can set UPN user2@fabric.com in Active directory

upvoted 3 times

  **Fidelak** 3 months, 2 weeks ago

I would venture this is more B than A, it says you add the domain as a custom domain in the admin.microsoft.com portal but doesn't mention anything about it being added into Azure AD connect as a domain. It's technically correct but only half of the true correct solution.

upvoted 3 times

  **ronin201** 6 months ago

Don't forget about Entra connect settings, if you add custom domain, it should be 1) verified 2) you must add it to Entra Connect for sync

upvoted 3 times

  **AAlmani** 11 months ago

Selected Answer: A

Correct answer is A

upvoted 2 times

  **RJTW070** 11 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 5 times

  **jbuexamtopics** 1 year, 1 month ago

Selected Answer: B

Didnt mentioned that it was verified.

upvoted 3 times

  **Constyle** 1 year, 2 months ago

Answer is A



upvoted 1 times

  **jbuexamtopics** 1 year, 2 months ago

Selected Answer: B

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

upvoted 5 times

  **Casticod** 1 year, 3 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 5 times

  **letters1234** 1 year, 4 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

  **NrdAirt** 1 year, 1 month 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 5 times

  **Greatone1** 1 year, 4 months ago

Looking at previous test no one has a real answer.

<https://www.examttopics.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

Suggested Answer: B

Community vote distribution


B (100%)

 **RJTW070** Highly Voted 3 months, 4 weeks ago

Selected Answer: B

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

upvoted 14 times

 **Takanami** Highly Voted 4 months, 1 week 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 6 times

 **RJTW070** Most Recent 3 months, 4 weeks ago

Selected Answer: B

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

upvoted 2 times

 **Greatone1** 4 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

Suggested Answer: B

Community vote distribution

B (100%)

 **RJTW070** Highly Voted 3 months, 4 weeks 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 8 times

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

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

Your network contains an Active Directory domain.

You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

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

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

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

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

Does this meet the goal?

A. Yes

B. No

Suggested Answer: B

Community vote distribution

B (81%)

A (19%)

 **Anonymous121011** Highly Voted 7 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 17 times

 **sherifhamed** Highly Voted 9 months 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.examttopics.com/discussions/microsoft/view/10379-exam-ms-100-topic-3-question-16-discussion/>

upvoted 7 times

 **e201546** Most Recent 1 month ago

Selected Answer: B

The OU can't be added via Sync Rules

upvoted 1 times

🗨️ **692a0df** 5 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 attribs 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 attribs from these 10 accounts.

So its A for me but only a 70% A.

upvoted 1 times

🗨️ **Abhishek1610** 5 months, 2 weeks ago

Selected Answer: B

From Azure AD Connect, you modify the filtering settings

upvoted 4 times

🗨️ **cpaljchc4** 5 months, 3 weeks ago

Selected Answer: B

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

upvoted 3 times

🗨️ **m2L** 6 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** 7 months ago

Selected Answer: B

This is a clear OU filtering question.

upvoted 2 times

🗨️ **benpatto** 7 months, 1 week ago

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

upvoted 1 times

🗨️ **daye** 7 months, 3 weeks ago

Selected Answer: B

No, It does not meet the goal since you don't 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

🗨️ **NrdAlrt** 7 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

🗨️ **[Removed]** 8 months, 1 week ago

Selected Answer: B

No.

Does not meet the goal.

upvoted 2 times

🗨️ **santi32** 9 months, 1 week 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

🗨️ **RJTW070** 10 months ago

Selected Answer: A

Yes, creating a new outbound synchronization rule from the Synchronization Rules Editor could potentially solve the issue¹. 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 synchronized². 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** 8 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 upn suffix will do the trick and is much easier.

upvoted 1 times

🗨️ **letters1234** 10 months 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** 8 months, 2 weeks ago

The rules editor is not the same as the ad configuration.

upvoted 1 times

🗨️ **Greatone1** 10 months, 1 week ago

Selected Answer: A

Correct answer should be yes

upvoted 2 times

🗨️ **osxvkwpcfxfobqjby** 10 months, 3 weeks ago

Selected Answer: A

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

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

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 subscription.

You need to review metrics for the following:

The daily active users in Microsoft Teams

Recent Microsoft service issues -

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

NOTE: Each correct selection is worth one point.

Answer Area

Teams daily active users:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

Recent Microsoft service issues:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

Answer Area

Teams daily active users:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

Suggested Answer:

Recent Microsoft service issues:

Microsoft Secure Score
Adoption Score
Service health
Usage reports

 **Casticod** Highly Voted 10 months, 2 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 10 times

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

1. Usage reports



2. Service Health

upvoted 2 times

 **Amir1909** 5 months ago

Correct

upvoted 1 times

  **daye** 7 months, 3 weeks ago

It's correct, easy one.

upvoted 2 times

  **gomezmax** 10 months, 1 week ago

Correct

upvoted 4 times

DRAG DROP -

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2. You need to ensure that each group can perform the tasks shown in the following table.

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

The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Roles

Billing Administrator

Global Administrator

Helpdesk Administrator

License Administrator

Service Support Administrator

User Administrator

Answer Area

Group1:

Group2:

Answer Area

Suggested Answer:


Group1:

Group2:

 **daye** 1 month, 2 weeks ago


correct

upvoted 3 times

 **amurp35** 3 months, 2 weeks ago

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

upvoted 4 times

 **Casticod** 4 months, 2 weeks ago

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

upvoted 3 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

Suggested Answer: C

Community vote distribution

C (83%)

A (17%)

🗨️ **nsotis28** Highly Voted 1 year, 4 months 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 13 times

🗨️ **TheMCT** 11 months, 1 week 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

🗨️ **Alecks** Highly Voted 1 year, 2 months 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 5 times

🗨️ **Subzerofrostbyt** Most Recent 1 month, 1 week ago

In Microsoft 365, the onmicrosoft.com domain is automatically created when you set up your subscription. However, Microsoft 365 subscriptions allow only one onmicrosoft.com domain per tenant.
upvoted 2 times

🗨️ **BurtSmart** 6 months, 3 weeks ago

<https://learn.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq?view=o365-worldwide> Maximum 5
upvoted 1 times

🗨️ **111112345345** 7 months, 2 weeks ago

Selected Answer: C

1 + 5 additional - tested
upvoted 1 times

🗨️ **Amir1909** 11 months ago

Correct
upvoted 1 times

🗨️ **TonyManero** 1 year ago

Selected Answer: C

In Microsoft documentation is specified max 5 onmicrosoft.com
upvoted 2 times

🗨️ **sherifhamed** 1 year, 3 months ago

Selected Answer: C

The correct answer is C. 5.

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

upvoted 1 times

🗨️ 👤 **Tjorno** 1 year, 3 months ago

Selected Answer: C

Only 5 onmicrosoft domains are possible

upvoted 2 times

🗨️ 👤 **martin_salan07** 1 year, 3 months 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

upvoted 1 times

🗨️ 👤 **santi32** 1 year, 3 months 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 2 times

🗨️ 👤 **Casticod** 1 year, 4 months 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 3 times

🗨️ 👤 **Casticod** 1 year, 4 months ago

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

upvoted 2 times

🗨️ 👤 **moshkoshbgosh** 1 year, 4 months ago

Selected Answer: A

The wording here could be misleading... while 5 is the maximum number of onmicrosoft.com domains that can be added, the questions 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 3 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"/>

Suggested Answer:

 **gbartumeu** Highly Voted 1 year, 3 months 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 14 times

Be41223 1 year, 3 months 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 51 times

JensV 1 year, 3 months ago

<https://learn.microsoft.com/en-us/azure/active-directory/roles/privileged-roles-permissions?tabs=admin-center#who-can-reset-passwords>
upvoted 8 times

basak 7 months, 3 weeks ago

wrong:

Password Administrator - Can reset passwords for non-administrators and Password Administrators.

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference>

upvoted 4 times

Exam2us 10 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 1 year, 1 month 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

JunetGoyal Most Recent 1 month, 1 week ago

NYN is correct, as

Password admin role is described bellow

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>

upvoted 3 times

MR_Eliot 3 months, 2 weeks ago

Correct:

Password Administrator Can reset passwords for non-administrators and Password Administrators.

upvoted 1 times

yaboo1617 4 months ago

Correct, password admin can't reset other types of admin passwords.

upvoted 1 times

wael_kodmani 4 months ago

correct answers

upvoted 1 times

APK1 4 months, 3 weeks ago

N,Y,N correct answer

upvoted 1 times

LakesWizard 5 months, 4 weeks ago

User1 can reset the password of User3.

Yes, it can, because of User3 is the User Administrator for the tenant not for the AD

User2 can update the display name of User1

Yes

User1 can reset the password of User2

No

upvoted 1 times

🗨️ **miki** 7 months, 3 weeks ago

The thing to pay attention to here is that a Password Administrator cannot change password of a user administrator - that's why its N, Y, N for me.

upvoted 3 times

🗨️ **ismaelo** 8 months, 3 weeks ago

Correct answer: YYY

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

🗨️ **Nico282** 6 months ago

You are reading the table the wrong way. Look at the COLUMN "Password Admin", the role can reset password only of Users, Directory readers, Guest inviters and other Password admins

upvoted 2 times

🗨️ **Amir1909** 11 months ago

Correct

upvoted 1 times

🗨️ **SBGM** 11 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** 1 year ago

Agree with Be41223

upvoted 1 times

🗨️ **spg1** 1 year, 1 month 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** 1 year, 1 month ago

I personally chose the answers: YYY!!

upvoted 3 times

🗨️ **Rylz** 1 year, 1 month 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** 1 year, 2 months 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** 1 year, 4 months ago

provided answer is correct

upvoted 1 times

Your network contains an Active Directory domain named adatum.com that is synced to Azure AD.

The domain contains 100 user accounts.

The city attribute for all the users is set to the city where the user resides.

You need to modify the value of the city attribute to the three-letter airport code of each city.


What should you do?

- A. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.
- B. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets.
- C. From Windows PowerShell on a domain controller, run the Get-MgUser and Update-MgUser cmdlets.
- D. From Azure Cloud Shell, run the Get-MgUser and Update-MgUser cmdlets.

Suggested Answer: A

Community vote distribution

A (100%)

 **Greatone1** Highly Voted 1 year, 4 months 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 9 times

 **Motanel** Most Recent 8 months, 4 weeks ago


Azure AD Powershell will be deprecated, so get_MgUser needs to be used.

upvoted 2 times

 **BJS78** 4 months, 3 weeks ago

Does not matter. Here you need to apply change on on-prem AD, not Azure-AD

upvoted 1 times


 **sherifhamed** 1 year, 3 months 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** 1 year, 3 months 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

HOTSPOT -

Your company has a Microsoft 365 E5 subscription.

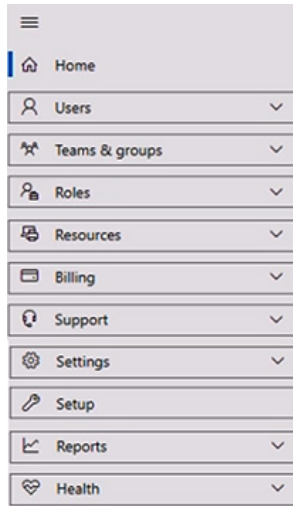
You need to perform the following tasks:

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.



Suggested Answer:

A screenshot of the Microsoft 365 admin center navigation menu, identical to the one above. In this version, the 'Support' and 'Reports' menu items are highlighted with a thick black border, indicating they are the correct answers for the tasks described in the question.

Casticod Highly Voted 10 months, 2 weeks ago

Correct.

Support to open case a MS

Report to access to the adoption Score

upvoted 5 times

Amir1909 Most Recent 5 months ago

Correct

upvoted 1 times

daye 7 months, 3 weeks ago

correct

upvoted 3 times

  **gomezmax** 10 months, 1 week ago

IT is Reports then Adoption Score

upvoted 4 times

You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Type
Group1	Security
Group2	Mail-enabled security
Group3	Microsoft 365
Group4	Distribution

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

You need to identify which two management tasks User5 can perform.

Which two tasks should you identify? Each correct answer presents a complete solution.


NOTE: Each correct selection is worth one point.

- A. Delete User2 and User4 only.
- B. Reset the password of User4 only.
- C. Reset the password of any user in Azure AD.
- D. Delete User1, User2, and User4 only.
- E. Reset the password of User2 and User4 only.
- F. Delete any user in Azure AD.

Suggested Answer: AE


Community vote distribution

AE (100%)

 **sherifhamed** Highly Voted 1 year, 3 months ago

The Question with the right picture here:

<https://www.examttopics.com/discussions/microsoft/view/98896-exam-ms-100-topic-3-question-21-discussion/>
upvoted 41 times

 **shaffer** 10 months, 1 week ago

Thank you, I was so confused
upvoted 1 times

 **Martham** 1 year, 2 months ago

Thanks alot
upvoted 1 times

 **Mustardonk** Highly Voted 1 year, 4 months ago

Wrong picture?
upvoted 6 times

 **Kock** Most Recent 1 month, 1 week ago

<https://learn.microsoft.com/pt-br/training/modules/manage-roles-groups-microsoft-365/4-explore-admin-roles-microsoft-365>

O administrador do usuário também pode concluir as seguintes ações:

- Gerencie nomes de usuários.
- Exclua e restaure usuários.
- Redefina senhas.
- Forçe usuários a sair.
- Atualize as chaves do dispositivo (FIDO).

upvoted 1 times

 **kayci** 8 months, 3 weeks 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 3 times

🗨️ **nordbymikael** 9 months, 1 week ago

Selected Answer: AE

Correct

upvoted 3 times

🗨️ **TheMCT** 11 months, 1 week 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 3 times

🗨️ **sergioandreslq** 1 year, 2 months 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** 1 year, 3 months ago

!!!!!!! Wrong picture !!!!!!!!

upvoted 1 times

🗨️ **Tisi** 1 year, 3 months ago

Wrong picture

upvoted 3 times

🗨️ **Master_Tx** 1 year, 3 months ago

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

upvoted 2 times

🗨️ **Casticod** 1 year, 4 months ago

Selected Answer: AE

A and E are correct.

upvoted 3 times

🗨️ **f7d3be6** 1 year, 4 months ago

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

upvoted 3 times

🗨️ **Vaati** 1 year, 4 months ago

Seems Wrong picture indeed

upvoted 3 times

HOTSPOT -

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.

Group1
Private group • 1 owner • 1 member

General Members **Settings** Microsoft Teams

General settings

Allow external senders to email this group

Send copies of group conversations and events to group members

Hide from my organization's global address list

Privacy

Private

Public

An external user named User1 has an email address of user1@outlook.com.

You need to add User1 to Group1.

What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Action:

Add User1 to the subscription as an active user.
For Group1, change the Privacy setting to Public.
For Group1, select Allow external senders to email this group.
Invite User1 to collaborate with your organization as a guest.

Portal:

The Microsoft Entra admin center
The Exchange admin center
The Microsoft 365 admin center
The Microsoft Purview compliance portal

Answer Area

Suggested Answer:

Action:

Add User1 to the subscription as an active user.
For Group1, change the Privacy setting to Public.
For Group1, select Allow external senders to email this group.
Invite User1 to collaborate with your organization as a guest.

Portal:

The Microsoft Entra admin center
The Exchange admin center
The Microsoft 365 admin center
The Microsoft Purview compliance portal


GLLimaBR **Highly Voted** 4 months 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 5 times

  **Casticod** Most Recent 10 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

  **GLL** 9 months, 2 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** 7 months, 3 weeks ago

True, you will be redirected to Entra...

upvoted 1 times

  **Master_Tx** 9 months, 3 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

  **hogehehoge** 10 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

  **hogehehoge** 10 months, 1 week ago

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

upvoted 1 times

  **Greatone1** 10 months, 2 weeks ago

Given answer is correct

<https://www.examttopics.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)

Suggested Answer: D

Community vote distribution

D (100%)

  **RJTW070** Highly Voted  10 months ago

Selected Answer: D

Pim should be right

upvoted 6 times

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

PIM is correct.

You need to ensure that User1 only has admin access for eight hours and requires approval before the role assignment takes place.

upvoted 1 times

  **Amir1909** 5 months ago

Correct

upvoted 1 times

  **daye** 7 months, 3 weeks ago

Selected Answer: D

Correct, PIM

upvoted 3 times

HOTSPOT -

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

Name	Type
Group1	Security
Group2	Mail-enabled security
Group3	Microsoft 365
Group4	Distribution

All the groups are deleted.

Which groups can be restored, and what is the retention period? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Groups that can be restored:

- Group3 only
- Group1 and Group2 only
- Group2 and Group4 only
- Group1, Group2, and Group3 only
- Group1, Group2, Group3, and Group4

Retention period:

- 24 hours
- 7 days
- 14 days
- 30 days
- 90 days

Answer Area

Groups that can be restored:

- Group3 only
- Group1 and Group2 only
- Group2 and Group4 only
- Group1, Group2, and Group3 only
- Group1, Group2, Group3, and Group4

Retention period:

- 24 hours
- 7 days
- 14 days
- 30 days
- 90 days

Suggested Answer:

 **amurp35** Highly Voted 1 year, 3 months 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 9 times

 **Kock** Most Recent 1 month, 1 week ago

. It isn't available for security groups and distribution groups. The 30-day group restoration period isn't customizable.

<https://learn.microsoft.com/en-us/entra/identity/users/groups-restore-deleted>

upvoted 1 times

 **Kock** 1 month, 1 week ago

Restore a deleted Microsoft 365 group in Microsoft Entra ID

<https://learn.microsoft.com/en-us/entra/identity/users/groups-restore-deleted>

upvoted 1 times

 **Hchfyvggjj** 1 month, 3 weeks ago

Release Preferences: This setting controls the release channel for Microsoft 365 updates. By configuring it to a faster release channel, User4 will receive early access to new features and updates.

* User1 only: User1 is the Global Administrator, possessing the highest level of permissions in the Microsoft 365 environment. They have the authority to modify the release preferences for all users, including User4.

upvoted 1 times

🗨️ 👤 **wael_kodmani** 4 months ago

correct!!

upvoted 1 times

🗨️ 👤 **KerrAvon** 10 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 2 times

🗨️ 👤 **imlearningstuffagain** 1 year, 2 months 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

upvoted 1 times

🗨️ 👤 **sherifhamed** 1 year, 3 months 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

🗨️ 👤 **Greatone1** 1 year, 4 months ago

Letters already provided the answer only m 365 groups can be restored not security or distribution groups

This functionality is restricted exclusively to Microsoft 365 groups in Azure AD. It isn't available for security groups and distribution groups.

Please note that the 30-day group restoration period isn't customizable.

upvoted 3 times

🗨️ 👤 **letters1234** 1 year, 4 months 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** 1 year, 4 months ago

Should be group 3 and 30 days

upvoted 3 times

🗨️ 👤 **DiligentSam** 1 year, 4 months ago

From ChatGPT: Mail-enabled security: Microsoft 365 and Distribution can be restored.

but i can't find this answer

Q2 30 days

upvoted 1 times

🗨️ 👤 **amurp35** 1 year, 3 months ago

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

upvoted 7 times

🗨️ 👤 **Khanbaba43** 4 months, 2 weeks ago

Yeah I agree. You can use chatGBT, but I wouldn't trust it 100%

upvoted 1 times

🗨️ 👤 **Greatone1** 1 year, 4 months ago

Deleted users and deleted Office 365 groups are available for restore for 30 days. You cannot restore a deleted security group.

upvoted 2 times

HOTSPOT -

You have a Microsoft 365 E5 subscription.

From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
On activation, require	Azure MFA
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	15 day(s)
Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	Yes

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

NOTE: Each correct selection is worth one point.

Answer Area

A user that is assigned the Global Administrator role as active [answer choice].

will lose the role after eight hours
 can reactivate the role every eight hours
 can reactivate the role every 15 days
 will lose the role after 15 days

You can make the Global Administrator role available to activation requests [answer choice].

for up to eight hours
 for up to three months
 for up to 15 days
 until the requests are revoked manually

Suggested Answer:

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

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 32 times

🗨️ **omnomsnom** 11 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** 1 year, 3 months ago

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

upvoted 6 times

🗨️ **amurp35** 1 year, 3 months 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 1 year, 3 months 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 16 times

🗨️ **mikl** 7 months, 4 weeks ago

Agree here.

upvoted 1 times

🗨️ **Vaerox** 11 months, 2 weeks ago

Agreed!

upvoted 2 times

🗨️ **Tomtom11** Most Recent 3 months, 3 weeks ago

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-resource-roles-configure-role-settings>
Activation maximum duration

Use the Activation maximum duration slider to set the maximum time, in hours, that an activation request for a role assignment remains active before it expires. This value can be from 1 to 24 hours.

upvoted 1 times

🗨️ **jarattdavis** 4 months, 2 weeks ago

These are trick questions, but the answer lies in the Question.

1. assigned (Solution is under the assignment section) = Active Assignment will Expire (lose) after 15 days

2. Activation (Solution is under the activation section) = Maximum Activation duration 8 hours.

I hope this clarify the question

upvoted 1 times

🗨️ **APK1** 4 months, 3 weeks ago

my selection

Box1) will lose the role after 15 days

Box2) for upto 3 months

upvoted 1 times

🗨️ **Atos** 5 months, 1 week ago

Given answer is correct, comments all look wrong imo.

upvoted 1 times

🗨️ **Turlin** 5 months, 3 weeks ago

poor wording because

1. the user will lose the role after 15 days, but they can have it activated every 15 days so both fits.

2. activation request last for 8 hours, but they can also request activations for the next 3 months

1. i would go with lose the role after 15 days because they would need privileged role admin to reactive it or have someone with that role do it.
2. i would go with for up to three months because its talk about how long the user is eligible to make request. to be the other way it should read available to activation request that last...

upvoted 4 times

🗨️ 👤 **miki** 7 months, 4 weeks ago

How I see it.

1. will lose the role after 15 days
2. for up to eight hours

upvoted 1 times

🗨️ 👤 **DONPHYLO** 8 months, 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 noter 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 2 times

🗨️ 👤 **Amir1909** 11 months ago

Correct

upvoted 1 times

🗨️ 👤 **m2L** 1 year 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 5 times

🗨️ 👤 **Nyamnyam** 1 year 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 4 times

🗨️ 👤 **daye** 1 year, 1 month 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** 1 year, 1 month ago

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

upvoted 2 times

🗨️ 👤 **northgaterebel** 1 year, 2 months 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 2 times

🗨️ 👤 **CheMetto** 1 year, 2 months 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** 1 year, 4 months ago

First one : will lose the role after 8 hours AND can reactivate every 8 hours

Right ?

upvoted 2 times

🗨️ 👤 **Casticod** 1 year, 4 months 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 5 times

🗨️ 👤 **nsotis28** 1 year, 4 months ago

first is correct - will lose the role after 8 hours

second is questionable -- why not 15 days ?

upvoted 4 times

🗨️ 👤 **cb0900** 1 year, 4 months ago

Re: the second question, agree it would be 15 days in this case.

The first question states "A user that is assigned the the Global Administrator role as active" and the active assignment is set to expire after 15 days.

upvoted 2 times

🗨️ 👤 **CheMetto** 1 year, 2 months 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

```

Connect-AzureAD -Scopes User.ReadWrite.All, Organization.Read.All
Connect-MgGraph
Connect-MSOLService

$E3 = Get-AzureADUser | Where SkuPartNumber -eq 'EnterprisePack'
Get-MgSubscribedSku
Get-MSOLAccountSKU

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

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

Set-AzureADUser -UserId User1@contoso.com -AddLicenses $LicenseOptions -RemoveLicenses @()
Set-MgUserLicense
Set-MSOLUser
  
```

Answer Area

```

Connect-AzureAD -Scopes User.ReadWrite.All, Organization.Read.All
Connect-MgGraph
Connect-MSOLService


$E3 = Get-AzureADUser | Where SkuPartNumber -eq 'EnterprisePack'
Get-MgSubscribedSku
Get-MSOLAccountSKU

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

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

Set-AzureADUser -UserId User1@contoso.com -AddLicenses $LicenseOptions -RemoveLicenses @()
Set-MgUserLicense
Set-MSOLUser
  
```

Suggested Answer:

 **Ruhansen** Highly Voted 1 year, 3 months ago

Correct - All Graph commands

upvoted 6 times

 **Kock** Most Recent 1 month, 1 week ago

Use Connect-MgGraph

Invoke Connect-MgGraph before any commands that access Microsoft Graph. This cmdlet gets the access token using the Microsoft Authentication Library.

upvoted 1 times

🗨️ 👤 **ronin201** 6 months ago

Azure AD and MSOnline PowerShell modules are deprecated as of March 30, 2024, this question may not be listed

upvoted 1 times

🗨️ 👤 **Amir1909** 11 months ago

Correct

upvoted 1 times

🗨️ 👤 **929826d** 1 year, 4 months 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

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

Suggested Answer: A

Community vote distribution

A (100%)

 **mikl** 1 month, 3 weeks ago

PIM is correct.

upvoted 2 times

 **nordbymikael** 3 months, 1 week ago

Selected Answer: A

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


upvoted 3 times

 **benpatto** 7 months, 1 week ago

Selected Answer: A

Correct

upvoted 4 times

 **BossLG** 8 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** 9 months ago

GIVEN ANSWERS IS CORRECT!!!

upvoted 4 times

 **BRico6969** 4 months, 3 weeks ago

Calm down Paul

upvoted 9 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.

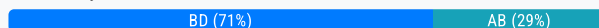
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

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.

Suggested Answer: BD

Community vote distribution



sherifhamed Highly Voted 1 year, 3 months ago

Selected Answer: BD

B & D is correct

Take a look here:

<https://www.examttopics.com/discussions/microsoft/view/26962-exam-ms-100-topic-2-question-19-discussion/>

upvoted 17 times

daye 1 year, 1 month ago

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

upvoted 5 times

Hard1k Highly Voted 1 year, 4 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 applications or services have been recently updated. Option D, reviewing the messages in the Microsoft 365 Admin mobile app, will only show you messages that have been sent to you personally.

upvoted 6 times

mikl 7 months, 4 weeks ago

Service health is only for when services are down - not updates.

Check your facts dude!

upvoted 1 times

Shloeb 1 year, 3 months 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

wael_kodmani Most Recent 4 months ago

Selected Answer: BD

B and D correct

upvoted 1 times

🗨️ 👤 **ubiquituz** 11 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** 11 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** 1 year, 3 months ago

A&B is correct.

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

upvoted 1 times

🗨️ 👤 **saya_222** 1 year, 3 months ago

Topic2 #19

upvoted 1 times

🗨️ 👤 **sherifhamed** 1 year, 3 months 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 4 times

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

Domains

+ Add domain Buy domain Refresh

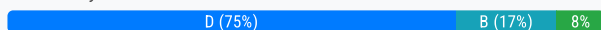
Domain name ↑	Status	Choose columns
<input type="checkbox"/> Sub1.contoso221018.onmicrosoft.com (D...	▲ Possible service issues	
<input type="checkbox"/> contoso.com	i Incomplete setup	
<input type="checkbox"/> contoso221018.onmicrosoft.com	✓ Healthy	
<input type="checkbox"/> Sub2.contoso221018.onmicrosoft.com	i Incomplete setup	

Which domain name suffixes can you use when you create users?

- A. only Sub1.contoso221018.onmicrosoft.com
- B. only contoso221018.onmicrosoft.com and Sub2.contoso221018.onmicrosoft.com
- C. only contoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com
- D. all the domains in the subscription

Suggested Answer: B

Community vote distribution



amurp35 Highly Voted 1 year, 3 months 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 44 times

kosikovec 1 month ago

agree.

upvoted 1 times

Vaerox 11 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 3 times

PMR24875 3 months, 2 weeks ago

I agree, just tested it

upvoted 2 times

m43s 11 months, 2 weeks ago

I agree too

upvoted 2 times

krzysztofbr 1 year, 1 month ago

agree.

upvoted 4 times

  **nsotis28** Highly Voted 1 year, 4 months ago

Domains with status "incomplete setup" can not be used

upvoted 9 times

  **justITtopics** Most Recent 1 month, 2 weeks ago

Selected Answer: B

I vote for B because I think is the only one that has the correct option (even though it is also incorrect): contoso221018.onmicrosoft.com

Copilot says:

You can only use the domain name suffix that has a healthy status for creating users, which is contoso221018.onmicrosoft.com.

Thus, the correct answer is B. only contoso221018.onmicrosoft.com and Sub2.contoso221018.onmicrosoft.com.

Even though Sub2.contoso221018.onmicrosoft.com is listed in option B, it isn't used as it has an incomplete setup, so only contoso221018.onmicrosoft.com is the correct and available suffix. Let me know if you need further assistance or have any other questions!



upvoted 2 times

  **Tr619899** 3 months ago

The domain name suffixes that can be used when creating users are those that have a "Healthy" status in your Microsoft 365 subscription. In this case, contoso221018.onmicrosoft.com is marked as Healthy, so it can be used. Other domains like Sub1.contoso221018.onmicrosoft.com and Sub2.contoso221018.onmicrosoft.com have issues or incomplete setups, meaning they cannot be used until the setup is completed and issues resolved.

Therefore, the correct answer is: B. only contoso221018.onmicrosoft.com and Sub2.contoso221018.onmicrosoft.com.



upvoted 1 times

  **radamelca** 3 months, 1 week ago

Selected Answer: B

B is the correct option, the other domains cannot be used.

upvoted 1 times

  **jarattdavis** 4 months, 2 weeks ago

Selected Answer: B

The image only shows two verified domains (contoso221018.onmicrosoft.com and Sub2.contoso221018.onmicrosoft.com), and it's not recommended to use the default [invalid URL removed] domain for user accounts.



upvoted 2 times

  **HelloItsSam** 6 months ago

Selected Answer: C

You can still create a user with an incomplete setup domain



upvoted 1 times

  **Eckay9** 8 months, 1 week 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 2 times

  **momowagdy** 8 months, 3 weeks 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 2 times

  **jedboy88** 3 weeks, 2 days ago

I tested too, But you can't add a user with a incomplete setup domain. When you're creating the user only appears the healthy or correct domains

upvoted 1 times

  **CharlesS76** 9 months 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 3 times

🗨️ 👤 **TheMCT** 11 months, 1 week 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** 1 year 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 2 times

🗨️ 👤 **m2L** 1 year 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** 1 year ago

Selected Answer: D

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

upvoted 4 times

🗨️ 👤 **passy951** 1 year 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** 1 year ago

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

upvoted 1 times

🗨️ 👤 **benpatto** 1 year, 1 month 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** 1 year, 1 month 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.

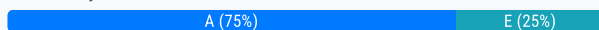
upvoted 5 times

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

Suggested Answer: A

Community vote distribution



certma2023 Highly Voted 1 year, 4 months ago

Selected Answer: A

Answer A.

PAM only works with Exchange Online at that time. Based on my test you see only Exchange roles inside the O365 Admin Portal (Settings -> Org Settings -> Security & Privacy -> Privileged Access)

The documentation also says:

"When will privileged access support Office 365 workloads beyond Exchange?
Privileged access management will be available in other Office 365 workloads soon. Visit the Microsoft 365 Roadmap for more details."

<https://learn.microsoft.com/en-us/purview/privileged-access-management>
upvoted 24 times

Clinson 1 year, 1 month ago

Additional in my customer's E5 tenant When I add a policy, the only scope available is Exchange. I suspect that will change moving forward but as of today's date it is only Exchange.
upvoted 1 times

mrac Highly Voted 1 year, 4 months ago

Selected Answer: E

Microsoft Purview Privileged Access Management (PAM) helps you manage, control, and monitor access within Microsoft 365. It's designed to manage privileged access for various Microsoft Office 365 workloads, including Microsoft Teams, Exchange Online, and SharePoint Online.

So, the correct answer is E. Microsoft Teams, Exchange Online, and SharePoint Online.
upvoted 10 times

jedboy88 Most Recent 3 weeks, 2 days ago

Selected Answer: E

Copilot: Microsoft Purview Privileged Access Management supports privileged access for multiple Office 365 workloads. Specifically, it supports: Exchange Online, SharePoint Online and Microsoft Teams
upvoted 2 times

Rooza 1 month ago

Selected Answer: E

I think its E
upvoted 1 times

Gaspar196431 4 months ago

Confusing but I think this statement on Microsoft's web site clears it up:

When will privileged access support Office 365 workloads beyond Exchange?

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

upvoted 2 times

🗨️ **ikarooo** 4 months, 1 week ago

I Think its E

upvoted 1 times

🗨️ **miki** 7 months, 4 weeks ago

Seems like its still only available for EoL.

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

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 2 times

🗨️ **Scotte2023** 8 months, 1 week 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** 8 months, 1 week 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** 10 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** 11 months, 2 weeks ago

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

upvoted 1 times

🗨️ **Charard** 11 months, 2 weeks ago

Selected Answer: A

EoL only.

upvoted 2 times

🗨️ **NrdAlrt** 1 year, 1 month 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** 1 year, 1 month ago

Selected Answer: E

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

upvoted 1 times

🗨️ **poesklap** 1 year, 2 months 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** 1 year, 2 months 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** 1 year, 3 months ago

Selected Answer: E

E. Microsoft Teams, Exchange Online, and SharePoint Online

Privileged Access Management (PAM) can be implemented for Microsoft Teams, Exchange Online, and SharePoint Online, among other workloads. It's not limited to just one or two of these services but can be extended to cover these services and more, depending on your organization's requirements.

upvoted 2 times

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

Suggested Answer:

User:

- User1 only
- User2 only
- User3 only**
- User1 and User2 only
- User1 and User3 only


 **certma2023** Highly Voted 1 year, 4 months ago

Answer is wrong.

To have new features & updates on all users or some/targeted users you need to configure "release preference" for the entire organization/tenant. Only the Global Admins can change this.

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

upvoted 49 times

 **daye** 1 year, 1 month ago

Exactly!

Release Preferences and User 1

upvoted 6 times

  **miki** 7 months, 4 weeks ago

I agree!

upvoted 2 times

  **nsotis28**  1 year, 4 months ago

release preferences

user1

upvoted 16 times

  **Casticod** 1 year, 4 months ago

Me too

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

upvoted 7 times

  **Kock**  1 month, 1 week ago



User Administrator

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#user-administrator>

Cloud Application Administrator

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#cloud-application-administrator>

upvoted 1 times

  **GingaNinja** 3 months, 1 week ago


I think the answer is right:

Requirement 1: only give the user the insider channel (Current)

Requirement 2: Principle of least privlidge

To do this you would need to visit cloud policy config and be atleast a Cloud apps admin

upvoted 1 times

  **jarattdavis** 4 months, 2 weeks ago

To provide early access to Microsoft 365 features and service updates, you need to modify the "Release preferences" setting.

User2, with the role of "Service Administrator", has the necessary privileges to manage service settings and configurations. This aligns with the principle of least privilege, as they have the required permissions without being a Global Administrator.

upvoted 1 times

  **APK1** 4 months, 3 weeks ago

Release preference & Global Admin (question is tricky as least privilege given only to confuse D:)



upvoted 1 times

  **Atos** 5 months, 2 weeks ago

The given answer is completely wrong.

I would say: Release Preferences & User 1

upvoted 1 times

  **blairskimo** 5 months, 3 weeks ago

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

upvoted 1 times" princple of least privelage maybe ?

upvoted 1 times

  **haimrevolution** 11 months, 1 week ago

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

upvoted 1 times

  **Festus365** 1 year, 1 month ago

Can user2 service support administrator modify the setting?

upvoted 1 times

  **imlearningstuffagain** 1 year, 2 months ago

The suggested anwer 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:

- Anti-spam
- Anti-Phishing
- Safe Attachments
- Safe Links

Impersonation and spoofing attacks in email messages:

- Anti-spam
- Anti-Phishing
- Safe Attachments
- Safe Links

Answer Area**Suggested Answer:**


Opening files in SharePoint that contain malicious content:


- Anti-spam
- Anti-Phishing
- Safe Attachments
- Safe Links

Impersonation and spoofing attacks in email messages:

- Anti-spam
- Anti-Phishing
- Safe Attachments
- Safe Links

 **PhoenixMan** Highly Voted 7 months, 1 week ago
in today exam
upvoted 5 times

 **Tibo49100** Most Recent 1 month, 2 weeks ago
There is no mention of Defender for Office 365 License so it's a bit confusing
upvoted 1 times

 **gomezmax** 10 months ago
Correct
upvoted 3 times

 **Greatone1** 10 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

	Severity	Alert name	Status	Tags	Category	Activity count	Last occurrence...
<input type="checkbox"/>	Medium	Alert1	Active	-	Threat management	2	3 minutes ago
<input type="checkbox"/>	High	Alert5	Resolved	-	Permissions	1	8 minutes ago

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

NOTE: Each correct selection is worth one point.

Answer Area

For Alert1, you can change Status to [answer choice].

- Investigating only
- Investigating or Resolved only
- Investigating or Dismissed only
- Investigating, Resolved, or Dismissed

For Alert5, you can [answer choice].

- not change Status
- change Status to Dismissed only
- change Status to Dismissed or Active only
- change Status to Dismissed or Investigating only
- change Status to Dismissed, Investigating, or Active

Answer Area

For Alert1, you can change Status to [answer choice].

- Investigating only
- Investigating or Resolved only
- Investigating or Dismissed only
- Investigating, Resolved, or Dismissed

Suggested 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 Highly Voted 1 year, 3 months ago

1 : Investigating, Resolved, or Dismissed

2 : change Status to Dismissed, Investigating, or Active

<https://www.examtopycs.com/exams/microsoft/ms-101/>

→ Topc3 #140

upvoted 25 times

norbe01 3 months, 2 weeks ago

Tested on DEV tenant, correct

upvoted 1 times

sergioandreslq 1 year, 2 months ago

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

upvoted 2 times

Romke_en_Tomke 1 year, 2 months ago

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

  **faeem** Highly Voted 1 year, 3 months 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 5 times

  **sergioandreslq** 1 year, 2 months ago

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

upvoted 2 times



  **m2L** Most Recent 1 year ago

Please guys can you test a gain?

On my side I tested with 2 different Alertes, 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 4 times



  **amurp35** 1 year, 3 months 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 4 times



  **daye** 1 year, 1 month 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 3 times

  **AMDf** 1 year, 3 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)

Suggested Answer: BE

Community vote distribution

BE (100%)

🗨️ **Hard1k** Highly Voted 4 months ago

Selected Answer: BE

Correct answers

upvoted 7 times

🗨️ **jedboy88** Most Recent 3 weeks, 1 day ago

Selected Answer: DE

Copilot: With a Microsoft 365 E3 subscription that includes Microsoft Defender for Endpoint Plan 1, the two features available are: Attack surface reduction (ASR) (Option E): This feature helps harden devices, prevent zero-day attacks, and offers granular control over endpoint access and behaviors¹.

Device discovery (Option D): This feature allows you to identify unmanaged devices in your network

upvoted 1 times

🗨️ **sigvast** 1 month, 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** 4 months 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** 4 months, 2 weeks ago

Selected Answer: BE

Answer is correct

<https://www.examtactics.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

Suggested Answer: C

Community vote distribution

D (83%)

C (17%)

-  **northgaterebel** Highly Voted 1 year, 2 months 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 13 times
-  **[Removed]** Highly Voted 1 year, 1 month ago
Selected Answer: D
 It was 90 days but was changed in october to 180 days so make of that what you will
 upvoted 9 times
-  **AK_1234** Most Recent 1 week, 5 days ago
 90 Days
<https://learn.microsoft.com/en-us/defender-office-365/mdo-data-retention>
 upvoted 2 times
-  **jedboy88** 3 weeks, 1 day ago
Selected Answer: D
 Copilot: Alerts in the Microsoft 365 Defender portal are retained for 6 months (Option D). This retention period ensures that you have sufficient time to review and act on alerts.
 upvoted 1 times
-  **JunetGoyal** 1 month, 1 week ago
 6 MonthS
 upvoted 1 times
-  **Kallely** 2 months ago
 C
 The retention policy for alerts in the Microsoft 365 Defender portal depends on the type of alert and the service:
 Defender for Cloud: Alerts are displayed for 90 days, even if the related resource is deleted.
 Defender for Office 365 Plan 1: Alert metadata details are retained for 90 days, while entity metadata details for email are retained for 30 days.
 Activity alert details for audit logs are retained for 7 days.
 Microsoft Defender for Endpoint: Data is retained for 180 days, but advanced hunting data is only available for 30 days.
 upvoted 1 times
-  **Kallely** 2 months ago
<https://learn.microsoft.com/en-us/defender-office-365/mdo-data-retention>
 upvoted 1 times
-  **mark2525** 3 months, 1 week ago
Selected Answer: A
 Just searched this online, says 30 days
 upvoted 1 times

🗨️ **norbe01** 5 months, 3 weeks ago

Guys so which one?

upvoted 1 times

🗨️ **nicolasechavarria** 6 months, 2 weeks ago

Selected Answer: D

For Plan 1 is 90, for Plan 2 is upto 6 months.

upvoted 1 times

🗨️ **examcrammer** 8 months, 2 weeks 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** 9 months, 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** 11 months ago

C is correct

upvoted 1 times

🗨️ **AncaMada112233** 1 year, 1 month 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

🗨️ **HeirBourne** 1 year, 1 month ago

its correct

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview>

upvoted 1 times

🗨️ **daye** 1 year, 1 month 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** 1 year, 1 month 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** 1 year, 1 month 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

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

Suggested Answer: C

Community vote distribution



🗨️ 👤 **KairKnows** Highly Voted 👍 1 year 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 19 times

🗨️ 👤 **Kmkz83510** 1 year 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 7 times

🗨️ 👤 **kosikovec** 1 month ago

correct.

upvoted 1 times

🗨️ 👤 **martinods** 6 months, 3 weeks ago

From the Ms link

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.

upvoted 1 times

🗨️ 👤 **KairKnows** 1 year ago

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

upvoted 13 times

🗨️ 👤 **Y2** Highly Voted 👍 10 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 6 times

🗨️ 👤 **Y2** 10 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 2 times

🗨️ 👤 **JunetGoyal** Most Recent 🕒 1 month, 1 week ago

The aggregate view shows data for the last 90 days and the detail view shows data for the last 30 days.

As Q says detailed so its 30 days

option C

upvoted 1 times

🗨️ 👤 **Frank9020** 1 month, 2 weeks ago

Selected Answer: B

The Compromised users report shows the number of user accounts that were marked as Suspicious or Restricted within the last 7 days. Accounts in either of these states are problematic or even compromised. With frequent use, you can use the report to spot spikes, and even trends, in suspicious or restricted accounts

upvoted 1 times

🗨️ **radamelca** 3 months, 1 week ago

Selected Answer: C

30 days for detailed reports.

upvoted 1 times

🗨️ **MR_Eliot** 3 months, 2 weeks ago

Selected Answer: C

C is true. Just checked this in my test tenant:

Tips

Filters will be honored in export results.

For the aggregate view, only data of the last 90 days is available for export. For the details table, only data of the last 30 days is available for export.

If the data exceeds 150,000 entries, we'll split the output into multiple files.

upvoted 1 times

🗨️ **cerniauskas** 3 months, 3 weeks ago

Selected Answer: C

No portal do Microsoft 365 Defender, ao exportar um relatório detalhado de usuários comprometidos, o maior intervalo de tempo que pode ser incluído no relatório é de 30 dias.

upvoted 2 times

🗨️ **b2be347** 3 months, 2 weeks ago

Muito bem notado, também efetuei um teste e concordo com a resposta de 30 dias.

upvoted 1 times

🗨️ **norbe01** 3 months, 4 weeks ago

You can export detailed data from the last 30 days, but the report only allows you to select a specific one-day range within that 30-day period.

upvoted 1 times

🗨️ **abil** 4 months ago

30 days - C

upvoted 1 times

🗨️ **e201546** 7 months ago

Selected Answer: C

Detailed data for 30 days.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-email-security?view=o365-worldwide#compromised-users-report>

upvoted 1 times

🗨️ **TonyManero** 7 months, 3 weeks ago

Selected Answer: A

I agree with 1 Day.

upvoted 2 times

🗨️ **LLama33** 8 months, 3 weeks 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 5 times

🗨️ **eks913** 9 months ago

Selected Answer: A

MS Training says 1 DAY.

upvoted 4 times

🗨️ **HelloItsSam** 9 months, 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** 9 months, 3 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

🗨️ 👤 **Craig** 10 months, 2 weeks ago

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

upvoted 1 times

🗨️ 👤 **Hasa** 10 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

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

Suggested Answer:

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

sergioandreslq Highly Voted 1 year, 2 months 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 6 times

MR_Eliot Most Recent 3 months, 2 weeks ago

First Box: Enable Users To Protect

Second Box: Enable in... protection

Enables enhanced impersonation results based on each user's individual sender map and allows you to define specific actions on impersonated messages

upvoted 2 times

🗨️ **omnomsnom** 11 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

🗨️ **faeem** 1 year, 3 months 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** 1 year, 3 months 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** 1 year, 4 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 3 times

🗨️ **letters1234** 1 year, 4 months ago

Would probably go for Phishing threshold as looking at the policy in [security.microsoft.com](https://security.microsoft.com/policies) / 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:

Server1-London:

Answer Area

Suggested Answer:

Computer1-London:

Server1-London:

Greatone1 Highly Voted 1 year, 4 months 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 16 times

jt2214 Highly Voted 1 year, 3 months ago

I I wish they were all this easy.
upvoted 11 times

sehlohomoletsane 1 year, 2 months ago

No cause same
upvoted 1 times

Kock Most Recent 1 month, 1 week ago

The appropriate policy types to the correct requirements:
Create anti-malware policies in the Microsoft Defender portal

<https://learn.microsoft.com/pt-br/training/modules/examine-exchange-online-protection/2-implement-anti-malware-policies>

upvoted 1 times

🗨️ 👤 **MR_Eliot** 3 months, 2 weeks ago

Correct.

upvoted 1 times

🗨️ 👤 **Tomtom11** 10 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 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.

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

upvoted 1 times

🗨️ 👤 **Festus365** 1 year, 1 month 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** 1 year, 1 month 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 3 times

🗨️ 👤 **amurp35** 1 year, 3 months ago

Yes, answer is correct due to rankings.

upvoted 4 times

DRAG DROP -

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

You need to configure policies to meet the following requirements:

Customize the common attachments filter.

Enable impersonation protection for sender domains.

Which type of policy should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements.

Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Policy Types	Answer Area
Anti-malware	Customize the common attachments filter: <input type="text"/>
Anti-phishing	Enable impersonation protection for sender domains: <input type="text"/>
Anti-spam	
Safe Attachments	

Policy Types	Answer Area
Anti-spam	Customize the common attachments filter: <input type="text" value="Anti-malware"/>
Safe Attachments	Enable impersonation protection for sender domains: <input type="text" value="Anti-phishing"/>

Suggested Answer:

f7d3be6 Highly Voted 1 year, 4 months ago

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

upvoted 10 times

Kock Most Recent 1 month, 1 week ago

The following anti-spam technologies are useful when you want to allow or block messages based on the message envelope (for example, the sender's domain or the source IP address of the message).

<https://learn.microsoft.com/pt-br/training/modules/examine-exchange-online-protection/7-examine-outbound-spam-filtering>

upvoted 1 times

Hchfyvggjj 1 month, 3 weeks ago

I think it's wrong

Safe Attachments:

This policy allows you to define rules for scanning and handling attachments. You can specify which file types to block, allow, or scan, and how to handle suspicious attachments (e.g., quarantine, sanitize, or block).

Anti-phishing:

This policy helps protect against phishing attacks by identifying and blocking emails that spoof the identity of legitimate senders.

upvoted 1 times

Amir1909 11 months ago

Correct

upvoted 1 times

benpatto 1 year, 1 month 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 differenet.

upvoted 4 times

  **amurp35** 1 year, 3 months ago

Correct

upvoted 1 times

You have an Azure AD tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Security Operator
User3	Security Reader
User4	Compliance Administrator

You plan to implement Microsoft Defender for Endpoint.

You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint.

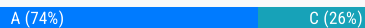
You need to identify which user can view security incidents from the Microsoft 365 Defender portal.

Which user should you identify?

- A. User1
- B. User2
- C. User3
- D. User4

Suggested Answer: A

Community vote distribution



AMDF Highly Voted 1 year, 3 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 21 times

amurp35 Highly Voted 1 year, 3 months 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 6 times

jedboy88 Most Recent 3 weeks, 1 day ago

Selected Answer: C

Copilot: C. User3 (Security Reader), as this role is specifically designed for viewing security incidents

<https://learn.microsoft.com/en-us/defender-endpoint/manage-incidents>

upvoted 1 times

Kock 1 month, 1 week ago

Políticas anti-phishing no Microsoft 365

<https://learn.microsoft.com/en-us/defender-office-365/anti-phishing-policies-about>

upvoted 1 times

AleFCI1908 2 months, 3 weeks ago

Selected Answer: C

"When you first sign in to the Microsoft Defender portal, you're granted either full access or read only access. Full access rights are granted to users with the Security Administrator role in Microsoft Entra ID.

Read only access is granted to users with a Security Reader role in Microsoft Entra ID."

upvoted 2 times

  **Tr619899** 3 months ago



The statement "You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint" means that "role-based permissions" are being enforced within the Microsoft Defender for Endpoint environment. When RBAC is enabled, access to security data (such as incidents, alerts, or reports) is controlled based on the user's assigned role in Azure AD. Each role has specific permissions regarding what they can view or manage.

In the context of the question:

- "Security Reader (User3)" is a role that grants "view-only access" to security information, including security incidents and alerts. With RBAC enabled, this role can view security incidents but cannot make changes to them, making "User3" the correct answer.

Thus, turning on RBAC ensures that "only those with the proper permissions (e.g., Security Reader)" can view the security incidents in Microsoft 365 Defender. This is why "Option C (User3)" is correct.

upvoted 2 times

  **MR_Eliot** 3 months, 2 weeks ago

Selected Answer: A

Initially, only those with Microsoft Entra Global Administrator or Security Administrator rights can 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 causes 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 administrator 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 who aren't Microsoft Entra Global Administrators 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

  **Jillis** 1 year, 3 months ago

Selected Answer: A

AMDF is correct

upvoted 3 times

  **letters1234** 1 year, 4 months 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 4 times

  **mccheesey** 1 year, 4 months 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 5 times

  **Greatone1** 1 year, 4 months ago

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

upvoted 3 times


  **Greatone1** 1 year, 4 months 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

  **Casticod** 1 year, 4 months 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 4 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

Suggested 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 1 year, 3 months 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 16 times

 **Murad01** Most Recent 6 months, 2 weeks ago

Given answer is correct

upvoted 2 times

 **Amir1909** 11 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	Ungrouped devices (default)	Not applicable

You create an incident email notification rule configured as shown in the following table.

Setting	Value
Name	Rule1
Alert severity	Low
Device group scope	Group1, Group2
Recipient email address	User1@contoso.com

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	<input type="radio"/>	<input type="radio"/>
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	<input type="radio"/>	<input type="radio"/>
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements

Suggested Answer:

	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	<input type="radio"/>	<input checked="" type="radio"/>
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	<input type="radio"/>	<input checked="" type="radio"/>
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	<input checked="" type="radio"/>	<input type="radio"/>

Greatone1 Highly Voted 1 year, 4 months ago

No - High severity Alert.

No - Doesn't have 'Device' in name

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

upvoted 14 times

Motanel Highly Voted 8 months, 3 weeks ago

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

No

Yes

upvoted 7 times

MR_Eliot Most Recent 3 months, 2 weeks ago

1. NO: You need to assign multiple alert severity. Checked this in test lab.

2. NO: Not member of Group1 and Group 2.

3. YES: Member of group 2 and low-severity alert.

Answers are correct.

upvoted 3 times

🗨️ 👤 **Besxp** 1 month, 1 week ago

Agree!

upvoted 1 times

🗨️ 👤 **665d390** 3 months, 2 weeks ago

You can create an alert only for "Low" (to Reduce Alert Fatigue) alerts..so will be NNY

upvoted 1 times

🗨️ 👤 **abill** 4 months ago

Yes - If you set a incident notification rule to "low," you will receive notifications for all incidents classified as low, medium, and high severity.

No

Yes

upvoted 1 times

🗨️ 👤 **spatrick** 7 months, 2 weeks ago

Tricky question. In this case you need to select high, medium, low or informational seperately.

<https://learn.microsoft.com/en-us/defender-xdr/configure-email-notifications>. Answer based on this is correct.

upvoted 1 times

🗨️ 👤 **OwerGame** 9 months, 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 3 times

🗨️ 👤 **amurp35** 1 year, 3 months ago

Correct

upvoted 3 times

🗨️ 👤 **nsotis28** 1 year, 4 months ago

correct answer

upvoted 2 times

You have a Microsoft 365 tenant that contains two users named User1 and User2.
You create the alert policy shown in the following exhibit.

Policy1

The screenshot shows the configuration for an alert policy named "Policy1". At the top, there are buttons for "Edit policy" and "Delete policy". The status is "On".

Name your alert

- Description: Add a description
- Severity: Medium
- Category: Information governance
- Policy contains tags: -

Create alert settings

- Conditions: Activity is FileChangeActivity
- Aggregation: Aggregated
- Scope: All users
- Threshold: 5
- Window: 1 hour

Set your recipients

- Recipients: User1@sk220912outlook.onmicrosoft.com
- Daily notification limit: 25

User2 runs a script that modifies a file in a Microsoft SharePoint library once every four minutes and runs for a period of two hours.
How many alerts will User1 receive?

- A. 2
- B. 5
- C. 10
- D. 25
- E. 30

Suggested Answer: D

Community vote distribution

A (68%)

D (32%)

Jillis Highly Voted 1 year, 3 months 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 20 times

Jahanzeb88 1 year, 3 months ago

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

upvoted 1 times

🗨️ 👤 **daye** 1 year, 1 month ago

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

upvoted 13 times

🗨️ 👤 **9711d59** 11 months ago

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

upvoted 3 times

🗨️ 👤 **KennehBE** 3 months, 1 week ago

Aggregation is on, so just 1 alert for the same thing per hour

upvoted 1 times

🗨️ 👤 **santi32** Highly Voted 👍 1 year, 3 months 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 10 times

🗨️ 👤 **daye** 1 year, 1 month ago

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

upvoted 1 times

🗨️ 👤 **Frank9020** Most Recent 1 month, 2 weeks ago

Selected Answer: A

User1 will receive 2 alert e-mails totally. This is because of the alert aggregation is enabled and the window is set to 1 hour.

upvoted 1 times

🗨️ 👤 **BayeSolutions** 6 months, 1 week ago

Answer is C

Alert Notifications for Policy Settings

Given the scenario where User2 runs a script that modifies a file in a Microsoft SharePoint library every four minutes and runs for two hours, with the alert policy set to trigger an alert after five activities within one hour:

The script runs for a total of 120 minutes (2 hours).

Modifications occur every 4 minutes, resulting in 30 modifications.

The policy triggers an alert for every 5 modifications.

Therefore, in 2 hours, the total number of alerts User1 will receive is:

C. 10 alerts

upvoted 1 times

🗨️ 👤 **ThomasMcThomasface** 1 year, 2 months ago

Selected Answer: A

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

upvoted 2 times

🗨️ 👤 **sergioandreslq** 1 year, 2 months 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 intervale which in this case the max is 15 min but each threshold is reached ever 20 min. each even will generate a single alert.

upvoted 1 times

🗨️ 👤 **sergioandreslq** 1 year, 1 month ago

Sorry for my wrong answer, the window interval is 1 hour, which means that 1 alert will be triggered per hour is threshold 5 is reached in this hour.

The correct answer is the A.

upvoted 2 times

🗨️ 👤 **gomezmax** 1 year, 2 months ago

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

upvoted 1 times

🗨️ 👤 **Greatone1** 1 year, 3 months ago

2 is correct answer

<https://www.examttopics.com/discussions/microsoft/view/94370-exam-ms-101-topic-3-question-150-discussion/>

upvoted 2 times

🗨️ 👤 **spectre786** 1 year, 3 months ago

Anyone got the right answer please ?

upvoted 1 times

🗨️ 👤 **nsotis28** 1 year, 4 months ago

picture is wrong

In any case key here is "aggregation"

<https://learn.microsoft.com/en-us/purview/alert-policies?view=o365-worldwide>

upvoted 1 times

🗨️ 👤 **spectre786** 1 year, 3 months ago

So right answer is A. 2 ?

upvoted 2 times

🗨️ 👤 **gomezmax** 1 year, 4 months ago

D Good 25

upvoted 3 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.

Suggested Answer: B

Community vote distribution

B (100%)

 **solderboy** Highly Voted 6 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 6 times


 **Greatone1** Most Recent 10 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 4 times

 **Casticod** 10 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.)

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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

USER SIGN-IN



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

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can authenticate to Azure AD by using a username of user1@contoso.com.	<input type="radio"/>	<input type="radio"/>
User2 can authenticate to Azure AD by using a username of user2@contoso.com.	<input type="radio"/>	<input type="radio"/>
User3 can authenticate to Azure AD by using a username of user3@contoso.com.	<input type="radio"/>	<input type="radio"/>

Suggested Answer:

Statements	Yes	No
User1 can authenticate to Azure AD by using a username of user1@contoso.com.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can authenticate to Azure AD by using a username of user2@contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can authenticate to Azure AD by using a username of user3@contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>

Greatone1 Highly Voted 1 year, 4 months 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 24 times

OwerGame Most Recent 10 months, 1 week ago

Federation is disabled

upvoted 1 times

Vaerox 11 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 1 year ago

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

upvoted 2 times

Khanbaba43 4 months, 2 weeks ago

Answers would be the same even if PHS was enabled. i.e. YNN

Because "Federation" is disabled

upvoted 1 times

rfree 1 year, 3 months 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 1 year, 3 months ago

Pass-through is enabled so the AD server authenticates the password

upvoted 5 times

profitchannel 3 months ago

in my opinion, user1 can logon to Azure AD, but is authenticated by Windows AD. So the phrasing of the questions is technically not correct.

upvoted 1 times

HOTSPOT -

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2022	Domain controller
Server2	Windows Server 2016	Member server
Server3	Server Core installation of Windows Server 2022	Member server

You purchase a Microsoft 365 E5 subscription.

You need to implement Azure AD Connect cloud sync.

What should you install first and on which server? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Install:

- The Azure AD Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server:

- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

Answer Area


Suggested 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 1 year, 4 months ago

Answer is correct.

You need to install a small agent on an On-Premises server. This server must run Windows Server 2016 or later. Agent installation on DC is supported. Agent installation on Windows Server Core is not supported.

upvoted 8 times

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

Ok I checked, server core isn't supported, but would server2 be the only option then?

upvoted 1 times

 **Hchfyvggjj** 1 month, 3 weeks ago

Isn't it more advisable to install the provisioning agent on server core because its light weight and offers better performance, I would think that because domain controllers are so busy, it wouldn't be the first option.



upvoted 1 times

 **jarattdavis** 4 months, 2 weeks ago

Install: The software you need to install for Microsoft Entra Connect cloud sync is "The Azure AD Connect provisioning agent."



Server: The best practice is to install the Azure AD Connect provisioning agent on a member server, not on a domain controller. Thus, you should choose "Server2 only." (since Server2 is a member server).

upvoted 4 times

  **KakTak** 6 months, 1 week ago



I don't understand why would we install agent when we need azure ad connect?

upvoted 1 times

  **KakTak** 6 months, 1 week ago

Ah sorry, I missed cloud sync. Answers are correct.

upvoted 1 times

  **daye** 1 year, 1 month 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 2 times

  **letters1234** 1 year, 4 months 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 3 times

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Member of	Device
User1	Group1	Device1
User2	Group1	Device2, Device3

The devices are configured as shown in the following table.

Name	Platform	Azure AD join type
Device1	Windows 11	None
Device2	Windows 10	Joined
Device3	Android	Registered

You have a Conditional Access policy named CAPolicy1 that has the following settings:

Assignments -

Users or workload identities: Group1

Cloud apps or actions: Office 365 SharePoint Online

Conditions -

Filter for devices: Exclude filtered devices from the policy

Rule syntax: device.displayName -startsWith "Device"

Access controls -

Grant -

Grant: Block access -

Session: 0 controls selected -

Enable policy: On -

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access Site1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device2.	<input type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device3.	<input type="radio"/>	<input type="radio"/>

Answer Area			
	Statements	Yes	No
Suggested Answer:	User1 can access Site1 from Device1.	<input type="radio"/>	<input checked="" type="radio"/>
	User2 can access Site1 from Device2.	<input checked="" type="radio"/>	<input type="radio"/>
	User2 can access Site1 from Device3.	<input checked="" type="radio"/>	<input type="radio"/>

  **amurp35** Highly Voted  1 year, 3 months 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 50 times

  **Khanbaba43** 4 months, 1 week ago

Amurp35, You should take up teaching as a profession. *thumbs up*
upvoted 1 times

  **Paul_white** 1 year, 2 months ago



MY BROTHER YOU ARE TOO GOOD!!!! EXCELLENT RESPONSE
upvoted 7 times

  **ghjbhj** 1 year, 3 months 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 therefor blocked. N/Y/Y
upvoted 5 times

  **Motanel** 8 months, 1 week ago

But if the filter is not applied, then the default will be applied, which is allow, right?
upvoted 1 times

  **ThomasMcThomasface** 1 year, 2 months ago

This translation is so very useful to me. Thank you so much. We need more people like you

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)

Suggested Answer: D

Community vote distribution

D (81%)

Other

 **letters1234**  1 year, 4 months 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** 1 year, 3 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 any more. Have a look:



<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#countriesregions>

upvoted 3 times

 **amurp35** 1 year, 3 months ago

You are thinking of user-risk, which gets remediated through SSPR.

upvoted 1 times

 **jedboy88**  2 weeks, 6 days ago

Selected Answer: C

By configuring named locations, you can define trusted IP ranges or countries. This way, you can adjust the Conditional Access policies to allow sign-ins from these locations, reducing the likelihood of users being blocked while traveling. This approach helps maintain security while providing flexibility for users on the move.

upvoted 1 times

 **Subzerofrostbyt** 1 month, 1 week ago

answer is D., Since the goal is to allow users to remediate the issue without administrator intervention, enabling Self-Service Password Reset (SSPR) is the most suitable choice. This allows users to recover access when their sign-ins are blocked, for instance, when traveling to new locations.

upvoted 1 times

 **arielreyes2712** 4 months, 1 week ago

Selected Answer: B

Answer is B. Sign-in risk events can self-remediated by MFA. The impossible travels will trigger a sign-in risk alert, not a user-risk one.

upvoted 3 times

🗨️ **Scotte2023** 8 months, 1 week 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** 8 months, 3 weeks 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 authenticateur , ceci est plus efficace et adéquat que de demander à un utilisateur de changer son mot de passe à chaque connexion

upvoted 2 times

🗨️ **OwerGame** 10 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** 11 months ago

D is correct

upvoted 1 times

🗨️ **Blixa** 1 year 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

🗨️ **NrdAirt** 1 year, 1 month 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

🗨️ **NrdAirt** 1 year, 1 month 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** 1 year, 2 months 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** 1 year, 2 months 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** 1 year, 2 months ago

ops... sorry,. All users are in france, so modifying MFA doesn't make any sense... yes, go with D

upvoted 1 times

🗨️ **sergioandreslq** 1 year, 2 months 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** 1 year, 3 months 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** 1 year, 3 months 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** 1 year, 3 months ago

I agree that sign-in risk is remediated by MFA, but re-reading the question shows that all users are in France, and all have MFA. If all users are already registered for MFA, what can be changed in the MFA policy to allow self-remediate?

B is most likely the answer but can't find the justification

upvoted 1 times

🗨️ **gomezmax** 1 year, 4 months ago

The Answer Is C

upvoted 1 times

🗨️ **DiligentSam** 1 year, 4 months 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 2 times

🗨️ **amurp35** 1 year, 3 months ago

Why do people supply 'answers' from ChatGPT? It makes things up, literally.

upvoted 1 times

🗨️ **amurp35** 1 year, 3 months ago

Also, you actually quoted the correct answer even though you chose the wrong one. See your comment "Additionally, if they are blocked, they can remediate the issue themselves by verifying their identity through MFA". Think, why would you add whole countries as named locations? That defeats the purpose of MFA.

upvoted 2 times

You have a Microsoft 365 E5 subscription that contains the following user:

Name: User1 -

UPN: user1@contoso.com -

Email address: user1@marketing.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.

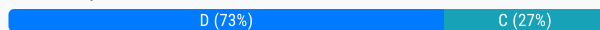
You need to ensure that User1 can sign in to Outlook on the web by using user1@marketing.contoso.com.

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.

Suggested Answer: D

Community vote distribution



benpatto Highly Voted 1 year, 1 month 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 6 times

miki Most Recent 7 months, 3 weeks ago

Selected Answer: D

To ensure that User1 can sign in to Outlook on the web using the email address user1@marketing.contoso.com, you should modify the UPN of User1. The User Principal Name (UPN) is the login name for Office 365 services, and it needs to match the email address the user is trying to sign in with. Since the UPN currently is user1@contoso.com, changing it to match the email address user1@marketing.contoso.com should resolve the sign-in issue.

So, the correct answer is:

D. Modify the UPN of User1.

upvoted 4 times

CharlesS76 9 months 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 9 months, 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 11 months ago

D is correct

upvoted 1 times

2dwarf 1 year, 1 month ago

Selected Answer: D

D is right

upvoted 1 times

🗨️ 👤 **TP447** 1 year, 1 month 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** 1 year, 2 months ago

Selected Answer: D

I agree with Milad

upvoted 1 times

🗨️ 👤 **MZeeshanTayyab** 1 year, 2 months ago

Selected Answer: D

D is right

upvoted 2 times

🗨️ 👤 **Paul_white** 1 year, 3 months ago

ANSWER IS D

upvoted 3 times

🗨️ 👤 **[Removed]** 1 year, 3 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** 1 year, 2 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 9 times

🗨️ 👤 **It2673** 4 months, 2 weeks ago

Well Bro actually you can login with an email address (<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-use-email-signin>) but as every MS question it's unclear if this is enabled or not so I guess we'll go with the default settings

upvoted 1 times

🗨️ 👤 **spectre786** 1 year, 3 months ago

I think it's D. Modify the UPN

upvoted 2 times

HOTSPOT -

Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2
Group2	Security Group - Global	OU2

The groups have the members shown in the following table.

Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.

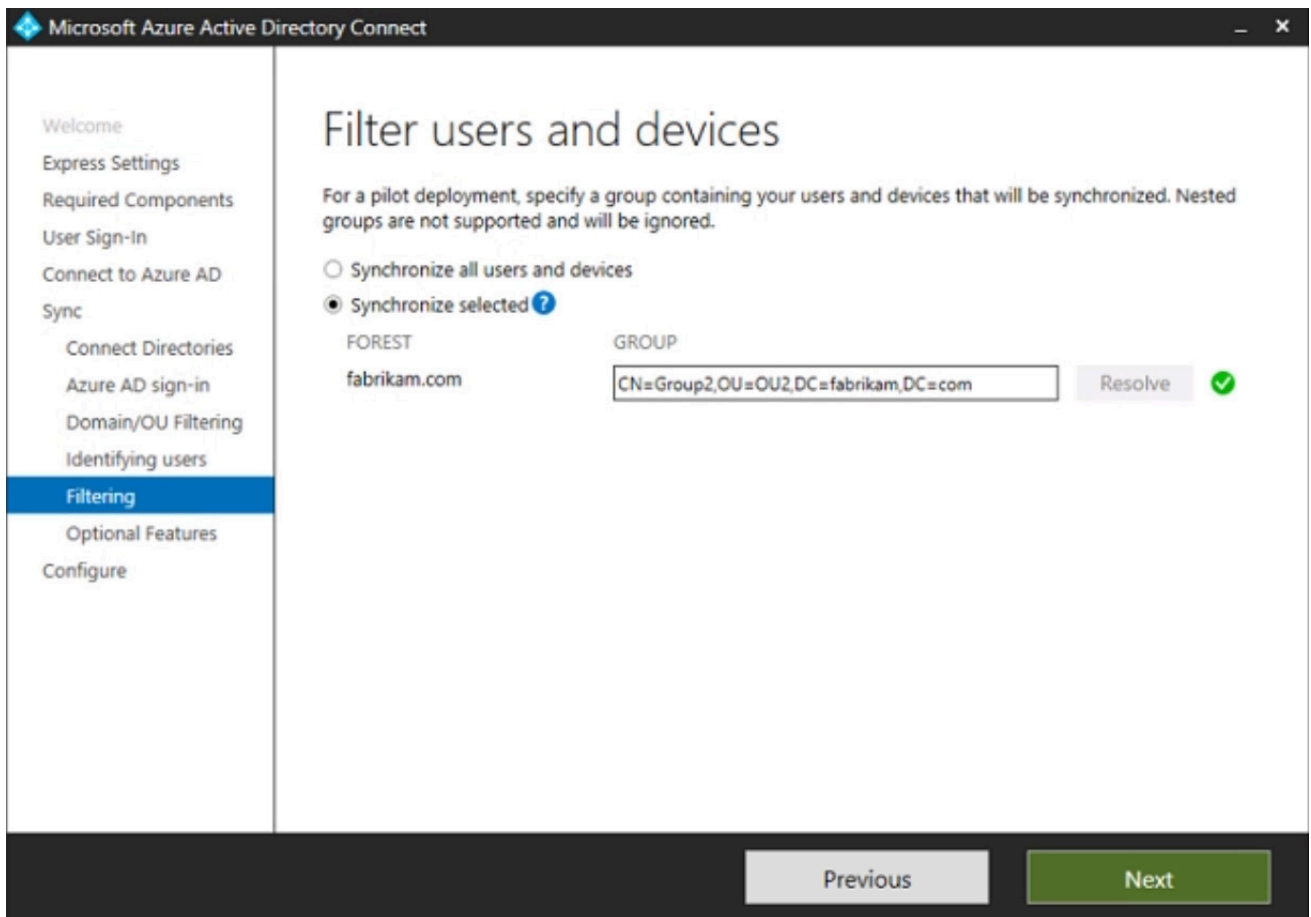
You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)

The screenshot shows the Microsoft Azure Active Directory Connect interface. The title bar reads "Microsoft Azure Active Directory Connect". On the left is a navigation pane with the following items: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, Connect Directories, Azure AD sign-in, **Domain/OU Filtering** (highlighted), Identifying users, Filtering, Optional Features, and Configure. The main content area is titled "Domain and OU filtering". It shows a "Directory:" dropdown menu set to "fabrikam.com" and a "Refresh Ou/Domain" button with a question mark. Below this are two radio button options: "Sync all domains and OUs" (unselected) and "Sync selected domains and OUs" (selected). A list of organizational units is displayed with checkboxes:

- fabrikam.com
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Infrastructure
 - LostAndFound
 - Managed Service Accounts
 - OU1
 - OU2
 - Program Data
 - System
 - Users

 At the bottom of the window are "Previous" and "Next" buttons.

You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering tab.)



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"/>

Suggested Answer:

Answer Area

Statements	Yes	No
User2 will synchronize to Azure AD.	<input type="radio"/>	<input checked="" type="radio"/>
Group2 will synchronize to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User3 will synchronize to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>

Greatone1 Highly Voted 1 year, 4 months 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 12 times

ATHOOS Highly Voted 1 year, 1 month ago

Group2 will not be synchronized...

NNY

upvoted 7 times

  **rcristiano** Most Recent 1 month, 4 weeks ago

YNY. A filtragem esta habilitada portanto somente membros do GRUPO 2 serão sincronizados. GRUPO 2 nao sincroniza porque não pode ser membro de si mesmo.

upvoted 1 times

  **It2673** 4 months, 2 weeks ago

So many wrong comments ...

Filtering is enabled so only members of Group2 will be synced. Group2 cannot be a member of itself. Group2 will not be synced (even if it is in OU2)

upvoted 4 times

  **Tomtom11** 9 months, 1 week ago

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

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 E5 subscription.

From Azure AD Identity Protection on August 1, you configure a Multifactor authentication registration policy that has the following settings:

Assignments: All users -

Controls: Require Azure AD multifactor authentication registration

Enforce Policy: On -

On August 3, you create two users named User1 and User2.

Users authenticate by using Azure Multi-Factor Authentication (MFA) for the first time on the dates shown in the following table.

User	Date
User1	August 5
User2	August 7

By which dates will User1 and User2 be forced to complete their Azure MFA registration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:

- August 6
- August 17
- August 19
- September 3
- September 5

User2:

- August 8
- August 17
- August 19
- August 21
- September 7

Answer Area

User1:

- August 6
- August 17
- August 19
- September 3
- September 5

User2:

- August 8
- August 17
- August 19
- August 21
- September 7

Suggested Answer:

 **fim322** Highly Voted 1 year, 4 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 14 times

 **Khanbaba43** Most Recent 4 months, 2 weeks ago

You have 14 days to register.

User1: Aug 19

User2: Aug 21

Easy stuff!

upvoted 3 times

🗨️ 👤 **miki** 7 months, 3 weeks ago

User experience

Microsoft Entra ID Protection will prompt your users to register the next time they sign in interactively and they'll have 14 days to complete registration. During this 14-day period, they can bypass registration if MFA isn't required as a condition, but at the end of the period they're required to register before they can complete the sign-in process.

upvoted 1 times

🗨️ 👤 **ELQUMS** 12 months ago

Just stupid question, would be better to just ask how many days you need to register the MFA

upvoted 3 times

🗨️ 👤 **spektrum1988** 11 months ago

Now you also have to do math.

upvoted 3 times

🗨️ 👤 **passy951** 1 year ago

Answers are correct.

Imagine beeing bad at math during the exam :D

upvoted 4 times

🗨️ 👤 **Vaerox** 11 months, 1 week ago

Exactly, because of this...I don't expect the question will be in the exam.

upvoted 2 times

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 subscription.

You need to sync the domain with the subscription. The solution must meet the following requirements:

On-premises Active Directory password complexity policies must be enforced.

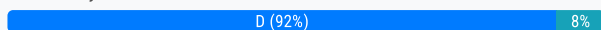
Users must be able to use self-service password reset (SSPR) in Azure AD.

What should you use?

- A. password hash synchronization
- B. Azure AD Identity Protection
- C. Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
- D. pass-through authentication

Suggested Answer: D

Community vote distribution



Rick_James 2 months, 3 weeks ago

PTA provides enhanced security by enforcing on-premises policies in real-time, suited for organizations with complex security requirements
upvoted 1 times

APK1 4 months, 2 weeks ago

Selected Answer: D

Complex password = PTA
upvoted 2 times

diasblackdc 5 months, 1 week ago

D "However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead."
upvoted 1 times

mikl 7 months, 3 weeks ago

Selected Answer: D

I would go for D here.
upvoted 1 times

spektrum1988 11 months, 1 week ago

Answer A works if password writeback is enabled, but they don't mention it.
upvoted 2 times

TheMCT 11 months, 1 week 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 1 year, 1 month 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 3 times

Bouncy 11 months, 1 week 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 1 year, 4 months 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

  **Casticed** 1 year, 4 months 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 2 times

  **Casticed** 1 year, 4 months 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

  **sergioandreslq** 1 year, 2 months ago

D: On-premises Active Directory password complexity policies must be enforced.

this is PTA

upvoted 2 times

  **sergioandreslq** 1 year, 1 month 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** 1 year, 4 months ago

answer is correct, SSPR works for both Pass- thru and hash sync. The key here is that on-prem password policies need enforced.

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

upvoted 3 times

  **Greatone1** 1 year, 4 months 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

  **hogegehoge** 1 year, 4 months ago

I think A is correct. Because Users must use SSPR in AzureAD.

upvoted 3 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

Suggested Answer: B

Community vote distribution

B (100%)

 **sherifhamed** Highly Voted 1 year, 3 months 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 7 times

 **arielreyes2712** Most Recent 4 months, 1 week ago

Selected Answer: B

Right answer is B

upvoted 1 times

 **jarattdavis** 4 months, 3 weeks ago

Selected Answer: B

By defining the VDI's IP range as a trusted location, you can reduce the likelihood of sign-in attempts being flagged as high-risk.

upvoted 1 times

 **mikl** 7 months, 3 weeks ago

Selected Answer: B

When users are regularly blocked from accessing Microsoft 365 services while using a corporate Virtual Desktop Infrastructure (VDI) solution, it's likely due to the sign-in risk policy detecting something unusual about the sign-ins from the VDI environment. To address this issue without compromising security, you should configure a trusted location.

By setting up a trusted location in Azure AD, you can define a named location that is considered safe. Sign-ins from this location are less likely to be marked as risky, which can help prevent legitimate users from being blocked when accessing Microsoft 365 services from the VDI solution.

So, the correct answer is:

B. a trusted location.

This will allow users to access Microsoft 365 without being impeded by the sign-in risk policy when they are signing in from the VDI environment, which is considered a secure and controlled access point.



upvoted 2 times



 **Moazzamfarooqiiii** 10 months, 2 weeks 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 3 times

  **markcasera** 10 months ago
Stop posting CGPT Responses bro!
upvoted 5 times

  **Amir1909** 11 months ago
B is correct
upvoted 1 times

  **Paul_white** 1 year, 3 months ago
CORRECT ANSWER SHOULD BE C
upvoted 3 times

  **Paul_white** 1 year, 2 months ago
NEVER MIND, ITS B. A TRUSTED LOCATION
upvoted 1 times

  **certma2023** 1 year, 4 months ago

Selected Answer: B

Answer B.

Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives.

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>
upvoted 3 times

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains a user named User1.
Azure AD Password Protection is configured as shown in the following exhibit.

Custom smart lockout

Lockout threshold ⓘ

15 ✓

Lockout duration in seconds ⓘ

600 ✓

Custom banned passwords

Enforce custom list ⓘ

Yes

No

Custom banned password list ⓘ

3hundred
Eleven
Falcon
Project
Tailspin

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

Enforced

Audit

User1 attempts to update their password to the following passwords:

F@lcon -

Project22 -

T4il\$pin45dg4 -

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

NOTE: Each correct selection is worth one point.

Answer Area

[Answer choice] will be accepted as a password.

Only T4il\$pin45dg4
Only F@lcon and T4il\$pin45dg4
Only Project22 and T4il\$pin45dg4
F@lcon, Project22, and T4il\$pin45dg4

If User1 enters the same wrong password 15 times, waits 11 minutes, and then enters the same wrong password again, the user [answer choice].

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.

Suggested 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].

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



  **vercracked_007** Highly Voted 1 year, 3 months 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 19 times

  **MR_Eliot** 3 months, 1 week ago


I second this.

upvoted 1 times

  **EM1234** 1 year, 3 months 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** 1 year 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 5 times

  **Kmkz83510** 1 year 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 4 times

  **letters1234** Highly Voted 1 year, 4 months ago

Answers are correct

Only T4il\$pin45dg4 will be allowed to change, the other two have an exact or within 1 character match to the banned passwords:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#fuzzy-matching-behavior>

Lockout period is 10 minutes (600 seconds) meaning on the 11th minute, the count starts again from 1 and would need another 15 bad passwords within the next 9 minutes to lock the user out.

upvoted 18 times

  **Kmkz83510** 1 year 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

  **mikl** 7 months, 3 weeks ago



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 1 times

  **Noble00** 1 year ago

You are very right.

upvoted 1 times

  **GingaNinja** Most Recent 3 months, 1 week ago

I think people are missing the point. 15 bad password attempts does not go over the threshold. Lockout happens on 16th try

upvoted 1 times

🗨️ 👤 **jarattdavis** 4 months, 2 weeks ago

Box 1 - T4il\$pin45dg4

Box 2 - Can attempt to sign in again immediately.

Explanation for Box2:

After 15times user will be locked out. If user wait more than 600 seconds, he will be allowed to try again. Now the user has waited $60\text{sec} \times 11 = 660$.

That means the user will be allowed to try again immediately

upvoted 1 times

🗨️ 👤 **mikl** 7 months, 3 weeks ago

Box 1 - T4il\$pin45dg4

Box 2 will be locked out again

The reason why the F@lcon does not work is documented here : <https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-configure-custom-password-protection#configure-custom-banned-passwords>

Regarding why its locked out again is found here : <https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-smart-lockout>

upvoted 2 times

🗨️ 👤 **GeorgeMar** 8 months, 3 weeks 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 5 times

🗨️ 👤 **Vukosir** 10 months, 2 weeks 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

🗨️ 👤 **mikl** 7 months, 3 weeks ago

Wrong.

Read here : <https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-configure-custom-password-protection#configure-custom-banned-passwords>

upvoted 1 times

🗨️ 👤 **TP447** 1 year, 1 month 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 wouldnt trigger a lockout. Therefore the user could just attempt to sign in again.

Seems like a poorly worded question or a trick..

upvoted 6 times

🗨️ 👤 **mikl** 7 months, 3 weeks ago

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 1 times

🗨️ 👤 **ExamCheater1993** 1 year, 3 months ago

Picture is correct. The trap is, that this persons enters the SAME password multiple times. This doesn't count to the lockout policy because of smart lock out .

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout>

upvoted 8 times

🗨️ 👤 **TP447** 1 year, 1 month ago

Totally agree here.



upvoted 1 times

🗨️ 👤 **SandyBridge** 1 year, 3 months 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** 1 year, 1 month ago

Totally agree here.

upvoted 2 times

  **amurp35** 1 year, 3 months 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** 1 year, 3 months ago

1 Box Correct T4il\$pin45dg4

The 2nd Box is incorrect it should be lockout

upvoted 2 times

  **mikl** 7 months, 3 weeks ago

Agree my friend!

upvoted 1 times

  **nsotis28** 1 year, 4 months ago

Box 1 - only T4il\$pin45dg4

Box 2 - will be locked

upvoted 2 times

  **hogegehohoge** 1 year, 4 months ago

Box1:Only F@lcon and T4il\$pin45dg4.

Because "a" is replaced "@", and match this policy.

upvoted 2 times

  **Romke_en_Tomke** 1 year, 3 months 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 4 times

  **mikl** 7 months, 3 weeks ago

Thank you for clarifying this :)

upvoted 1 times

  **Vaati** 1 year, 4 months ago

If you fail again after a lockout periode, you are locked again no?

upvoted 2 times

  **spectre786** 1 year, 3 months 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

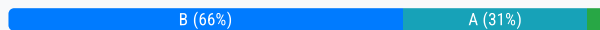
You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the internet is lost.

Which users should you identify?

- A. none
- B. User1 only
- C. User1 and User2 only
- D. User1, User2, and User3

Suggested Answer: D

Community vote distribution



certma2023 Highly Voted 1 year, 4 months ago

Selected Answer: A

I would choose A.

According to the MS documentation:

"Does password hash synchronization act as a fallback to Pass-through Authentication?"

No. Pass-through Authentication does not automatically failover to password hash synchronization. To avoid user sign-in failures, you should configure Pass-through Authentication for high availability."

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-faq#does-password-hash-synchronization-act-as-a-fallback-to-pass-through-authentication->

Therefore, without any admin actions, authentication won't be possible for any user until the admin make some changes on the tenant.

upvoted 8 times

amurp35 1 year, 3 months ago

Correct, except for cloud-only users. Therefore, the correct answer is B.

upvoted 11 times

miki 7 months, 3 weeks ago

But how come user 2 can't sign in?

Passwords are hashed in the Cloud for user 2 - so should be able to logon no?

upvoted 2 times

FiRem00 3 weeks, 1 day ago

No, even though it serves as a backup, PHS would need to be changed in the backend by Microsoft in order for User2 or User3 to login that way. It's not an automatic thing, nor can it be changed by a customer

upvoted 1 times

amurp35 Highly Voted 1 year, 3 months ago

Selected Answer: B

B. Cloud user won't be affected. Why? Because Pass-through auth is ON for the on-prem sourced 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 6 times

MR_Eliot **Most Recent** 3 months, 1 week ago

Selected Answer: B

B is true. PTA doesn't fallback automatically to Password Hash. Since user1 is a cloud only user, user 1 will still be able to login.

upvoted 2 times

APK1 4 months, 3 weeks ago

Selected Answer: B

My selection is B

User 1 only. Direct authentication requires the local network to be available.

upvoted 1 times

blairkimo 5 months, 3 weeks ago

Selected Answer: D

The users have been synched then connection to on prem was lost . So you cant log in to on prem but can you log in to the cloud . The question asks "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?"

So yes you will be able to log in to azure and seeing the creds for all three users have been synched previously then I would choose D

upvoted 2 times

angra01 7 months, 3 weeks ago

Selected Answer: B

Lost connection

upvoted 1 times

MarcMouelle 8 months, 3 weeks ago

Selected Answer: B

L'utilisateur 1 uniquement. L'authentification directe nécessite que le réseau local soit disponible or le hachage dee mot de passe crypte les mots de passes et les stocke dans l' entra id

upvoted 1 times

nordbymikael 9 months, 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 3 times

Tomtom11 10 months, 2 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn>

upvoted 1 times

Tomtom11 10 months, 2 weeks ago

https://www.reddit.com/r/Office365/comments/zqmfo/passthrough_authentication_and_password_hash/

upvoted 1 times

TP447 1 year, 1 month 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 1 year, 1 month 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 1 year, 2 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

  **AMDf** 1 year, 3 months ago



Selected Answer: B

Vote for B
upvoted 3 times

  **ae88d96** 1 year, 3 months ago

Selected Answer: B

Correct Answer B, Cloud User won't be affected. Tested on my lab.
upvoted 4 times

  **Carine** 1 year, 4 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** 1 year, 4 months ago

it Should be A
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

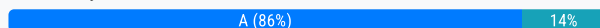
You need to recommend a solution to ensure that the logon hour restrictions apply when synced users sign in to Azure AD.

What should you include in the recommendation?

- A. pass-through authentication
- B. conditional access policies
- C. password synchronization
- D. Azure AD Identity Protection policies

Suggested Answer: A

Community vote distribution



Casticod Highly Voted 1 year, 4 months ago

Selected Answer: A

This requirement can be achieved only if you have Pass through Authentication configured as a sign in option with Azure AD and with Logon hours setting configured in on-premise AD.

Other solution it's PIM but not valid in that question

upvoted 14 times

APK1 Most Recent 4 months, 3 weeks ago

Selected Answer: A

PTA

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

nordbymikael 9 months, 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 3 times

TonyManero 1 year, 2 months 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 2 times

Alscoran 1 year, 2 months 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 1 year, 3 months 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 3 times

  **Lovell88** 1 year, 2 months ago



There is no time condition in CA. This isn't correct. Don't trust this answer.

upvoted 3 times

  **ATHOOS** 1 year, 1 month ago


Nonsense response ...

upvoted 2 times

  **Perycles** 11 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** 1 year, 4 months ago

Conditional access policies. From ChatGPT

You should recommend using conditional access policies in Azure AD to enforce logon hour restrictions for synced users. Conditional access policies allow you to define access rules based on various conditions, including time of day. By creating a conditional access policy that requires users to sign in during business hours, you can ensure that logon hour restrictions are enforced for synced users in Azure AD.

upvoted 2 times

  **RJTW070** 1 year, 3 months 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** 1 year, 4 months ago

I was wrong given answer is correct

upvoted 1 times

  **Greatone1** 1 year, 4 months ago

I believe answer is b conditional access

upvoted 2 times

Your network contains three Active Directory forests. There are forests trust relationships between the forests.

You create an Azure AD tenant.

You plan to sync the on-premises Active Directory to Azure AD.

You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails.

What should you include in the recommendation?

- A. one Azure AD Connect sync server and one Azure AD Connect sync server in staging mode
- B. three Azure AD Connect sync servers and one Azure AD Connect sync server in staging mode
- C. six Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode
- D. three Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

Suggested Answer: A

Community vote distribution

A (100%)

 **nsotis28** Highly Voted 1 year, 4 months 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 5 times

 **arielreyes2712** Most Recent 4 months, 1 week ago

Selected Answer: A

Only one Azure AD connect instance can run as active. On the other hand, you can have many staging mode server configured.

upvoted 1 times

 **nordbymikael** 9 months, 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 4 times

 **Shuihe** 1 year, 1 month 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 2 times

You have a Microsoft 365 subscription.

You have the retention policies shown in the following table.

Name	Location	Retain items for a specific period	Start the retention period based on	At the end of the retention period
Policy1	SharePoint sites	1 years	When items were created	Delete items automatically
Policy2	SharePoint sites	2 years	When items were last modified	Do nothing

Both policies are applied to a Microsoft SharePoint site named Site1 that contains a file named File1.docx.

File1.docx was created on January 1, 2022 and last modified on January 31, 2022. The file was NOT modified again.

When will File1.docx be deleted automatically?


- A. January 1, 2023
- B. January 1, 2024
- C. January 31, 2023
- D. January 31, 2024
- E. never

Suggested Answer: D

Community vote distribution

D (83%)

E (18%)

 **amurp35** Highly Voted 1 year, 3 months ago

Selected Answer: D

D is correct. Source: <https://learn.microsoft.com/en-us/purview/retention?tabs=table-override#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 18 times

 **gbartumeu** Highly Voted 1 year, 3 months 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.

Source: <https://learn.microsoft.com/en-us/purview/retention?tabs=table-removed>

upvoted 7 times

 **norbe01** Most Recent 3 months, 2 weeks ago

Selected Answer: E



Since Policy2 retains the file for 2 years from the last modified date and does nothing at the end, this policy ensures that the file remains in place for at least 2 years.

Policy1, which requires deletion after 1 year, is overridden by Policy2 because retention (Policy2) is a more conservative action compared to deletion.

Therefore, Policy2 has priority because it retains the file for a longer period, and retention always wins over deletion.

Correct answer: E. Never.

upvoted 2 times

  **Big076** 1 month, 3 weeks ago

In this scenario: Policy1 retains items for 1 year and deletes them afterward. Policy2 retains items for 2 years without deleting them.

Since Policy2 has the longest retention period, File1.docx will be retained for 2 years (until January 31, 2024) and won't be deleted at the end of that period because Policy2 specifies "Do nothing."

If there are multiple retention policies applied to the same content, the policy with the longest retention period will take precedence, even if another policy specifies deletion at the end of its retention period. When two retention policies conflict, Azure will respect the one that has the longest retention duration. The file will never be automatically deleted due to the longer retention period in Policy2 and its "Do nothing" instruction at the end. So has to be E.

upvoted 1 times

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

Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

You plan to publish a sensitivity label named Label1.

To which groups can you publish Label1?

- A. Group1 only
- B. Group1 and Group2 only
- C. Group1 and Group4 only
- D. Group1, Group2, and Group3 only
- E. Group1, Group2, Group3, and Group4

Suggested Answer: A

Community vote distribution

D (87%)

9%

 **amurp35** Highly Voted 1 year, 3 months 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 19 times

 **sergioandreslq** 1 year, 2 months 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 4 times

 **odeo4all** Most Recent 3 months, 2 weeks ago

Answer is 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 1 times

 **NedaSim** 4 months, 1 week 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 1 times

 **9711d59** 11 months, 2 weeks ago

Selected Answer: D

This is good answer. I have tested it

upvoted 2 times

 **cpaljchc4** 1 year 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** 1 year 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 2 times

  **mhmyz** 1 year, 3 months 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** 1 year, 2 months 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** 1 year, 3 months 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 groups¹. 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 labels¹.

upvoted 2 times



  **rfree** 1 year, 3 months 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

The "Group writeback state" oddly includes options Security, Mail Enabled Security and Distribution.

upvoted 1 times

  **spectre786** 1 year, 4 months 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** 1 year, 4 months ago

(A) it is Correct only applied into the Email

upvoted 1 times

  **sergioandreslq** 1 year, 2 months 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** 1 year, 4 months ago

Correct

upvoted 1 times

  **Greatone1** 1 year, 4 months ago

Correct answer is D

upvoted 1 times

  **certma2023** 1 year, 4 months ago

Answer D.

According to the documentation:

"Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD."

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

upvoted 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

File1.docx:

- Rule1 tip only
- Rule2 tip only
- Rule3 tip only
- Rule1 tip and Rule2 tip only
- Rule1 tip, Rule2 tip, and Rule3 tip

Suggested Answer:


File2.docx:

- Rule1 tip only
- Rule3 tip only
- Rule4 tip only
- Rule1 tip and Rule4 tip only
- Rule1 tip, Rule3 tip, and Rule4 tip

 **hogehogehoge** Highly Voted 1 year, 4 months 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 52 times

 **blairskimo** 5 months, 3 weeks ago
This is correct . I looked at the doc

"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 I dont know how they rule 1 for both
upvoted 2 times

 **martinods** 7 months ago
why not File1.docx:rule3 only. rule 3 is most restrictive than rule 2, no ?
upvoted 2 times

 **blairskimo** 5 months, 3 weeks ago
rule 3 enables user over rides while rule 2 disables them there for more restrictive .
upvoted 1 times


 **Frank9020** Most Recent 1 month, 3 weeks ago
File1.docx is Rule 2
File2.docx is Rule 4
upvoted 2 times

 **APK1** 4 months, 1 week ago

Same question in the MS practice lab.


Rule 1 for both, when multiple rules matches, the rule with the higher priority is enabled.

upvoted 3 times

 **f09257a** 10 months, 2 weeks ago

Rule 1 for both, when multiple rules matches, the rule with the higher priority is enabled.

upvoted 4 times

 **9711d59** 11 months, 2 weeks 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 3 times

 **KairKnows** 1 year 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

 **NrdAlrt** 1 year, 1 month 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 actions are the same in terms of restrictions. File 1 : Rule 2 only, File 2 : Rule 4 only

upvoted 1 times

 **rfree** 1 year, 2 months ago

Correction, Rule 2 then Rule 4 as each is the Most Restrictive.

upvoted 1 times


 **rfree** 1 year, 2 months 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** 1 year, 3 months ago

As its not asking which rules are applied, but which rules are Shown.

upvoted 1 times

 **rfree** 1 year, 3 months 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** 1 year, 3 months ago

Agree with hoge

upvoted 1 times

 **letters1234** 1 year, 4 months ago

Agree with Hoge, specific reference in the doc:

<https://learn.microsoft.com/en-us/purview/dlp-policy-reference#the-priority-by-which-rules-are-evaluated-and-applied>

upvoted 4 times

 **Greatone1** 1 year, 4 months ago

Rule 1 Tip Only" for both

upvoted 3 times

You have a Microsoft 365 subscription.

You configure a data loss prevention (DLP) policy.

You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.

You need to prevent the users from bypassing the DLP policy.

What should you configure?

- A. actions
- B. incident reports
- C. exceptions
- D. user overrides

Suggested Answer: D

Community vote distribution

D (100%)

 **Greatone1** Highly Voted 10 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 10 times

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

Selected Answer: D

To prevent users from bypassing the DLP policy after incorrectly marking content as a false positive, you should configure user overrides. This option allows you to control whether users can override a DLP policy and under what circumstances they can report a false positive. By adjusting the settings for user overrides, you can ensure that sensitive information is properly protected according to your organization's policies and compliance requirements.

upvoted 1 times

 **TheMCT** 5 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?

- A. Create a new label policy.
- B. Modify the Authority type setting for Retention1.
- C. Modify the Business function/department setting for Retention1.
- D. Use a file plan CSV template to import Retention1.

Suggested Answer: A

Community vote distribution

A (100%)

ZZNZ Highly Voted 1 year, 3 months ago

Selected Answer: A

wrong image : <https://www.examttopics.com/discussions/microsoft/view/65184-exam-ms-101-topic-3-question-105-discussion/>
upvoted 11 times

mikl 7 months, 3 weeks ago

But why is the solution here to create a new label policy?
upvoted 1 times

Frank9020 Most Recent 1 month, 2 weeks ago

Selected Answer: A

To ensure that the Retention1 label is available to all users, you should A. Create a new label policy. This will allow you to publish the label to the necessary users and locations, making it accessible for them to apply as needed.
upvoted 1 times

APK1 4 months, 3 weeks ago

Admin please change the image.

correct one is below

<https://www.examttopics.com/discussions/microsoft/view/65184-exam-ms-101-topic-3-question-105-discussion/>
upvoted 1 times

🗨️ 👤 **spectre786** 1 year, 3 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** 1 year, 4 months 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** 1 year, 4 months ago

Selected Answer: A

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide>

upvoted 1 times

You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels Label policies Auto-labeling (preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ 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

Suggested Answer: D

Community vote distribution

C (100%)

amurp35 Highly Voted 9 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 17 times

sergioandreslq 8 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

hogegehoge Highly Voted 10 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

miki Most Recent 1 month, 3 weeks ago

Selected Answer: C

C. Label1, Label3, Label4, and Label6 only
upvoted 1 times

dvmhike 1 month, 3 weeks ago

Answer: D

Explanation:

Sublabels are simply a way to present labels to users in logical groups. Sublabels don't inherit any settings from their parent label. When you publish a sublabel for a user, that user can then apply that sublabel to content but can't apply just the parent label.

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365->

worldwide

upvoted 1 times

🗨️ **nordbymikael** 3 months, 1 week ago

Selected Answer: C

Parent labels cannot be applied if they have child labels

upvoted 2 times

🗨️ **Tomtom11** 4 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 their 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 2 times

🗨️ **cyp99** 6 months, 4 weeks ago

Selected Answer: C

Agree with amurp35. Parent labels cannot be used by user

upvoted 2 times

🗨️ **letters1234** 10 months, 1 week ago

Selected Answer: C

<https://learn.microsoft.com/en-us/purview/sensitivity-labels#sublabels-grouping-labels>

upvoted 5 times

🗨️ **gomezmax** 10 months, 1 week ago

Should be C. Label1, Label3, Label4, and Label6 only

upvoted 3 times

🗨️ **f7d3be6** 10 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** 10 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

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

Suggested Answer:

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

northgaterebel Highly Voted 1 year, 2 months ago

Office 2016 and Office 2019 only

.doc, .docx, .xls, and .xlsx

upvoted 15 times

ShlomiR 1 year, 2 months ago

<https://learn.microsoft.com/en-us/purview/sensitivity-labels-office-apps#office-file-types-supported>

second answer only docx and xlsx,

upvoted 25 times

🗨️ 👤 **Big076** 1 month, 3 weeks ago

also Office 2016: Requires an add-in to enable sensitivity labels because native support for these labels was only introduced in later versions. Office 2019 and Microsoft 365 Apps for Enterprise: These versions have native support for sensitivity labels without the need for an add-in. Microsoft introduced built-in sensitivity labeling for Office apps starting with Office 2019, which continued in Microsoft 365 Apps. Office for the web: Also supports sensitivity labels natively without requiring an add-in.

upvoted 1 times

🗨️ 👤 **miki** 7 months, 3 weeks ago

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 1 times

🗨️ 👤 **daye** 1 year, 1 month 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 👍 1 year, 4 months ago

365 versions of Office (365 Apps) have it built in. Meaning only the 2016/2019 currently require the AIP UL add-in (which is being deprecated soon).

<https://techcommunity.microsoft.com/t5/security-compliance-and-identity/sensitivity-labeling-now-built-into-office-apps-for-windows-to/ba-p/844506>

<https://learn.microsoft.com/en-us/purview/sensitivity-labels-office-apps#labeling-client-for-desktop-apps>

Office 2016 is out of mainstream support (meaning no new features/functions added) and wouldn't expect them to develop the integrated label handling since it's in security patching only mode.

<https://learn.microsoft.com/en-us/lifecycle/products/microsoft-office-2016>

Would go with 2016 & 2019, however not sure how much longer this question will be around considering the add-in is being deprecated.

upvoted 10 times

🗨️ 👤 **RJTW070** 1 year, 3 months 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** 1 year, 3 months ago

So I will go for Office 2016 and 2019 the second answer is correct

upvoted 5 times

🗨️ 👤 **Milad666** 1 year, 2 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** 1 year, 1 month 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 2 times

🗨️ **tome** 1 year, 1 month ago

*is correct, sry!

upvoted 1 times

🗨️ **MR_Eliot** Most Recent 3 months, 1 week ago

Supported file types for Office apps on Windows, macOS, iOS, and Android:

Word: .docx, .docm, .dotx, .dotm

Excel: .xlsx, .xlsb, .xlsm, .xltx

PowerPoint: .pptx, .pptm, .potx, .potm, .ppsx, .ppsm

upvoted 1 times

🗨️ **MR_Eliot** 3 months, 1 week ago

Sensitivity labeling support in apps

To use sensitivity labels in Office apps, you must use a subscription edition of Office. Use the licensing link at the top of this page to identify eligible plans. Sensitivity labels aren't supported for standalone editions of Office, sometimes called "Office Perpetual".

upvoted 1 times

🗨️ **LakesWizard** 4 months ago

This is an old question because Office 2019 and Office 2016 no longer supports sensitivity labels

upvoted 2 times

🗨️ **APK1** 4 months, 3 weeks ago

This question must be obsolete, there is already office version 2021 and 2024 is due for Oct2024.

Any way the answer to the question

1) Office 2016 and Office 2019 only

2) .docx, and .xlsx

upvoted 4 times

🗨️ **Tomtom11** 10 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** 1 year, 4 months ago

Given answer is correct.

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)

Create retention label

You create a label policy as shown in the Label Policy exhibit. (Click the Label Policy tab.)

Auto-labeling > Create auto-labeling policy

The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input type="radio"/>
Any sent email message that contains the word ProjectX will be retained for six months.	<input type="radio"/>	<input type="radio"/>
Users are required to manually apply a label to email messages that contain the word ProjectX.	<input type="radio"/>	<input type="radio"/>

Suggested Answer:

Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input checked="" type="radio"/>
Any sent email message that contains the word ProjectX will be retained for six months.	<input checked="" type="radio"/>	<input type="radio"/>
Users are required to manually apply a label to email messages that contain the word ProjectX.	<input type="radio"/>	<input checked="" type="radio"/>

spectre786 Highly Voted 1 year, 3 months ago
Should be N/Y/N
upvoted 23 times

momowagdy 8 months, 3 weeks ago
It is actually N, Y, N
Maybe they have updated the answer
upvoted 5 times

Crille Most Recent 1 month, 3 weeks ago
Second one it says based on created
upvoted 1 times

Murad01 6 months, 1 week ago
Given Answer is correct !
upvoted 1 times

nordbymikael 9 months, 1 week ago
1: No
2: Yes
3: No
upvoted 2 times

You have a Microsoft 365 subscription.

Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de-fghij.

You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs.

What should you create to ensure that the DLP policy can detect the customer IDs?

- A. a PowerShell script
- B. a sensitivity label
- C. a sensitive information type
- D. a retention label

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ **sherifhamed** Highly Voted 1 year, 3 months 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 11 times

🗨️ **FredC** Most Recent 2 months, 3 weeks ago

why not sensitivity label?

upvoted 1 times

🗨️ **Tomtom11** 10 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** 1 year, 3 months ago

Yes correct 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?

upvoted 1 times

🗨️ **Greatone1** 1 year, 4 months 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

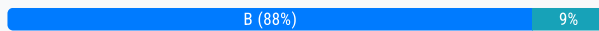
You need to prevent the removal of the label once the label is applied to a file.

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

Suggested Answer: A

Community vote distribution



gbartumeu Highly Voted 1 year, 3 months 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 is applied then should be "Regulatory Record".

upvoted 15 times

2651b14 Most Recent 2 months, 2 weeks ago

i think B

upvoted 1 times

jarattdavis 4 months, 3 weeks ago

Selected Answer: C

"Mark items as a regulatory record," is used for stricter compliance requirements but isn't necessary for simply preventing label removal.

upvoted 3 times

Jol 2 days, 23 hours ago

I agree. Regulatory record seems to be an over-kill. According to AI Overview:

"In Microsoft 365, the main difference between a record and a legal record is the level of control that admins have over the label:

Record

Users can't edit or delete items, and only admins can change or remove the label.

Legal record

Users can't edit or delete items, and admins can't change or remove the label. Admins can only increase the retention period or publish the label to other locations."

upvoted 1 times

Nuance 6 months, 2 weeks ago

Selected Answer: A

B is incorrect because you can only apply that setting via powershell

upvoted 2 times

Motanel 8 months, 3 weeks ago

I am starting to believe that these provided answers are simply aleatory without checking any if it's correct or not.

upvoted 2 times

🗨️ **nordbymikael** 9 months, 1 week ago

Selected Answer: B

A regulatory record can never be deleted
upvoted 3 times

🗨️ **Tomtom11** 10 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** 1 year, 2 months ago

<https://learn.microsoft.com/en-us/purview/records-management#compare-restrictions-for-what-actions-are-allowed-or-blocked>

upvoted 1 times

🗨️ **jt2214** 1 year, 3 months ago

Selected Answer: B

B all the way

upvoted 2 times

🗨️ **Jslei** 1 year, 3 months 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** 1 year, 4 months 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** 1 year, 4 months ago

Selected Answer: B

Sorry I meant B

upvoted 4 times

🗨️ **Greatone1** 1 year, 4 months ago

Selected Answer: A

Correct answer is A

<https://www.examttopics.com/discussions/microsoft/view/80391-exam-ms-101-topic-3-question-121-discussion/>

upvoted 1 times

🗨️ **Khanbaba43** 4 months, 2 weeks ago

You've chosen correct answer "A" from the exam MS-101 you've referenced.

Here the same answer (from MS-101) is listed under option B lol.

Answer B for me!

upvoted 3 times

  **manschadow** 1 month, 2 weeks ago

It shows the effort he is willing to take for the community.

Zero to be honest.

Like you mentioned. Answer "A" in that link is "B" here.

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
🗑️

Any of these ▾ 🗑️

Sensitive info types

Credit Card Number High confidence ⓘ instance count to Any ⓘ 🗑️

Retention labels

RetentionLabel1 🗑️

Add ▾

[🔗 Create group](#)

+ Add condition ▾

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

Suggested 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

🗨️ **hogegehoge** Highly Voted 1 year, 4 months ago

Box1:Exchange email. I tested this configuration in my lab.

Box2:ether a credit card number or the Retention label1 label applied.

upvoted 43 times

🗨️ **Hamouda1** 1 month, 1 week ago

Agree with hogegehoge

upvoted 1 times

🗨️ **sergioandreslq** 1 year, 2 months 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 3 times

🗨️ **daye** 1 year, 1 month 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**  1 year, 4 months ago

Box1: Correct the policy cannot be applied to Exchange

Box2: either a credit card number or the Retention label1 label will be applied

upvoted 12 times

  **Tomtom11**  4 months, 3 weeks ago

You cannot select Exchange online with a Retention label Box 1 correct

upvoted 1 times

  **Shadowcatest** 1 year, 2 months 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** 1 year, 4 months 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

Suggested Answer: B

Community vote distribution

B (100%)

Greatone1 Highly Voted 10 months 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 8 times

miki Most Recent 1 month, 3 weeks ago

Selected Answer: B

No brainer here.

Answer is B - this is not an issue that would be solved by : Allow logon locally user right.



upvoted 1 times

nordbymikael 3 months, 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

  **Greatone1** 10 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

Suggested Answer: B

Community vote distribution

B (100%)


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

Selected Answer: B

B. No

Assigning SecAdmin1 the SharePoint Administrator role does not meet the goal of ensuring that they can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive. The SharePoint Administrator role primarily provides permissions to manage SharePoint and does not include permissions for managing security policies across Microsoft 365 services.

upvoted 5 times

 **nordbymikael** Most Recent 3 months, 1 week ago

Selected Answer: B

Does not meet all the requirements.

upvoted 3 times

 **60ed5c2** 8 months 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 2 times

 **NrdAlrt** 7 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 2 times

 **Shadowcatest** 8 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** 9 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

Suggested Answer: A

Community vote distribution

A (85%)

B (15%)

 **aleksdj** Highly Voted 7 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 24 times

 **tzzz1986** Highly Voted 9 months, 2 weeks ago

Selected Answer: B

Security administrator role does not seem to have access in Teams, Sharepoint. Reference: <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator>

upvoted 9 times

 **Alscoran** 8 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 8 times

 **sergioandreslq** 8 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

 **sergioandreslq** 7 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

🗨️ **[Removed]** 8 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

🗨️ **miki** Most Recent 1 month, 3 weeks ago

Selected Answer: A

A. Yes

Assigning SecAdmin1 the Security Administrator role from the Microsoft Entra admin center does meet the goal. The Security Administrator role includes permissions to manage security policies and settings across Microsoft 365 services, which would cover Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

upvoted 1 times

🗨️ **nordbymikael** 3 months, 1 week ago

Selected Answer: A

I believe that A is the right answer. The question is spelled a bit wrong.

upvoted 3 times

🗨️ **TheMCT** 5 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** 7 months ago

Selected Answer: A

Answer A is correct

upvoted 3 times

🗨️ **Memdroid** 7 months ago

Selected Answer: A

A is correct

upvoted 2 times

🗨️ **2dwarf** 7 months, 1 week ago

Selected Answer: A

A Can manage policies

upvoted 2 times

🗨️ **ckanoz** 7 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 questions is asking if the role can make Security policies FOR, Teams, Sharepoint or Exchange.

upvoted 2 times

🗨️ **TP447** 7 months, 3 weeks ago

This is correct - the question isnt 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

🗨️ **NrdAirt** 7 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

🗨️ 👤 **NrdAirt** 7 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

🗨️ 👤 **TP447** 7 months, 3 weeks ago

I agree here.

upvoted 1 times

🗨️ 👤 **60ed5c2** 8 months 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** 8 months, 2 weeks ago

Selected Answer: A

For me it's A

upvoted 2 times

🗨️ 👤 **PhoenixMan** 8 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** 8 months, 3 weeks ago

Selected Answer: A

I agree with Darekmso based on

<https://www.examttopics.com/discussions/microsoft/view/76446-exam-ms-101-topic-2-question-50-discussion/>

upvoted 3 times

🗨️ 👤 **Darekmso** 8 months, 3 weeks ago

Selected Answer: A

<https://www.examttopics.com/discussions/microsoft/view/76446-exam-ms-101-topic-2-question-50-discussion/>

upvoted 2 times

🗨️ 👤 **Paul_white** 9 months ago

ANSWER FOR ME IS A

upvoted 2 times

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

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

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

Suggested Answer: B

Community vote distribution

B (100%)

  **mikl** 1 month, 3 weeks ago

Selected Answer: B

B. No

Assigning SecAdmin1 the Exchange Administrator role from the Microsoft 365 admin center does not fully meet the goal. While the Exchange Administrator role provides some permissions related to email security in Microsoft Defender for Office 365, it does not grant comprehensive management capabilities for settings and policies across Microsoft Teams, SharePoint, and OneDrive.



upvoted 1 times

  **nordbymikael** 3 months, 1 week ago

Selected Answer: B

Does not meet all the requirements.

upvoted 2 times

  **DiligentSam** 9 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:

Briefing email
Help desk information
Organization information

To limit access:

Privileged Access
Release preferences
Office installation options

Answer Area

Suggested Answer:

To configure the notifications:

Briefing email
Help desk information
Organization information

To limit access:

Privileged Access
Release preferences
Office installation options

 **Casticod** Highly Voted 1 year, 3 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.examttopics.com/discussions/microsoft/view/81376-exam-ms-100-topic-8-question-1-discussion/>
upvoted 21 times

 **lali11** 12 months ago

Shouldn't this be helpdesk information?
upvoted 1 times


 **lali11** 12 months ago

pls ignore.
upvoted 1 times


 **APK1** Most Recent 4 months, 3 weeks ago

My selections are

1. Organization information
 2. Release preferences
- upvoted 1 times

 **Tomtom11** 4 months, 3 weeks ago

Release preferences is correct. Just checked in admin portal = Choose how your organization gets new features and service updates from Microsoft 365.
upvoted 1 times

 **Tomtom11** 4 months, 3 weeks ago

First Answer should be Organization information. I Just check it on the admin portal
upvoted 1 times

 **lali11** 12 months ago

1st answer: Organization information
<https://o365info.com/help-desk-information-microsoft-365/>
upvoted 2 times

 **NrdAlrt** 1 year, 1 month 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

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.

Suggested Answer: C

Community vote distribution

C (100%)

 **Casticod** Highly Voted 1 year, 3 months ago

Selected Answer: C

Correct <https://www.examttopics.com/discussions/microsoft/view/89165-exam-ms-100-topic-13-question-2-discussion/>
upvoted 6 times

 **APK1** Most Recent 4 months, 3 weeks ago

Selected Answer: C

C is the correct answer
upvoted 1 times

 **blairkimo** 5 months, 3 weeks ago

I actually got this one correct . There is hope for me . I see MS Blathers on with a bunch of nonsense and eventually you get the question whis a one liner .

upvoted 2 times

  **miki** 7 months, 3 weeks ago

Selected Answer: C

To configure Azure AD Connect to sync specific organizational units (OUs) like the Montreal Users OU and the Seattle Users OU, you should:

C. From the Microsoft Azure AD Connect wizard, select Customize synchronization options.

This option allows you to specify which OUs you want to synchronize with Azure AD. You can use it to ensure that only the Montreal Users OU and the Seattle Users OU are included in the synchronization process. Remember to review and confirm the changes to ensure that the synchronization settings are correctly applied to meet your planned changes.

upvoted 2 times

  **nordbymikael** 9 months, 1 week ago

Selected Answer: C

C should be correct, because there you can enable OU filtering.

upvoted 4 times

Overview -

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

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

Existing Environment -

Active Directory Environment -

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

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

Fabrikam does NOT plan to implement identity federation.

Network Infrastructure -

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

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

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

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

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

Requirements -

Planned Changes -

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

Fabrikam plans to implement two pilot projects:

- Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
- Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.

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

Technical Requirements -

Fabrikam identifies the following technical requirements:

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

- Users must be able to authenticate to cloud services if Active Directory becomes unavailable.
- A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.
- Microsoft 365 Apps for enterprise applications must be installed from a network share only.
- Disruptions to email access must be minimized.

Application Requirements -

Fabrikam identifies the following application requirements:

- An on-premises web application named App1 must allow users to complete their expense reports online. App1 must be available to users from the My Apps portal.
- The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.

Security Requirements -

Fabrikam identifies the following security requirements:

- After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
- The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.
- After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
- The principle of least privilege must be used.

You are evaluating the required processes for Project1.

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


Which DNS record should you recommend?

- A. host (A)
- B. alias (CNAME)
- C. text (TXT)
- D. host (AAAA)

Suggested Answer: B

Community vote distribution

C (100%)

 **Casticod** Highly Voted 1 year, 3 months ago

Selected Answer: C

Not necessary Cname record to add Email Only TXT o MX Record are Valid. Correct C <https://learn.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide#step-1-add-a-txt-or-mx-record-to-verify-you-own-the-domain>
upvoted 14 times

 **blairskimo** Most Recent 5 months, 3 weeks ago

Ok every one agrees with me . I am not crazy . Its .TXT
upvoted 1 times

 **mikl** 7 months, 3 weeks ago

Selected Answer: C



Copilot says :

For Project1, when adding a domain name to Microsoft 365, the DNS record you need to create is:

C. text (TXT)

This is because during the initial domain setup in Microsoft 365, you are required to add a TXT record to verify that you own the domain. This TXT record does not affect your existing services and can be removed once the domain is verified and connected to Microsoft 365. After verification, other DNS records will be needed to connect services like email, but the TXT record is the first step for domain verification.

upvoted 1 times

  **Motanel** 8 months, 3 weeks ago

Selected Answer: C

Obviously C.

upvoted 1 times

  **nordbymikael** 9 months, 1 week ago

Selected Answer: C

TXT is the required DNS record for domain ownership validation.


upvoted 3 times

  **spektrum1988** 11 months, 1 week ago

Selected Answer: C

TXT is correct



upvoted 3 times

  **cyp99** 1 year ago

Selected Answer: C

TXT or MX for domain add/validation

upvoted 3 times

  **passy951** 1 year ago

Selected Answer: C

CNAME is for Autodiscover

upvoted 4 times



  **EEMS700** 1 year, 2 months ago

Selected Answer: C

You can add a domain only with TXT or MX.

So it's C

upvoted 4 times

  **AMDf** 1 year, 3 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

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ **mikl** 1 month, 3 weeks ago

Selected Answer: B

B. No

Security Administrator is required

upvoted 1 times

🗨️ **nordbymikael** 3 months, 1 week ago

Selected Answer: B

Security Administrator is required.

upvoted 4 times

🗨️ **TonyManero** 6 months ago

Selected Answer: B

Needs Security Admin Role

upvoted 2 times

🗨️ **daye** 7 months, 1 week ago

Selected Answer: B

Similar questions asking about assigning Teams, Sharepoint or Exchange admin. Always NO. It should be Security Admin since it will be used within 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:

- Azure AD only
- On-premises Active Directory only
- On-premises Active Directory or Azure AD

User20:

- Azure AD only
- On-premises Active Directory only
- On-premises Active Directory or Azure AD


Suggested Answer:

User10:

- Azure AD only
- On-premises Active Directory only
- On-premises Active Directory or Azure AD

User20:

- Azure AD only
- On-premises Active Directory only
- On-premises Active Directory or Azure AD

 **Greatone1** Highly Voted 1 year, 2 months ago

Answers are correct

<https://www.examtopycs.com/discussions/microsoft/view/49675-exam-ms-100-topic-3-question-37-discussion/>

upvoted 13 times

 **miki** Most Recent 7 months, 3 weeks ago

User10 : On Prem only

User20 : Entra ID only

upvoted 3 times

 **nordbymikael** 9 months, 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

 **Besxp** 1 month ago



Correct, but it's "without password writeback configured you cannot sync password change from on prem to Azure AD and vice versa."

upvoted 1 times

 **spektrum1988** 11 months, 1 week 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** 11 months, 1 week ago

Unfortunately, you cannot reset this user's password because password writeback is not enabled in your tenant. Correct.

upvoted 2 times

  **EEMS700** 1 year, 2 months ago

correct

upvoted 4 times

HOTSPOT

You have an Azure AD tenant that contains the groups shown in the following exhibit.

Search

Search mode Contains

5 groups found

<input type="checkbox"/>	Name	Group type	Membership type	Source	Security enabled
<input type="checkbox"/>	Group1	Microsoft 365	Assigned	Cloud	Yes
<input type="checkbox"/>	Group2	Microsoft 365	Assigned	Cloud	No
<input type="checkbox"/>	Group3	Security	Assigned	Cloud	Yes
<input type="checkbox"/>	Group4	Security	Dynamic	Cloud	Yes
<input type="checkbox"/>	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

Suggested Answer:

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

AMDf Highly Voted 1 year, 3 months ago

- 1) Group 1, Group 2 and Group 3
 - 2) Group 3 only
- upvoted 60 times

norbe01 3 months, 2 weeks ago

Tested on LAB. Given Answer is correct. Who is saying its not able for group 2 as not security enabled they are wrong!

upvoted 1 times

🗨️ **mikl** 7 months, 3 weeks ago

You sure about Group 2 for question 1? Since security is not enabled?
upvoted 1 times

🗨️ **EEMS700** 1 year, 2 months ago

i would agree with AMDf
upvoted 1 times

🗨️ **cyp99** 1 year ago

agree as G4 is dynamic and G5 synced from onprem
upvoted 2 times

🗨️ **665d390** Most Recent 3 months, 2 weeks ago

1) Group 1, Group 2 and Group 3 (Security enabled is for assign permissions to various resources like files, folders, applications, or SharePoint sites, so you can add users)

2) Group 3 only
upvoted 1 times

🗨️ **APK1** 4 months, 3 weeks ago

Given answer is correct.

You can add security group which is security enabled and membership assigned to another security group which is already security enabled and membership assigned.
upvoted 1 times

🗨️ **Tomtom11** 4 months, 3 weeks ago

<https://learn.microsoft.com/it-it/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>
upvoted 1 times

🗨️ **KakTak** 6 months, 1 week ago

Answers are:

1) Group 1 group 2 and group 3 -- you can add users to security enabled m365 group.

2) Group 3 only
upvoted 2 times

🗨️ **BigTone** 1 year, 1 month 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 2 times

🗨️ **Festus365** 1 year, 1 month 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** 1 year, 1 month ago

Group 4 is a Dynamic Group. You can not add any users or groups to it manually.
upvoted 4 times

🗨️ **Festus365** 11 months, 3 weeks ago

Answers are correct!(1)Group 1 & 3 only

(2) Group 3 only
upvoted 1 times

🗨️ **NrdAlrt** 1 year, 1 month ago

What does Group 2 not being security enabled mean though? Implications?
upvoted 3 times

🗨️ **daye** 1 year, 1 month ago

you can assign Entra roles there. This attribute can be enabled if you create the group from Entra instead of M365 admin.
upvoted 3 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.

Suggested Answer: C

Community vote distribution

B (82%)

Other

 **gbartumeu** Highly Voted 1 year, 3 months 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 14 times

 **xeni66** Highly Voted 4 months, 2 weeks ago

Selected Answer: C

Starting September 1st 2024, the Microsoft Entra ID Admin Center and the Microsoft Azure portal will no longer support license assignment through their user interfaces. To manage license assignments for users and groups, administrators must use the Microsoft 365 Admin Center. This update is designed to streamline the license management process within the Microsoft ecosystem. This change is limited to the user interface. API and PowerShell access remain unaffected.

<https://learn.microsoft.com/en-us/entra/identity/users/licensing-groups-assign>

upvoted 11 times

 **Hossam_Khorshed** Most Recent 2 weeks, 4 days ago

Selected Answer: A

In Azure Entra ID , when you select group - > license - > "Adding, removing, and reprocessing licensing assignments is only available within the M365 Admin Center. Go to M365 Admin Center"

upvoted 1 times

 **justITtopics** 1 month, 1 week ago

Selected Answer: A

The correct answer, starting September 1st 2024 is A.

<https://learn.microsoft.com/en-us/entra/identity/users/licensing-groups-assign>

A. From the Licenses page of the Microsoft 365 admin center, assign the licenses.

<https://learn.microsoft.com/en-us/entra/identity/users/licensing-admin-center>

1. Sign in to the Microsoft 365 admin center as at least a License Administrator.
2. Browse to Billing > Licenses to open a page where you can see all licenses available in your organization.
3. Under Licenses, select the license that you would like to assign.
4. In the License details section, choose Groups at the top of the page.
5. Choose + Assign licenses
6. From the + Assign licenses page search for the group that you would like to use for license assignment.
7. To complete the assignment, on the Assign license page, select Assign at the bottom of the page.

upvoted 4 times

🗨️ 👤 **Big076** 1 month, 2 weeks ago

Selected Answer: A

as of testing this 18th November its now A.
upvoted 3 times

🗨️ 👤 **Vince_MCT** 1 month, 2 weeks ago

Selected Answer: B

If you have a Microsoft 365 E5 subscription, you can use group-based licensing in Azure AD (now called Microsoft Entra ID) to automatically assign licenses to group members. By setting this up in the Microsoft Entra admin center, you can ensure that any member of a group like "Voice" will automatically receive the Microsoft 365 Business Voice add-on license. This way, license management is hands-free for everyone in the group.
upvoted 1 times

🗨️ 👤 **Frank9020** 1 month, 3 weeks ago

Selected Answer: A

Starting September 1st, the Microsoft Entra ID Admin Center and the Microsoft Azure portal will no longer support license assignment through their user interfaces. To manage license assignments for users and groups, administrators must use the Microsoft 365 Admin Center. This update is designed to streamline the license management process within the Microsoft ecosystem. This change is limited to the user interface. API and PowerShell access remain unaffected.
upvoted 5 times

🗨️ 👤 **mido3100** 1 month, 3 weeks ago

Selected Answer: A

A is the correct
upvoted 3 times

🗨️ 👤 **Hiyas** 1 month, 3 weeks ago

Selected Answer: A

Has been changed. No longer available in Entra
upvoted 2 times

🗨️ 👤 **RFULL** 3 months, 3 weeks ago

Selected Answer: A

Based off this link: <https://learn.microsoft.com/en-us/entra/identity/users/licensing-admin-center>. From the Licenses blade, adding the Voice group to this add-on License will automatically assign the license to all members.
upvoted 6 times

🗨️ 👤 **KennehBE** 3 months, 1 week ago

Correct answer is A, this has been changed.

You can assign a group to a license from the License page in the Admin Center
upvoted 2 times

🗨️ 👤 **elwa1** 3 months, 3 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/users/licensing-admin-center>
upvoted 1 times

🗨️ 👤 **APK1** 4 months, 3 weeks ago

Selected Answer: B

Here the point is "Voice add-on license automatically"
upvoted 1 times

🗨️ 👤 **mikl** 7 months, 3 weeks ago

Selected Answer: B

Copilot says :

To ensure that the members of a group named Voice are assigned a Microsoft 365 Business Voice add-on license automatically, you should:

B. From the Microsoft Entra admin center, modify the settings of the Voice group.

By modifying the settings of the Voice group in the Microsoft Entra admin center, you can set up dynamic group membership based on certain attributes or rules. This allows for automatic assignment of licenses to all members of the group, including any new members who meet the criteria in the future.

upvoted 1 times

🗨️ 👤 **Fran22** 10 months ago

I just checked. You can apply License to group from the License blade in Ms.365 Admin Center
upvoted 1 times

🗨️ 👤 **9711d59** 11 months, 1 week ago

Selected Answer: A

You can apply License to group with License blade in Admin 365
upvoted 3 times

🗨️ 👤 **Motanel** 8 months, 3 weeks ago

yes, but it's not done automatically. You need to manually add the groups.

upvoted 1 times

🗨️ 👤 **elwa1** 3 months, 3 weeks ago

Yeah, but after you manually add the group, the members of the group will be assigned the license automatically through their group membership

upvoted 1 times

🗨️ 👤 **PhoenixMan** 1 year, 1 month ago

In today exam

upvoted 2 times

🗨️ 👤 **EEMS700** 1 year, 2 months ago

Selected Answer: B

Only B

upvoted 2 times

You have a Microsoft 365 E5 subscription that uses Endpoint security.

You need to create a group and assign the Endpoint Security Manager role to the group.

Which type of group can you use?

- A. Microsoft 365 only
- B. security only
- C. mail-enabled security and security only
- D. mail-enabled security, Microsoft 365, and security only
- E. distribution, mail-enabled security, Microsoft 365, and security

Suggested Answer: D

Community vote distribution

D (81%)

B (19%)


 **cb0900** Highly Voted 1 year, 3 months 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 20 times

 **daye** 1 year, 1 month ago

tricky question because based on this article you need to use a security group, but indeed you can select a M356 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** 1 year, 1 month ago

So I will use B because you need to apply the role successfully


upvoted 1 times

 **Darekms0** Highly Voted 1 year, 2 months 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 9 times

 **rass1981** 11 months, 3 weeks ago

I did the same and can confirm all options in D can be chosen.

upvoted 2 times

 **Frank9020** Most Recent 1 month, 3 weeks ago

Selected Answer: C


Microsoft 365 groups cannot be used for role assignments, so including them in this answer is incorrect.

upvoted 1 times

 **Frank9020** 1 month, 3 weeks ago

Microsoft 365 groups are designed primarily for collaboration within Microsoft 365 apps, like Teams, SharePoint, and Outlook, rather than for security or administrative role assignments.

upvoted 1 times

 **justITtopics** 2 months, 4 weeks ago

Selected Answer: D

The correct option is D, because it is the only answer that contains both groups to which roles can be assigned: To assign a role to a group, you must create a new security or Microsoft 365 group with the isAssignableToRole property set to true

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

upvoted 1 times

🗨️ **wael_kodmani** 4 months, 1 week ago

copilot and Chatgpt choose security only because you can't use Microsoft 365 and mail-enabled security for role assignment!

upvoted 2 times

🗨️ **miki** 7 months, 3 weeks ago

Selected Answer: D

You CAN use : D. mail-enabled security, Microsoft 365, and security only

But recommended would be : B. security only.

But question here is about what you CAN do.

upvoted 1 times

🗨️ **nordbymikael** 9 months, 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 3 times

🗨️ **Shuihe** 1 year, 1 month ago

D

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

upvoted 1 times

🗨️ **Christianbrivio1991** 1 year, 1 month 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** 1 year ago

Sorry, the correct answer is C

upvoted 1 times

🗨️ **TP447** 1 year, 1 month 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** 1 year, 2 months 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 5 times

🗨️ **Darekms0** 1 year, 2 months 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

🗨️ **Darekms0** 1 year, 2 months 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** 1 year, 2 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/microsoft/view/80188-exam-ms-100-topic-5-question-64-discussion/>

upvoted 4 times

🗨️ 👤 **RJTW070** 1 year, 3 months ago

Selected Answer: B

To create a group and assign the Endpoint Security Manager role to the group, you can use a role-assignable group. A role-assignable group is a type of Azure AD security group that can be assigned to a role in Microsoft Endpoint Manager¹. You can create a role-assignable group by using the Azure portal, PowerShell, or Microsoft Graph².

upvoted 2 times

🗨️ 👤 **ae88d96** 1 year, 3 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** 1 year, 2 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

🗨️ 👤 **NrdAlrt** 1 year, 1 month ago

Ex-actly.

upvoted 1 times

HOTSPOT

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

Name	Department	Job title
User1	IT engineering	Technician
User2	Engineering	Senior executive
User3	Finance	Manager

You create a new administrative unit named AU1 and configure the following AU1 dynamic membership rule.

(user.department -eq "Engineering") and (user.jobTitle -notContains "Executive")

The subscription contains the role assignments shown in the following table.

Name	Role
Admin1	AU1\User Administrator
Admin2	Global Administrator

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>
Admin1 can reset the password of User2.	<input type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>

Answer Area

Suggested Answer:

Statements	Yes	No
Admin1 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin1 can reset the password of User2.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2 can reset the password of User3.	<input checked="" type="radio"/>	<input type="radio"/>

Casticod Highly Voted 1 year, 3 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 agument and (must match the 2)

User 1 and user 2 do not belong as the 2 conditions do not match

Therefore user 1 and user 2 do not belong to AU1 and are outside the scope of Admin 1

Option 1 NO

Option 2 NO

Option 3 YES

upvoted 60 times

ct1984 3 months ago

I agree. None of the users are a member of AU1 because of the dynamic membership syntax.

NNY

upvoted 1 times

  **APK1** 4 months, 3 weeks ago

Agree



NNY

upvoted 2 times

  **CloudCanary** 1 year, 3 months ago

Definitely N,N,Y, I agree 100%

upvoted 7 times

  **cb0900** 1 year, 3 months ago

Agree.

NO

NO



YES

upvoted 6 times

  **FredC** Most Recent 2 months, 3 weeks ago

why is user1 not in au1? they have the word engineering in their department and no executive in their title? case sensitivity?

upvoted 1 times

  **3abmula** 1 month, 3 weeks ago

User1 Department: IT engineering

user.department -eq "Engineering" | User1 wouldn't be a member.

user.department -Contains "Engineering" | User1 would be a member.

upvoted 1 times

  **arielreyes2712** 4 months, 1 week ago



Answer is:

N

N



Y

upvoted 1 times

  **blairskimo** 5 months, 3 weeks ago

Answers are correct . user 2 is excluded from the dynamic group as they are a sales executive . The word executive kicks them . The word executive excludes them from AU1 which they need to be in to have their pwd reset as admin 1 is only an admin for the au1 DYNAMIC admin unit

upvoted 1 times

  **LiamAzure** 6 months, 2 weeks ago

Why is the second one no?

upvoted 1 times

  **nordbymikael** 9 months, 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** 1 year ago

I believe NNY

upvoted 2 times

  **TP447** 1 year, 1 month ago

N/N/Y for me.

upvoted 2 times

  **PhoenixMan** 1 year, 2 months 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.

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **APK1** 4 months, 3 weeks ago

Selected Answer: D

Answer is correct

upvoted 1 times

🗨️ 👤 **miki** 7 months, 3 weeks ago

Selected Answer: D

Copilot says :

To receive notifications at your personal email address when a Microsoft Exchange Online service issue occurs, you should:

D. From the Microsoft 365 admin center, customize the Service health settings.

By customizing the Service health settings in the Microsoft 365 admin center, you can set up alerts and notifications to be sent to your personal email address whenever there is a service issue with Exchange Online. This ensures that you are promptly informed about any disruptions or problems that may affect your organization's email services.

upvoted 1 times

🗨️ 👤 **nordbymikael** 9 months, 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** 1 year, 2 months 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** 1 year, 2 months ago

Correct answer is D

upvoted 1 times

🗨️ 👤 **mhmyz** 1 year, 3 months ago

Selected Answer: D

D

Service Health can mail only Exchange issue.



Technical contact get mail M365 total issue.

upvoted 2 times

🗨️ 👤 **Master_Tx** 1 year, 3 months ago

You can do C and D.

upvoted 1 times

  **daye** 1 year, 1 month 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

Suggested Answer:

 **PhoenixMan** Highly Voted 1 year, 1 month ago

I'll go for

1) 1,2,3 and 4

2) 2

upvoted 13 times

🗨️ 👤 **AAlmani** 11 months ago

the request is to Create a guest user not to Invite one! so User 2 only for both! regards,
upvoted 6 times

🗨️ 👤 **Casticod** Highly Voted 1 year, 3 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** 1 year, 3 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** 1 year, 1 month 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** 1 year, 1 month 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

🗨️ 👤 **Frank9020** Most Recent 1 month, 2 weeks ago

1: - Only User2: User Administrators have the necessary permissions to manage user accounts, including creating guest users.

2: - User1 + User2 + User3 (Privileged Role Administrator) Can manage administrative accounts and modify group memberships. User2 (User Administrator) Can manage user accounts and group memberships.

User3 in reality cannot himself to Admin1, because users cannot modify their own group memberships to prevent privilege escalation. This is a security measure to ensure that no single user can unilaterally increase their own permissions. But there is no answer alternative for User1 and User2 only.

upvoted 1 times

🗨️ 👤 **radamelca** 3 months, 1 week ago

I think the answer is correct, neither Billing, security nor privileged administrator can CREATE guest users... so: 1) user 2. 2) user2.

upvoted 1 times

🗨️ 👤 **wael_kodmani** 4 months, 1 week ago

created guest users restricted to admin such as Global Admin, and User Admin.

the question is create not invite!!

the difference between create and invite is:

create: create a guest without sending an invite mail.

invite: send an invitation to the guest.

upvoted 1 times

🗨️ 👤 **APK1** 4 months, 2 weeks ago

B2B "External collaboration settings have default configuration" = means anyone can invite guest users.

Answer is

Box1: All users

Box2: user2

upvoted 2 times

🗨️ 👤 **Barachan** 6 months, 3 weeks ago

This question is tricky, there is NO create guest option in Entra users, just invite guest so

1) All users

2)User2

upvoted 3 times

🗨️ 👤 **Scotte2023** 8 months 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 4 times

 **cpaljchc4** 1 year 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 Administrator.

upvoted 3 times

 **AncaMada112233** 1 year, 1 month ago

"Create" guest users or "Invite" guest users is the same action?

upvoted 5 times

 **Contactfornitish** 1 year, 2 months 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** 1 year, 2 months 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** 1 year, 2 months 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** 1 year, 2 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** 1 year, 3 months 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

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

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ **mikl** 1 month, 3 weeks ago

Selected Answer: D

Copilot votes for D.

To ensure that reports display the names of users who have activated Microsoft 365 apps and on how many devices, you should modify:

D. Org settings for Reports
upvoted 1 times

🗨️ **Amir1909** 4 months, 4 weeks ago

D is correct

upvoted 3 times

🗨️ **solderboy** 6 months ago

Selected Answer: D

<https://learn.microsoft.com/en-us/microsoft-365/troubleshoot/miscellaneous/reports-show-anonymous-user-name>

upvoted 2 times

🗨️ **cb0900** 9 months, 3 weeks ago

Selected Answer: D

D Uncheck "Display concealed user, group, and site names in all reports".

upvoted 4 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:

- Organization profile
- Security & privacy
- Services

Integrate the internal support tool with Office:

- Organization profile
- Security & privacy
- Services

Answer Area

Sign users out after one hour of inactivity:

- Organization profile
- Security & privacy
- Services

Suggested Answer:

Integrate the internal support tool with Office:

- Organization profile
- Security & privacy
- Services

- ae88d96 **Highly Voted** 1 year, 3 months ago
 Security & privacy and Organization profile. Tested on my lab.
 upvoted 24 times
- Frank9020 **Most Recent** 1 month, 2 weeks ago
 Given answers are correct: Security & privacy + Services
 upvoted 1 times
- APK1 4 months, 3 weeks ago
 Correct answers are
 Security & Privacy
 Organization Profile
 upvoted 1 times
- blairkimo 5 months, 2 weeks ago
 correct "Security & privacy and Organization profile." why do they give the wrong answeres some times
 upvoted 2 times
- samsa1 4 months, 2 weeks ago
 i'm asking the same question
 upvoted 1 times
- Amir1909 11 months ago

- Security & Privacy
- Organization Profile
upvoted 4 times

🗨️ 👤 **smiff** 1 year, 3 months ago

Security and Privacy
Org Profile

checked on my demo tenant
upvoted 3 times

🗨️ 👤 **DiligentSam** 1 year, 3 months 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** 1 year, 3 months ago

Yes - "Support integration"
upvoted 3 times

🗨️ 👤 **daye** 1 year, 1 month ago

Yes
Idle session timeout from the Security & privacy tab.
Support integration from the org profile tab.
upvoted 1 times

You have a Microsoft 365 subscription.

You add a domain named contoso.com.

When you attempt to verify the domain, you are prompted to send a verification email to admin@contoso.com.

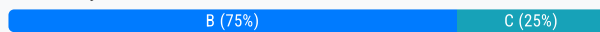
You need to change the email address used to verify the domain.

What should you do?

- A. Add a TXT record to the DNS zone of the domain.
- B. From the domain registrar, modify the contact information of the domain.
- C. From the Microsoft 365 admin center, change the global administrator of the Microsoft 365 subscription.
- D. Modify the NS records for the domain.

Suggested Answer: B

Community vote distribution



NrdAlrt Highly Voted 1 year, 1 month ago

Selected Answer: B

A would be way less hassle to verify the domain, but B answers the question's requirement.

upvoted 7 times

Vaerox 11 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 3 times

pinky285 Most Recent 1 month, 1 week ago

Selected Answer: B

since this is verifying your domain and txt/mx is not being used and email is, then to verify your domain using email ms will send it to the contact of the domain (the admin email whois).

upvoted 1 times

jarattdavis 4 months, 2 weeks ago

Selected Answer: C

Correct answer = C. From the Microsoft 365 admin center, change the global administrator of the Microsoft 365 subscription.

A. Add a TXT record to the DNS zone of the domain: This is a valid step for verifying the domain ownership, but it won't change the email address used for verification.

B. Modify the contact information of the domain: This might update some contact details associated with the domain, but it wouldn't affect the specific email used for Microsoft 365 domain verification.

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

Suggested Answer:

Computer2:

- Group1 only
- Group3 only
- Group1 and Group3

cb0900 Highly Voted 1 year, 3 months 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 11 times

LiamAzure Most Recent 6 months, 2 weeks ago

Group 1 for both, it gets added to the highest ranked group it hits and no others
upvoted 2 times

miki 7 months, 3 weeks ago

Group 1 for both here.
upvoted 1 times

Greatone1 1 year, 2 months ago

Group 1 for both

upvoted 2 times

  **Greatone1** 1 year, 2 months ago

<https://www.examttopics.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

Suggested 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 1 year, 3 months 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.examtactics.com/discussions/microsoft/view/110910-exam-ms-101-topic-2-question-138-discussion/>

upvoted 15 times

  **imlearningstuffagain** 1 year, 2 months ago

this is nice wording, the Application Administrator didn't have access to begin with. So he/she doesn't lose access. Correct?

upvoted 7 times

  **nils241** 1 year ago

Users with "Application Admin Role" can only create and manage all aspects of enterprise applications, application registrations, and application proxy settings.

upvoted 2 times

  **sergioandreslq** 1 year, 1 month 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

  **APK1**  4 months, 2 weeks ago

Given answer is correct.

For the second question here is the key point in the question "Users that will NO LONGER have access" - The Application Admin never had access so shouldn't be included.



upvoted 1 times

  **jarattdavis** 4 months, 2 weeks ago

= Admin1 and Admin2 can enable RBAC because they have the highest-level administrative privileges (Global Administrator and Security Administrator).



= Admin3, Admin4, and Admin5 will lose access to the Microsoft 365 Defender portal after RBAC is enabled. This is because they have roles that are typically granted limited or read-only access, and RBAC allows for granular control over permissions.

upvoted 1 times

  **Murad01** 6 months, 1 week ago

Given answer are correct

upvoted 1 times

  **Jamesat** 8 months, 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** 10 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** 1 year ago

NO2 : Admin3, Admin4, Admin5

upvoted 4 times

Your company has a Microsoft 365 E5 subscription.

You onboard a device on the company's network to Microsoft Defender for Endpoint.

In the Microsoft 365 Defender portal, you notice that the device inventory displays many devices that have an Onboarding status of Can be onboarded.

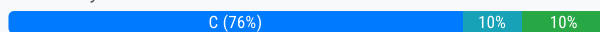
You need to ensure that onboarded devices are prevented from polling the network for device discovery but can still discover devices with which they communicate directly.

What should you configure in the Microsoft 365 Defender portal?

- A. standard discovery
- B. device discovery exclusions
- C. basic discovery
- D. a network assessment job

Suggested Answer: B

Community vote distribution



netbw Highly Voted 1 year, 3 months 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 12 times

jarattdavis Most Recent 4 months, 2 weeks ago

Selected Answer: B

B. device discovery exclusions

Here's why:

Standard discovery and basic discovery are both discovery methods that allow devices to poll the network for other devices. This is not what you want to prevent.

A network assessment job is used to assess the security posture of your network. It doesn't directly address the issue of preventing onboarded devices from polling the network.

Device discovery exclusions allow you to specify devices that should be excluded from network-wide device discovery. By excluding onboarded devices from this discovery method, you can prevent them from polling the network for other devices while still allowing them to discover devices with which they communicate directly.

upvoted 1 times

XylosSW 5 months, 2 weeks ago

Selected Answer: C

"In the Device Discovery settings, select Basic Device Discovery mode. This mode restricts the devices from polling the network to discover other devices. Instead, it allows devices to discover only those with which they directly communicate."

Explanation:

Standard Discovery: This mode might allow for broader network polling which doesn't meet the requirement of limiting discovery to direct communications only.

Device Discovery Exclusions: These settings are typically used to exclude specific devices or IP ranges from being discovered but don't inherently restrict onboarded devices from polling the network for discovery.

ChatGPT 4-o says C

upvoted 1 times

🗨️ 👤 **BossLG** 9 months, 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** 10 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 4 times

🗨️ 👤 **Amir1909** 11 months ago

C is correct

upvoted 1 times

🗨️ 👤 **Vaerox** 11 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** 11 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 portal¹. 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 devices¹.

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** 11 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** 11 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** 1 year, 1 month ago

It could be D; A network assessment job

upvoted 2 times

🗨️ 👤 **Cfernandes** 1 year, 2 months ago

Selected Answer: C

C esta correta.

upvoted 4 times

🗨️ 👤 **jt2214** 1 year, 2 months 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** 1 year, 3 months 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** 1 year, 3 months 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

Suggested Answer:

Device1:

- A local script
- Group Policy
- Microsoft Intune
- An app from the Google Play store
- Integration with Microsoft Defender for Cloud

Device2:

- A local script
- Group Policy
- Microsoft Intune
- An app from the Google Play store
- Integration with Microsoft Defender for Cloud

 **cb0900** Highly Voted 9 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 15 times

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

I would agree with given answers:


1. Intune
2. Local script

upvoted 1 times

 **Cfernandes** 8 months, 1 week ago

Testado no meu laboratório, intune e script local

upvoted 2 times



  **Contactfornitish** 8 months, 2 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 4 times

  **[Removed]** 9 months, 2 weeks ago

Agree with the answer

upvoted 1 times

  **Casticod** 10 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

HOTSPOT

-

You have a Microsoft 365 subscription.

You need to create two groups named Group1 and Group2. The solution must meet the following requirements:

- Group1 must be mail-enabled and have an associated Microsoft SharePoint Online site.
- Group2 must support dynamic membership and role assignments but must NOT be mail-enabled.

Which types of groups should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Group1:

- Distribution
- Dynamic distribution
- Microsoft 365
- Security

Group2:

- Distribution
- Dynamic distribution
- Microsoft 365
- Security

Answer Area

Suggested Answer:

Group1:

- Distribution
- Dynamic distribution
- Microsoft 365
- Security

Group2:

- Distribution
- Dynamic distribution
- Microsoft 365
- Security

 **vercracked_007** Highly Voted 1 year, 3 months ago

Box 1 Microsoft 365

Box 2 Security

They are swapped

upvoted 51 times

 **Tr619899** Most Recent 3 months ago

Group1: Microsoft 365

This type of group is mail-enabled, supports email communication, and comes with an associated SharePoint Online site by default.

=> Microsoft 365 Groups are designed for collaboration across Microsoft services like Teams, SharePoint, and Outlook, providing a mail-enabled option with access to a SharePoint Online site.

Group2: Security

Security groups support dynamic membership and role assignments but are not mail-enabled.

=> Security Groups are used primarily for controlling access to resources. They support dynamic membership and role assignments but are not mail-enabled, meeting the requirements for Group2.

upvoted 2 times

🗨️ **miki** 7 months, 3 weeks ago

Damn I was confused when I say the answer - total opposite! Oh well :D

For your Microsoft 365 subscription, to meet the specified requirements for Group1 and Group2, you should create the following types of groups:

Group1: Create a Microsoft 365 Group. This type of group is mail-enabled by default and comes with an associated SharePoint Online. When you create a Microsoft 365 Group, it includes a shared mailbox, calendar, and a SharePoint site among other features.

Group2: Create a Security Group with dynamic membership rules in Microsoft Entra ID. This group can support dynamic membership and role assignments. To ensure it is not mail-enabled, do not create it as a Microsoft 365 Group but rather as a security group which can be configured for dynamic membership and can have roles assigned without being mail-enabled.

upvoted 3 times

🗨️ **nordbymikael** 9 months, 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** 10 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** 11 months ago

- Microsoft 365

- Security

upvoted 2 times

🗨️ **mickey88** 1 year 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 No

Answer is 1: M365 2 security

upvoted 1 times

🗨️ **cpaljchc4** 1 year 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

🗨️ **jjdrost_11** 1 year 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** 1 year, 1 month 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** 1 year, 1 month ago

Box 1: Microsoft 365

Box 2: Dynamic distribution

upvoted 2 times



🗨️ **jt2214** 1 year, 2 months ago

It's the other way around. Exam topics please fix this. :)

Box 1 Microsoft 365

Box 2 Security



upvoted 2 times

  **DiligentSam** 1 year, 3 months ago

Support dynamic membership

why not choose Dynamic Distribution?

upvoted 1 times

  **netbw** 1 year, 3 months ago

Because it's gonna be email enabled

upvoted 1 times

  **Casticod** 1 year, 3 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

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
<input type="text" value="Message center"/>	To report issues regarding a Microsoft 365 service: <input type="text"/>
<input type="text" value="New service request"/>	To request help on how to add a new user to the tenant: <input type="text"/>
<input type="text" value="Product feedback"/>	
<input type="text" value="Service health"/>	

Suggested Answer:

To report issues regarding a Microsoft 365 service:

To request help on how to add a new user to the tenant:

Casticod Highly Voted 1 year, 3 months ago
 option 1 Service Health --> Report Issues
 option 2 new service request
 upvoted 45 times

jt2214 Highly Voted 1 year, 2 months ago
 Service Health
 New Service Requests

I do this at my organization.
 upvoted 9 times

cerniauskas Most Recent 7 months, 1 week ago
 Examtopics is all about money, terrible questions and answers
 upvoted 6 times

Jamesat 8 months, 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 2 times

Tomtom11 9 months ago
 Option 2 should be Health from the Entra ID portal?
 upvoted 1 times

shaffer 10 months, 1 week ago

I'm glad you all confirmed my suspicions

upvoted 1 times

🗨️ 👤 **pri27** 1 year ago

Discussion ppl are Right,If you still have doubt go here...

<https://www.examttopics.com/discussions/microsoft/view/96073-exam-ms-100-topic-2-question-87-discussion/>

upvoted 2 times

🗨️ 👤 **Noble00** 1 year, 1 month ago

The answer is so wrong.

upvoted 3 times

🗨️ 👤 **benpatto** 1 year, 1 month 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 4 times

🗨️ 👤 **Khattak3143** 4 months, 3 weeks ago

I was thinking the same, but thank goodness for the community discussion. This in itself is a learning curve!

upvoted 1 times

🗨️ 👤 **Greatone1** 1 year, 2 months ago

Service Health and second answer is new service requests

upvoted 2 times

🗨️ 👤 **flim322** 1 year, 3 months ago

<https://www.examttopics.com/discussions/microsoft/view/96073-exam-ms-100-topic-2-question-87-discussion/>

upvoted 1 times

You have a Microsoft 365 E5 subscription that contains the groups shown in the following exhibit.

The screenshot shows the 'Groups | All groups' page in the Azure Active Directory portal for Contoso Ltd. The page includes a search bar, a search mode toggle set to 'Contains', and a table of four groups. The table columns are Name, Group type, Security enabled, and Role assignments allowed. The groups are Group1, Group2, Group3, and Group4.

<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

Suggested Answer: C

Community vote distribution

E (100%)

cb0900 Highly Voted 1 year, 3 months 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-what-is-azure-portal?context=azure%2Factive-directory%2Fusers-groups-roles%2Fcontext%2Fugr-context#features>

Similar q from sc-300:

<https://www.examtactics.com/discussions/microsoft/view/51472-exam-sc-300-topic-1-question-1-discussion/>
upvoted 18 times

CloudCanary Highly Voted 1 year, 3 months ago

Selected Answer: E

Microsoft 365 Groups with Security Enabled can be assigned with licences.

upvoted 6 times

Frank9020 Most Recent 1 month, 2 weeks ago

Selected Answer: E

Given Answer is correct:

Group2: Microsoft 365 group, security enabled. Can be assigned licenses.

Group3: Security group, security enabled. Can be assigned licenses.

Group4: Security group, security enabled, allows role assignments. Can be assigned licences.



upvoted 1 times

  **APK1** 4 months, 3 weeks ago

Selected Answer: E

Given answer is wrong - it should be Group2, 3, 4

upvoted 2 times

  **Jamesat** 8 months, 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

  **Tomtom11** 9 months ago

security enabled means you can include these groups in DACLS

upvoted 1 times

  **Cfernandes** 1 year, 2 months ago

Concordo com grupo, 2 3 e 4

upvoted 2 times

HOTSPOT

You have a Microsoft 365 subscription.

From the Microsoft 365 admin center, you open the Microsoft 365 Apps usage report as shown in the following exhibit.

Username ⓘ	Last activation date (UTC)	Last activity date (UTC)	⌵ Choose columns
43188D0D1D05D877FDC4416			
2F2747649D4150B686307383			
659213C0E1D99EA1A4AD56D		Wednesday, August 3, 2022	
FE185622F642B0381DB633EC			
988D39ED225FC80FF2A5684			

You need ensure that the report meets the following requirements:

- The Username column must display the actual name of each user.
- Usage of the Microsoft Teams mobile app must be displayed.

What should you modify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

The Username column must display the actual name of each user:

▼

- Privacy profile in Org settings
- Reports in Org settings
- The membership of the Reports Reader role

Usage of the Teams mobile app must be displayed:

▼

- Microsoft Teams in Org settings
- The columns in the report
- The Teams license assignment

Suggested Answer:

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 9 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 33 times

m2L Most Recent 6 months, 2 weeks ago

Hello Guys,

the answers are :

1 : Reports in Org Setting by(Org Setting>Services)

2: Columns In the rappers 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 3 times

🗨️ 👤 **m2L** 6 months, 2 weeks ago

Hello Guys,

the answers are :

1 : Reports in Org Setting by(Org Setting>Services)

2: Columns In the rappers 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

🗨️ 👤 **Festus365** 7 months, 2 weeks ago

Box 1: Privacy profile in Org settings

Box 2: Microsoft Teams in Org settings

upvoted 1 times

🗨️ 👤 **spektrum1988** 5 months ago

100% sure box 1 is: Reports in Org settings.

100% sure box 2 is: choose columns

Tested and confirmed.

upvoted 4 times

🗨️ 👤 **Casticod** 10 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).

Suggested Answer: AC

Community vote distribution


AC (100%)

 **jt2214** Highly Voted 1 year, 3 months 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 11 times

 **Frank9020** Most Recent 1 month, 2 weeks ago

Selected Answer: AC

Given answer is correct

upvoted 1 times

 **miki** 7 months, 3 weeks ago

Selected Answer: AC

Copilot says :

To ensure that you can view the health status of Server1, which is not listed on the Azure AD Connect Servers list, you should consider the following two actions:

A. From Windows PowerShell, run the Register-AzureADConnectHealthSyncAgent cmdlet. This cmdlet is used to manually register the Azure AD Connect Health agent if it fails to register during installation or if it has been unregistered.

C. From Server1, reinstall the Azure AD Connect Health agent. Reinstalling the agent can help resolve issues where the server is not listed due to a failed or incomplete installation.

upvoted 1 times

🗨️ 👤 **AAlmani** 11 months ago

Selected Answer: AC

A or C solve the issue.

<https://www.examttopics.com/discussions/microsoft/view/14496-exam-ms-100-topic-2-question-18-discussion/>

upvoted 2 times

🗨️ 👤 **TP447** 1 year, 1 month ago

Technically A + D is valid too (if the agent is still installed but timed out after 30 days on inactivity - you would just then 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

Answer Area

1

Add a custom domain name.

2

Verify the custom domain.

3

Modify the username of User1.

Suggested Answer:

Festus365 Highly Voted 1 year, 1 month 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 13 times

BossLG 9 months, 2 weeks ago

<https://www.examttopics.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 5 times

DiligentSam Highly Voted 1 year, 2 months ago

<https://www.examttopics.com/discussions/microsoft/view/49929-exam-ms-100-topic-2-question-7-discussion/>

upvoted 6 times

Frank9020 Most Recent 1 month, 2 weeks ago

Given answers are correct:

upvoted 1 times

DNGFORMA 7 months ago

Given answer is correct, modify the email doesn't change the login username

upvoted 1 times

Paul_white 1 year, 2 months ago

GIVEN ANSWER IS CORRECT !!!!

upvoted 5 times

  **spectre786** 1 year, 2 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

Suggested Answer: B

Community vote distribution

B (100%)



🗨️ 👤 **LiamAzure** 6 months, 2 weeks ago

Selected Answer: B

Microsoft 365 Admin App
upvoted 3 times

🗨️ 👤 **nils241** 1 year ago

Selected Answer: B

Correct
upvoted 3 times

🗨️ 👤 **DiligentSam** 1 year, 3 months ago

Option B is correct
upvoted 4 times

🗨️ 👤 **[Removed]** 1 year, 3 months ago

Agree with the answer
upvoted 4 times

HOTSPOT

-

Your company has a Microsoft 365 subscription that contains the domains shown in the following exhibit.

Domains

+ Add domain Buy domain Refresh

Domain name ↑	Status	Choose columns
<input type="checkbox"/> contoso221018.onmicrosoft.com (Default)	Healthy	
<input type="checkbox"/> contoso.com	Incomplete setup	
<input type="checkbox"/> east.contoso221018.onmicrosoft.com	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

Suggested Answer:

Exchange Online can receive inbound email messages sent to the [answer choice].

contoso221018.onmicrosoft.com domain only
 contoso221018.onmicrosoft.com domain and all its subdomains only
 contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only
 contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

 **Casticod** Highly Voted 1 year, 3 months ago

Tested

option 1 contoso@221018.onmicrosoft.com and eastcontoso@221018.onmicrosoft.com

Option 2 contoso@221018.onmicrosoft.com only

upvoted 47 times

 **basak** 7 months, 2 weeks ago

option 1 will be all domain. for contoso.com domain is verified just mx, autodiscover ,spf record not added. so user can be created but mail service will not work. tested in lab

upvoted 1 times

🗨️ 👤 **Bobalo** 6 months, 1 week ago

Why argue with someone who actually tested it?

upvoted 3 times

🗨️ 👤 **Frank9020** Most Recent 1 month, 2 weeks ago

1: - contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only.

2: - contoso221018.onmicrosoft.com domain only.

upvoted 1 times

🗨️ 👤 **APK1** 4 months, 3 weeks ago

First answer is wrong - you cannot add any services on incomplete domain

upvoted 2 times

🗨️ 👤 **blairkimo** 5 months, 2 weeks ago

You cant add UIDs with contoso.com domains . Its not set up . Why is this designated a right answer ?

upvoted 1 times

🗨️ 👤 **Fran22** 10 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 3 times

🗨️ 👤 **Vaerox** 11 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 2 times

🗨️ 👤 **Vaerox** 11 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 3 times

🗨️ 👤 **Testtest123** 1 year 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.

So the first question is correct: contoso@221018.onmicrosoft.com and eastcontoso@221018.onmicrosoft.com

Question two is also correct.

upvoted 3 times

🗨️ 👤 **TP447** 1 year, 1 month 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** 1 year, 1 month ago

Scratch this - it works for a subdomain that is incomplete but not a top level domain.

upvoted 2 times

🗨️ 👤 **mhmyz** 1 year, 3 months ago

"No Service Selected" is completed step1 but imcompleted 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

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

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

The storage usage of files stored in Microsoft Teams:

Number of active users per Microsoft Team:

Requirements**Suggested 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** Highly Voted 1 year, 3 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 22 times

 **Frank9020** Most Recent 1 month, 2 weeks ago

1: - The storage usage of files stored in Microsoft Teams: The SharePoint site usage report.

This report provides details on the storage usage of files stored in SharePoint, which includes files stored in Microsoft Teams.

2: - The number of active users per team: The User activity report in Teams. This report provides information on the activity levels of users within Microsoft Teams.

upvoted 1 times

 **Frank9020** 1 month, 2 weeks ago

Correction: 2=Teams usage report.

upvoted 1 times

 **APK1** 4 months, 3 weeks ago

Second answer should be = Teams usage report

upvoted 2 times

 **Tomtom11** 9 months 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** 9 months ago

<https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/sharepoint-site-usage-ww?view=o365-worldwide>

upvoted 1 times

  **m2L** 1 year ago

The First is typically OneDrive Usage

upvoted 1 times

  **solderboy** 12 months ago

You are incorrect. OneDrive is for personal chat files, not for Teams. Teams files stored in SharePoint.

upvoted 3 times

  **Blagojche** 1 year, 2 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

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 enterpriseregistration DNS records you should add? To answer, select the appropriate options in the answer area.

Answer Area

Domains: ▼

1
2
3

Enterpriseregistration DNS records: ▼

1
2
3

Answer Area

Suggested Answer:

Domains:

1
2
3

Enterpriseregistration DNS records:

1
2
3

cb0900 Highly Voted 1 year, 3 months ago

- 1 domain. Sub-domains don't need to be verified, so just fabrikam.com.
- 3 Enterpriseregistration DNS records.

<https://www.examttopics.com/discussions/microsoft/view/51183-exam-ms-100-topic-4-question-48-discussion/>
upvoted 25 times

Amir1909 Highly Voted 11 months ago

- 1
 - 3
- upvoted 5 times

Frank9020 Most Recent 1 month, 2 weeks ago

- Total Domains to Verify: 1 (fabrikam.com)
 - Minimum Enterpriseregistration DNS Records: 3 (one for each new domain and subdomain: fabrikam.com, east.fabrikam.com, west.contoso.com)
- upvoted 1 times

Cavazzana 4 months, 3 weeks ago

I tested in lab... any subdomain needs TXT record create when add domain in Office 365 Portal. Answer 3/3
upvoted 1 times

APK1 4 months, 3 weeks ago

1 and 3
Subdomains are not required to verify
upvoted 1 times

spatrick 7 months, 2 weeks ago

If you want to add a subdomain name such as 'europe.contoso.com' to your organization, you should first add and verify the root domain, such as contoso.com. The subdomain is automatically verified by Microsoft Entra ID. To see that the subdomain you added is verified, refresh the domain list in the browser.

Is it a tricky question again? It needs to be verified. In this case it is automatically verified. 1=3 Seems to correct.
2=3 Correct
upvoted 3 times

norbe01 4 months, 1 week ago



This hurt me so much, I'm also thinking 2=3 as it tricky question.
upvoted 1 times

Drubury 1 year, 2 months 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 2 times

  **Drubury** 1 year, 2 months 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** 1 year, 2 months ago

<https://www.examttopics.com/discussions/microsoft/view/51183-exam-ms-100-topic-4-question-48-discussion/>

upvoted 3 times

  **Greatone1** 1 year, 2 months ago

Should be 1 and second is 3

upvoted 4 times

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

Suggested Answer: D

Community vote distribution

D (100%)

 **Momskii** Highly Voted 9 months, 2 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 10 times

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

Selected Answer: D

For monitoring and reporting application access with a Microsoft 365 E5 subscription, while also supporting KQL (Kusto Query Language) for querying data and retaining report data for at least one year, you should include in the recommendation:

D. Azure Monitor workbooks

upvoted 1 times

 **Tomtom11** 3 months 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

Suggested 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 1 year, 3 months ago

Correct

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-quickstart-naming-policy>
upvoted 12 times

 **jarattdavis** Most Recent 4 months, 2 weeks ago

Correct:

<https://learn.microsoft.com/en-us/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide#:~:text=A-,Microsoft%20365%20group,->

naming%20policy%20only

upvoted 1 times

  **miki** 7 months, 3 weeks ago

To configure a group naming policy for your Microsoft 365 E5 subscription, you should use the Microsoft Entra admin center. Specifically, you would navigate to the Groups section under Manage, and then access the Naming policy settings.

The group naming policy will apply to Microsoft 365 Groups, which are used across various Microsoft services like Outlook, Microsoft Teams, SharePoint, Planner, and others. The policy affects both the group name and group alias and is enforced when a group is created or when an existing group's name, alias, description, or avatar is edited.

upvoted 2 times

  **Thomasname** 10 months, 1 week ago

Correct

<https://learn.microsoft.com/en-us/entra/identity/users/groups-naming-policy#configure-a-naming-policy>

upvoted 2 times

  **Amir1909** 11 months ago

Correct

upvoted 1 times

HOTSPOT

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

Name	Type	Security enabled	Role assignments allowed
Group1	Microsoft 365	No	No
Group2	Microsoft 365	No	No
Group3	Security	Yes	Yes
Group4	Security	Yes	No
Group5	Security	Yes	No
Group6	Distribution	No	No

Which groups can be members of Group1 and Group4? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Group1:

- None of the groups
- Group2 only
- Group2 and Group4 only
- Group2, Group4, Group5, and Group6 only
- Group2, Group3, Group4, Group5, and Group6

Group4:

- None of the groups
- Group5 only
- Group3 and Group5 only
- Group1, Group2, Group3, and Group5 only
- Group1, Group2, Group3, Group5, and Group6

Answer Area

Suggested Answer:

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

🗨️ **cb0900** Highly Voted 1 year, 3 months 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 24 times

🗨️ **vercracked_007** Highly Voted 1 year, 3 months 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 10 times

🗨️ **vercracked_007** 1 year, 3 months ago

The other way around wont work. Group 4 cant be a member of group 5

upvoted 1 times

🗨️ **vercracked_007** 1 year, 3 months ago

Sorry, group 3

upvoted 2 times

🗨️ **Kallely** Most Recent 2 months, 3 weeks ago

Group 1: None

Group 4: Only Group 5, Currently don't support: "Adding groups as members of a role-assignable group" Group 3 Role assignments allowed group.

upvoted 2 times

🗨️ **Tomtom11** 9 months ago

<https://learn.microsoft.com/it-it/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>

upvoted 1 times

🗨️ **Thomasname** 10 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 7 times

🗨️ **m2L** 1 year ago

Thank you @Flim322, you are righth,

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** 12 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 6 times

🗨️ 👤 **benpatto** 1 year, 1 month ago

seems no one has a good answer for this... :D

upvoted 1 times

🗨️ 👤 **Festus365** 1 year, 1 month 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** 1 year, 3 months 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 4 times

🗨️ 👤 **norbe01** 4 months, 1 week ago

Group3, being a role-assignable group, cannot have other groups nested within it, but it can be added as a member of Group4 since Group4 is not role-assignable. Therefore, the correct answer for Group4 is "Group3 and Group5 only."

upvoted 1 times

🗨️ 👤 **solderboy** 12 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

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

Suggested Answer: C

Community vote distribution

C (63%)

B (38%)

 **cb0900** Highly Voted 1 year, 3 months 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 13 times

 **JensV** 1 year, 3 months 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 6 times

 **60ed5c2** 1 year, 2 months 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 1 year, 3 months ago

Selected Answer: B

Usage location is mandatory to affect license.

upvoted 10 times

 **elwa1** Most Recent 3 months, 3 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/users/licensing-admin-center>:

Some Microsoft services are not available in all locations. Before a license can be assigned to a user, the administrator has to specify the Usage location property on the user.

For group license assignment, any users without a usage location specified inherit the location of the directory. If you have users in multiple locations, we recommend that you always set usage location as part of your user creation flow in Microsoft Entra ID. For example, configure Microsoft Entra Connect configuration to set usage location. This recommendation makes sure the result of license assignment is always correct and users do not receive services in locations that are not allowed.

upvoted 1 times

🗨️ 👤 **abill** 4 months, 1 week ago

Tested - answer is 3

upvoted 1 times

🗨️ 👤 **Khanbaba43** 4 months, 2 weeks ago

Selected Answer: C

Answer: C

<https://www.examttopics.com/discussions/microsoft/view/49561-exam-ms-100-topic-2-question-11-discussion/>

upvoted 1 times

🗨️ 👤 **miki** 7 months, 3 weeks ago

Selected Answer: C

I would go for C here.

upvoted 2 times

🗨️ 👤 **[Removed]** 8 months 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** 8 months, 1 week 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** 8 months, 1 week 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** 9 months ago

<https://learn.microsoft.com/en-us/entra/identity/users/licensing-group-advanced>

upvoted 1 times

🗨️ 👤 **msmamrs** 9 months, 3 weeks ago

Selected Answer: B

definitely B!

upvoted 2 times

🗨️ 👤 **692a0df** 11 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** 11 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** 11 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** 1 year, 1 month ago

Selected Answer: C

For group license assignment, any users without a usage location specified inherit the location of the directory.

upvoted 4 times

🗨️ 👤 **Darekmso** 1 year, 2 months ago

Selected Answer: C

<https://www.examttopics.com/discussions/microsoft/view/49561-exam-ms-100-topic-2-question-11-discussion/>

upvoted 3 times

🗨️ 👤 **Lud0** 1 year, 3 months 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

Suggested 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  1 year, 3 months 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 51 times

  **Fran22** 10 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 4 times

  **Frank9020** Most Recent 1 month, 2 weeks ago

CORRECT:

Y: - User2 can reset the password for User1 because User1 is in AU1, and User2 is a Password Administrator for AU1.

N: - User2 cannot reset the password for User4, because User4 is in AU2, and User2's scope is limited to AU1.

Y: User3 can assign licenses to User1, because User3 is a License Administrator with a scope of the entire organization, which includes User1.

upvoted 2 times



  **APK1** 4 months, 2 weeks ago

NNY is the correct answer.

for me the given answer was correct, but then this document made me the correct answer as NNY

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

upvoted 1 times



  **Tomtom11** 4 months, 2 weeks ago

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

The last answer is correct

Note that if you assign a role to a user that is not a member of an administrative unit, the scope of the role is the entire tenant.

upvoted 1 times

  **XylosSW** 5 months, 3 weeks ago

Answer is correct by Copilot:

1. Yes, User 2 can reset the password of User1. User 2 is a Password Administrator and has scope over AU1, which includes User1 as it's a member of Group1 in AU1.

2. No, User 2 cannot reset the password of User4. Although User 2 is a Password Administrator, User4 is not under the scope of User2 (AU1).

3. Yes, User 3 can assign licenses to User1. User 3 is a License Administrator and has an organization-wide scope, which includes all users.

upvoted 1 times

  **PMR24875** 3 months, 1 week ago

User1 not in AU1, so 1 should be No

upvoted 2 times

  **Frank9020** 1 month, 3 weeks ago



User1 is in Group1, that is member of AU1, so answer is YES

upvoted 1 times

  **Frank9020** 1 month, 3 weeks ago

My bad, correct is N+N+Y: n order for the User Administrator to manage the user properties or user authentication methods of individual members of the group, the group members (users) must be added directly as members of the administrative unit.

upvoted 1 times

  **oopspruu** 8 months, 2 weeks 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** 10 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 2 times

  **CheMetto** 1 year, 2 months ago

I confirm NNY, Nested group aren't supported from Administrative Unit!
upvoted 3 times

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

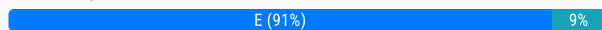
Name	Role
User1	Reports Reader
User2	Exchange Administrator
User3	User Experience Success Manager

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

Suggested Answer: E

Community vote distribution



Casticod Highly Voted 1 year, 3 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 13 times

Greatone1 Highly Voted 1 year, 2 months 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 8 times

norbe01 Most Recent 3 months, 2 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

<https://learn.microsoft.com/en-us/microsoft-365/admin/adoption/adoption-score?view=o365-worldwide>
upvoted 2 times

🗨️ 👤 **jarattdavis** 4 months, 2 weeks ago

Selected Answer: D

D. User1 and User3 only

Here's why:

User1 has the Reports Reader role, which provides access to various reports, including the Adoption Score.

User3 has the User Experience Success Manager role, which also includes access to the Adoption Score.

User2 has the Exchange Administrator role, which primarily focuses on Exchange Online administration tasks and doesn't include access to the Adoption Score

upvoted 1 times

🗨️ 👤 **jarattdavis** 4 months, 2 weeks ago

THis is wrong.

E: is the correct answer

upvoted 2 times

🗨️ 👤 **Amir1909** 11 months ago

E is correct

upvoted 3 times

HOTSPOT

-

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

Name	Type	Role
Group1	Security	Helpdesk Administrator
Group2	Security	None
Group3	Microsoft 365	User Administrator

The subscription contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

In Azure AD, you configure the External collaboration settings as shown in the following exhibit.

Guest user access

Guest user access restrictions ⓘ

[Learn more](#)

- Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- Only users assigned to specific admin roles can invite guest users
- No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

[Learn more](#)

Yes No

External user leave settings

Allow external users to remove themselves from your organization (recommended) ⓘ

[Learn more](#)

Yes No

Collaboration restrictions

- Allow invitations to be sent to any domain (most inclusive)
- Deny invitations to the specified domains
- Allow invitations only to the specified domains (most restrictive)

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can invite guest users.	<input type="radio"/>	<input type="radio"/>
User2 can invite guest users.	<input type="radio"/>	<input type="radio"/>
User3 can invite guest users.	<input type="radio"/>	<input type="radio"/>

Answer Area

Suggested Answer:

Statements

Yes

No

User1 can invite guest users.

User2 can invite guest users.

User3 can invite guest users.

 **jt2214** Highly Voted 1 year, 2 months 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 13 times

 **INSOMEA** Highly Voted 1 year, 3 months ago

correct

upvoted 8 times

 **wael_kodmani** Most Recent 4 months ago

correct I tested

upvoted 1 times

 **Tomtom11** 9 months 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

 **PhoenixMan** 1 year, 1 month ago

in today exam

upvoted 5 times

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You have an Azure AD tenant named contoso.com that contains the following users:

- Admin1
- Admin2
- User1

Contoso.com contains an administrative unit named AU1 that has no role assignments. User1 is a member of AU1.

You create an administrative unit named AU2 that does NOT have any members or role assignments.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can add Admin1 as a member of AU1.	<input type="radio"/>	<input type="radio"/>
You can add User1 as a member of AU2.	<input type="radio"/>	<input type="radio"/>
You can assign Admin2 the User administrator role for AU1.	<input type="radio"/>	<input type="radio"/>

Answer Area

Suggested Answer:

Statements	Yes	No
You can add Admin1 as a member of AU1.	<input checked="" type="radio"/>	<input type="radio"/>
You can add User1 as a member of AU2.	<input checked="" type="radio"/>	<input type="radio"/>
You can assign Admin2 the User administrator role for AU1.	<input type="radio"/>	<input checked="" type="radio"/>

cb0900 Highly Voted 1 year, 3 months ago

Y
Y
Y

<https://www.examttopics.com/discussions/microsoft/view/96500-exam-ms-100-topic-3-question-100-discussion/>
upvoted 24 times

Paul_white 1 year, 2 months ago

THANK YOU BROTHER
upvoted 3 times

APK1 Highly Voted 5 months ago

Who am I? I must be Global Admin for my Tenant - so the answer should be YYY
upvoted 7 times

Khattak3143 Most Recent 4 months, 3 weeks ago

and here I thought Microsoft exam creators claimed, they aren't in the business of tricking
upvoted 2 times

🗨️ 👤 **martinods** 7 months ago

ok but what is my role :-) ?
upvoted 4 times

🗨️ 👤 **e6d6bf4** 6 months, 2 weeks ago

Since the question stated "You create an administrative unit named AU2 that does NOT have any members or role assignments." --> to be able to create AU, you have to be "Global Admin or Privilege Role Admin". So it is safe to assume, "You" in this question has one of those role.

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-manage?tabs=ms-powershell>

upvoted 4 times

🗨️ 👤 **de0e20a** 8 months, 1 week 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** 1 year, 2 months ago

Should be Y,Y,Y

upvoted 5 times

HOTSPOT

Your company has a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Security Administrator, Guest Inviter
User3	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

Suggested 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 1 year, 3 months ago

1. Correct.
2. All users

<https://www.examttopics.com/discussions/microsoft/view/50897-exam-ms-100-topic-3-question-79-discussion/>
upvoted 13 times

aleksdj 1 year, 1 month ago



The first one is wrong, it is users 1 and 2 for sure!
upvoted 6 times

siulas 1 year, 3 months ago

1. User1 and User2 only

2. All users

upvoted 25 times

  **cb0900** 1 year, 3 months ago

Agree:

1. User 1 and User 2

2. All users

Tested in a lab.

upvoted 5 times

  **Casticod** 1 year, 3 months ago

I think The same

1. User1 and User2 only

2. All users

upvoted 9 times

  **EEMS700** 1 year, 2 months ago

1. User1 and User2 only

2. All users

upvoted 8 times

  **Frank9020** Most Recent 1 month, 2 weeks ago

Correct answers:

1: -User1 only - Global Administrator

2: -User1 & User2 - Global Administrator + Guest Inviter


upvoted 2 times

  **ct1984** 3 months ago

To modify the password protection policy you need Authentication Policy Administrator role. That is not available here, so here it's USER1, Global Administrator.

To CREATE (not invite) guest users in this exercise, it's Global administrator and Guest Inviter roles that apply. So User 1 and User 2.

upvoted 2 times

  **radamelca** 3 months, 1 week ago

1- User 1 and User 2

2- User 1 and User 2

Question is about CREATE guest users, not INVITE guest users.

upvoted 1 times

  **APK1** 4 months, 2 weeks ago

Inviting guest through B2B is different than inviting or creating guest to AZURE AD or ENTRA.

A role that allows you to create users in your tenant directory, such as at least a Guest Inviter role or a User Administrator. Create a guest, admin will be manually created with the required actions.

Question specifically asked for "Create guest user in Azure AD", so as per the scenario

User1 (Global Admin) and User2 (Security Admin with guest inviter role is the correct answer

So, the conclusion is

Box1: User1 and User2


Box2: User1 and User2

upvoted 2 times

  **wael_kodmani** 4 months, 2 weeks ago

the question is create a guest not invite a guest!! there is a difference between them, invite a guest by using B2B, and the guest will receive an invitation. Create a guest admin will be manually created with the required actions

upvoted 1 times

  **Khanbaba43** 4 months, 2 weeks ago

There is no option of creating guests. Safe to assume, creating guests means inviting guests!

upvoted 3 times

🗨️ 👤 **Khanbaba43** 4 months, 2 weeks ago

Nevermind my response above. I misread the question.

upvoted 1 times

🗨️ 👤 **Jamesat** 8 months, 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 3 times

🗨️ 👤 **TonyManero** 8 months, 3 weeks 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** 1 year 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** 1 year ago

1. User1 & User2(Tested)

upvoted 1 times

🗨️ 👤 **Festus365** 1 year 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** 1 year, 1 month 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** 11 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 2 times

🗨️ 👤 **5e0d3df** 11 months 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 2 times

🗨️ 👤 **imlearningstuffagain** 1 year, 2 months 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-](https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions?context=%2Fazure%2Factive-directory%2Froles%2Fcontext%2Fugr-context#compare-member-and-guest-default-permissions)

[directory%2Froles%2Fcontext%2Fugr-context#compare-member-and-guest-default-permissions](https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions?context=%2Fazure%2Factive-directory%2Froles%2Fcontext%2Fugr-context#compare-member-and-guest-default-permissions)

So answer should be: Users 1, 2 3,4

upvoted 1 times



🗨️ 👤 **rfree** 1 year, 3 months ago

2. am thinking Users 1, 2 and 4 as 3 has no roles.

A role that allows you to create users in your tenant directory, such as the Global Administrator role or a limited administrator directory role such as Guest Inviter or User Administrator.

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal>

upvoted 1 times

  **JensV** 1 year, 3 months 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

  **Casticod** 1 year, 3 months ago

Try in my lab tenant, Standard user (not assigned rol) to be able to create a Guest user.

upvoted 2 times

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

Name	Microsoft 365 admin role	Microsoft Exchange Online admin role
User1	Global Administrator	None
User2	Exchange Administrator	None
User3	Service Support Administrator	None
User4	None	Organization Management

You plan to use Exchange Online to manage email for a DNS domain.

An administrator adds the DNS domain to the subscription.


The DNS domain has a status of Incomplete setup.

You need to identify which user can complete the setup of the DNS domain. The solution must use the principle of least privilege.

Which user should you identify?


- A. User1
- B. User2
- C. User3
- D. User4

Suggested Answer: A

 **sigvast** Highly Voted 1 month, 2 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 5 times

 **8b43f56** Most Recent 3 weeks, 1 day ago
Selected Answer: D


Answer is D: User4.

Organization management role can complete the setup of the DNS domain.

<https://learn.microsoft.com/en-us/exchange/permissions-exo/permissions-exo>
upvoted 1 times

 **Greatone1** 2 months, 3 weeks ago
Given answer is correct

<https://www.examttopics.com/discussions/microsoft/view/55314-exam-ms-100-topic-3-question-76-discussion/>
upvoted 1 times

 **[Removed]** 3 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.


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


Suggested Answer: C

Community vote distribution


C (100%)

 **Vincent1966** Highly Voted 1 year, 3 months 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 10 times

 **Vaerox** 11 months, 1 week ago


So the answer is D? Both User 1 and User 3?
upvoted 1 times

 **Big076** 4 weeks ago

therefore its C: User1 Mobile/Cell Phone & Email is not supported for GPS location and GPS location doesn't work with passwordless authentication
upvoted 1 times

 **basak** 7 months, 3 weeks ago

Mobile Phone may be used for SMS service
upvoted 2 times

 **Frank9020** Most Recent 1 month, 2 weeks ago

Selected Answer: B

User1: Uses MFA with the Microsoft Authenticator app (push notification), which supports GPS-based conditions.
User2: Uses passwordless authentication with MFA push notifications enabled, which supports GPS-based conditions.
User3: Uses MFA with a mobile phone, which supports GPS-based conditions.
User4: Uses MFA with email, which supports GPS-based conditions.

GPS location can be used with passwordless phone sign-in only if MFA push notifications are also enabled.

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-assignment-network>

upvoted 1 times

 **APK1** 4 months, 3 weeks ago

Selected Answer: C

Ignore user2. From User1, User3, User4.
User4 is using email, User3 is using Mobile

upvoted 2 times

🗨️ 👤 **Tomtom11** 10 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 4 times

🗨️ 👤 **Amir1909** 11 months ago

C is correct

upvoted 2 times

🗨️ 👤 **Vaerox** 11 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

🗨️ 👤 **faem** 1 year, 3 months 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

HOTSPOT

-

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

Name	Member of	Role
User1	Group1	User Administrator
User2	Group1	None
User3	Group2	None
User4	None	Global Administrator

You enable self-service password reset (SSPR) for Group1. You configure security questions as the only authentication method for SSPR.

Which users can use SSPR, and which users must answer security questions to reset their password? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users that can use SSPR:

▼

- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

Users that must answer security questions to reset their password:

▼

- User1 only
- User2 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

Answer Area

Users that can use SSPR:

▼


- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

Suggested Answer:

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

 **Vincent1966** Highly Voted 1 year, 3 months 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 20 times

 **Frank9020** Most Recent 1 month, 2 weeks ago

Users who can use SSPR: User1, User2, and User4.

Users who must answer security questions to reset their password (under the Group1 policy): User2 only.

User1 and User4, as administrators, will follow the default two-gate policy, which does not include security questions.

upvoted 3 times

 **APK1** 4 months, 3 weeks ago

Box 1 = user1, user2, user4

Box 2 = user2

upvoted 2 times

🗨️ 👤 **Craig** 10 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** 8 months, 1 week 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** 1 year, 1 month ago

Agree with vincent, use entra / intune every day and 100% correct.

upvoted 2 times

🗨️ 👤 **vercracked_007** 1 year, 3 months 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 3 times

🗨️ 👤 **Vaerox** 11 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 2 times

🗨️ 👤 **Casticod** 1 year, 3 months 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 4 times

🗨️ 👤 **Casticod** 1 year, 3 months ago

Sorry error in the responses.

Option 1: User1, user2, and user4 (user 1 and 4 by admins, user 2 for group assignment)

Option 2: User 2 Only (the admins can't use the security Questions)

upvoted 8 times

🗨️ 👤 **Casticod** 1 year, 3 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** 1 year, 3 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.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **de0e20a** 2 months ago

This is a case of what is the Microsoft approved method versus what will work, Option D will work with out option C being put in place but its not the Microsoft approved method as is documented.

upvoted 1 times

🗨️ 👤 **DiligentSam** 9 months ago

Given Answer is correct

upvoted 2 times

🗨️ 👤 **spectre786** 9 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** 9 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 4 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

Suggested Answer: B

Community vote distribution

B (85%)

E (15%)

 **Demonster** Highly Voted 1 year, 3 months 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 17 times

 **Big076** 3 weeks, 5 days ago

Correct B. Atypical Travel and Unfamiliar Sign-In Properties rely on an established baseline
upvoted 1 times

 **Frank9020** Most Recent 1 month, 3 weeks ago

Selected Answer: E


E. anonymous IP address, atypical travel, and unfamiliar sign-in properties
upvoted 2 times

 **Amir1909** 11 months ago

- anonymous IP adress and atypical travel only
upvoted 2 times

 **benpatto** 1 year, 1 month 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** 1 year, 1 month 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 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** 1 year, 2 months 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 3 times

🗨️ 👤 **JensV** 1 year, 3 months 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** 1 year, 2 months 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

🗨️ 👤 **NrdAlrt** 1 year, 1 month 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 intentional 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** 1 year, 3 months 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** 1 year, 3 months ago

Should be A i think

upvoted 1 times

HOTSPOT

-

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

Name	Group	MFA Status
User1	Group1	Enabled
User2	Group1, Group2	Enforced

You have the named locations shown in the following table.

Named location	IP range
Montreal	133.107.0.0/16
Toronto	193.77.10.0/24

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

- Users or workload identities:
 - Include: Group1
 - Exclude: Group2
- Cloud apps or actions: Include all cloud apps
- Conditions:
 - Include: Any location
 - Exclude: Montreal
- Access control: Grant access, Require multi-factor authentication

User1 is on the multi-factor authentication (MFA) blocked users list.

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

NOTE: Each correct selection is worth one point.

Answer Area


Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	<input type="radio"/>	<input type="radio"/>
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	<input type="radio"/>	<input type="radio"/>

Suggested Answer:

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 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"/>


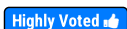
Y = User1 is on the MFA block list BUT IP range 133.107.10.20 is Montreal which is EXCLUDED from MFA so user1 can access
N = User1 is on the MFA block list AND IP range 193.77.10.15 is Toronto which is INCLUDED in MFA so User cannot access
Y = User2 is not in the MFA block list and and member of Group2 which is excluded from the conditional acces policy and therefore can access from 193.77.10.20 Toronto. User2 is even allowed to access M365 from Montreal because the policy is noit applied to User2.
upvoted 15 times

 **Motanel** 8 months, 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 4 times

 **2dwarf**  1 year, 1 month ago

I think it is NNY ,because MFA in not enforced by policy. When you are blocked with MFA you cannot sign in any way.
upvoted 11 times

 **Frank9020**  1 month, 2 weeks ago

NO: - User1 cannot access any cloud apps because User1 is on the MFA blocked users list, preventing them from completing the required MFA sign in.

NO: -User1 cannot access Microsoft Office 365 because User1 is blocked from completing MFA.


NO: -User2 is in Group1 and Group2. In conditional access the rule is that exclusions take precedence over inclusions, so User2 is not allowed to sign in being member of the exclusion group.

When there is a Conditional Access Policy with locations as we have here:

Excluded: Location Montreal: IP range 133.107.0.0/16. - The meaning of exclusion is that if you are in Montreal: - You are not allowed/blocked from signing in or accessing.

Included: Any Location - which includes Toronto: IP range 193.77.10.0/24, and many other locations they might have you are allowed to sign in with MFA, and you have to be in Group1 (included)

upvoted 1 times

 **Tr619899** 2 months, 2 weeks ago

User1 is in Group1, which is included in the conditional access policy. However, Montreal is an excluded location in the policy, and since the IP address 133.107.10.20 falls within the Montreal IP range, this location is excluded from the MFA requirement.

User1 is on the MFA blocked list, but since MFA is not required for this location, being blocked from MFA would not prevent access.

Answer: YES

The IP address 193.77.10.15 is from Toronto, which is not in the excluded location list. Therefore, MFA is required based on the policy.

Since User1 is on the MFA blocked list, they would not be able to complete the MFA process.


Answer: NO

User2 is in Group1 (included) and Group2 (excluded) in the conditional access policy. Since Group2 is excluded, User2 is not subject to this policy's conditions.

User2 can access Office 365 from any location, including the Toronto IP range (193.77.10.20), without being blocked by the policy.

Answer: YES

upvoted 2 times

 **3abmula** 1 month, 3 weeks ago

For first question, I think it should be NO.

Explanation: User1 MFA status is "Enabled", it means User1 still didn't complete MFA registration and will be prompted to register for MFA the next sign-in, which will not be able to do since he is on the MFA block list. Does that make any sense?

upvoted 1 times

 **Tomtom11** 4 months, 1 week ago

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

upvoted 1 times

 **APK1** 4 months, 2 weeks ago

NNY my choice

Once user blocked he is blocked everywhere irrespective of different IP.

Group 2 excluded for user2

upvoted 1 times

  **pali5178** 8 months ago

Statement 1: User1 can sign in to Microsoft SharePoint Online from Toronto.

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 2 times

  **DNGFORMA** 6 months, 2 weeks ago

I think your reply belong to Question 152 as there is no User 3 in this example

upvoted 3 times

  **de0e20a** 8 months ago

The issue here is that "Blocked MFA users List" according to Microsoft Learn is actually a report that says why a users 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 a 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** 11 months 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** 1 year ago

NNY

user MFA is enabled in lgeacy settings....

upvoted 4 times

🗨️ 👤 **itguys** 1 year ago

*legacy

upvoted 1 times

🗨️ 👤 **TP447** 1 year, 1 month ago

YNY is correct. User1 wouldnt trigger the CA Policy from Montreal due to the exclusion so would be granted access without requiring MFA.

upvoted 2 times

🗨️ 👤 **jt2214** 1 year, 1 month ago

I would assume since User 1 is on the blocked list they cannot access?

upvoted 3 times

🗨️ 👤 **rfree** 1 year, 2 months ago

YNY. 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

🗨️ 👤 **Darekms0** 1 year, 2 months ago

<https://www.examt0pics.com/discussions/microsoft/view/55435-exam-ms-100-topic-4-question-36-discussion/> NNY

upvoted 2 times

🗨️ 👤 **netbw** 1 year, 3 months ago

Answer is correct. User1 can connect from Montreal.

upvoted 1 times

🗨️ 👤 **BlackCat9588** 1 year, 3 months ago

NNY?

MFA of user1 is blocked

upvoted 4 times

🗨️ 👤 **BlackCat9588** 1 year, 3 months ago

Exclude: Montreal

upvoted 1 times

🗨️ 👤 **NrdAlrt** 1 year, 1 month 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

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



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	X
Group2	Group	Optional	Passwordless	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"/>

Answer Area

Suggested Answer:

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"/>

MarkusSan Highly Voted 1 year, 2 months ago

Answer look correct to me
upvoted 6 times

🗨️ 👤 **Big076** 3 weeks, 5 days ago

Correct...YES - User2 is in Group2, which is included in both the Conditional Access policy and the Authenticator app settings. Passwordless authentication is enforced due to the Conditional Access policy requiring MFA. User2 cannot bypass MFA using just a username and password.

No - User3 is in both Group1 and Group2, so they are included in the Conditional Access policy and the Authenticator settings.

However, User3 has not set up the Microsoft Authenticator app, making number matching unavailable.

No - User3 is in both Group1 and Group2, so they are included in the Conditional Access policy and the Authenticator settings.

However, User3 has not set up the Microsoft Authenticator app, making number matching unavailable.

upvoted 1 times

🗨️ 👤 **f0f4a76** Most Recent 3 months, 1 week ago

How can you say "everyone has -THE MICROSOFT AUTHENTICATOR- and -PHONE SIGN IN- But state in the above chart that USER 3 is not configured? Given answer seems correct if reviewing the top chart, but if reading the question its Y,N,Y. User 2 cannot because he needs to use his phone as required per Conditional Access. Regardless of setting up passwordless. Passwordless just means you get a phone popup with no password, The phone is required.

upvoted 2 times

🗨️ 👤 **APK1** 5 months ago

Thought user3 should be Yes, but found as no MFA configured. Answer YNN

upvoted 1 times

🗨️ 👤 **Murad01** 6 months ago

Given answers looks correct

upvoted 1 times

🗨️ 👤 **Scotte2023** 8 months, 1 week 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 username and password as usual, then you get prompted to enter your second factor to verify your identity.

<https://support.microsoft.com/en-gb/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661>

User2: It doesn't specify that they "only" enter a username and password? With passwordless MFA optional, I'd say User2 could sign in.

upvoted 2 times

🗨️ 👤 **saurekind** 8 months, 2 weeks ago

If all users have authenticator app, why can't user 3 use number matching?

upvoted 1 times

🗨️ 👤 **Khattak3143** 4 months, 3 weeks ago

User 3 does not have an authenticator app.

upvoted 1 times

🗨️ 👤 **Tomtom11** 8 months, 4 weeks ago

<https://learn.microsoft.com/en-ie/entra/identity/authentication/howto-authentication-passwordless-phone>

Recommended: Microsoft Entra multifactor authentication, with push notifications allowed as a verification method. Push notifications to your smartphone or tablet help the Authenticator app to prevent unauthorized access to accounts and stop fraudulent transactions. The Authenticator app automatically generates codes when set up to do push notifications. A user has a backup sign-in method even if their device doesn't have connectivity.

upvoted 1 times

🗨️ 👤 **Harau** 1 year, 2 months ago

YYN

User 2 can use username and password, since passwordless is optional

upvoted 1 times

🗨️ 👤 **MarkusSan** 1 year, 2 months ago

User 2 cannot use username and password only, because of Conditional Access Policy 1: Grant, require MFA for Group1 and Group2

upvoted 11 times

HOTSPOT

You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Report Reader
User2	User Administrator
User3	Security Administrator
User4	Global Administrator

From the Sign-ins blade of the Microsoft Entra admin center, for which users can User1 and User2 view the sign-ins? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1 can view the sign-ins for the following users:

▼

- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

User2 can view the sign-ins for the following users:

▼

- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Suggested Answer:

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

 **cb0900** Highly Voted 1 year, 3 months 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.examttopics.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 15 times

 **NrdAlrt** 1 year, 1 month 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 6 times

 **Frank9020** Most Recent 1 month, 3 weeks ago

Given answers are correct

upvoted 2 times

 **Frank9020** 1 month, 3 weeks ago

User1 - can only see sign in for User1

User2 - can see sign in for User1 and User2

upvoted 1 times

🗨️ 👤 **Frank9020** 1 month, 3 weeks ago

User1 (Reports Reader) can view the sign-in logs for themselves and standard users (non-administrators), but not for any administrator roles (like User2, User3, or User4).

User2 (User Administrator) can view the sign-in logs for themselves (User2), User1 (Reports Reader), and standard users, but cannot view the sign-ins for other administrators (like User3 (Security Administrator) or User4 (Global Administrator)).

upvoted 1 times

🗨️ 👤 **APK1** 4 months, 2 weeks ago

Following users can see the sign in for part one

Global administrator

Security administrator

Security reader

Global reader

Report reader

For part2 - Only User Admin (user admin can only see his/her sign-ins)

upvoted 2 times

🗨️ 👤 **Khattak3143** 4 months, 3 weeks ago

User1: Can view sign-in activities for all.

User2: Can only see user 2's sign-in activity.

Not sure why there isn't a 5th option, unless there's something I'm missing??

upvoted 2 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.

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **Frank9020** 1 month, 3 weeks ago

Selected Answer: B

Is correct

upvoted 1 times

🗨️ 👤 **TonyManero** 8 months, 3 weeks ago

Selected Answer: B

Correct

upvoted 2 times

🗨️ 👤 **DiligentSam** 1 year, 3 months ago

<https://www.examttopics.com/discussions/microsoft/view/45311-exam-ms-100-topic-3-question-66-discussion/>

upvoted 4 times

🗨️ 👤 **GLL** 1 year, 3 months ago

correct

upvoted 1 times

🗨️ 👤 **CloudCanary** 1 year, 3 months 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


Suggested Answer: B

Community vote distribution

B (100%)

 **Festus365** Highly Voted 1 year, 1 month ago

Answer is NO! B: because Active directory is unavailable for Pass through authentication.
upvoted 8 times

 **momowagdy** 8 months, 2 weeks 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

 **APK1** Most Recent 4 months, 3 weeks ago

Selected Answer: B
It should be PHS for A, if PTA then correct answer is B
upvoted 2 times

 **Paul_white** 1 year, 2 months ago

ANSWER IS B !!!!!
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.

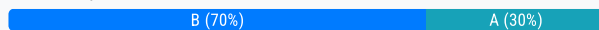
Solution: Implement password hash synchronization and configure password protection in the Azure AD tenant.

Does this meet the goal?

- A. Yes
- B. No

Suggested Answer: B

Community vote distribution



BSVIT Highly Voted 1 year, 1 month 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 19 times

e201546 7 months ago

Thanks for explaining that, it helps with more questions

upvoted 1 times

Hard1k Highly Voted 1 year, 3 months 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 12 times

  **Frippy** 1 year ago


There is no "minimum length and complexity" in AzureAD

upvoted 3 times

  **Milad666** 1 year, 2 months ago

WRONG! User that synchronized with PHS will just inherit Policies and attributes from Active Directory. So Solution doesnt meet the goal.

upvoted 14 times


  **EEMS700** 1 year, 1 month ago

I agree with Milad

Policies they will be used are from Active Directory

Correct answer is B

upvoted 4 times

  **Frank9020** Most Recent 1 month, 2 weeks ago

Selected Answer: A

Correct answer is A.

Password hash synchronization allows users to authenticate to Microsoft 365 services even if the on-premises Active Directory becomes unavailable, as the authentication is handled by Azure AD1. Additionally, configuring password protection in the Azure AD tenant ensures that user passwords meet the required complexity, such as being 10 characters or more2.

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/prepare-for-directory-synchronization?view=o365-worldwide>



<https://learn.microsoft.com/en-us/microsoft-365/enterprise/set-up-directory-synchronization?view=o365-worldwide>

upvoted 1 times

  **ExamCheater1993** 6 months, 3 weeks ago

Question 158,. Solution: Implement password hash synchronization and modify the password settings from the Default Domain Policy in Active Directory.



upvoted 2 times

  **oopspruu** 8 months, 1 week ago

Selected Answer: B

The solution doesn't satisfy the 2nd requirement. The password policies needs to be enforced in on-prem AD if PHS is used. With PHS, AD password policies always override AAD password policies.



upvoted 2 times

  **CharlesS76** 8 months, 4 weeks ago

Selected Answer: B

Password policies that will be used are from Active Directory...



upvoted 1 times

  **Tomtom11** 8 months, 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** 8 months, 4 weeks ago

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad-combined-policy>

upvoted 1 times

🗨️ 👤 **Tomtom11** 8 months, 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** 10 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** 10 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** 11 months 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** 11 months ago

Selected Answer: B

the given scenario is about synchronizing users from on-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** 11 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** 1 year, 1 month ago

Selected Answer: B

Correct Answer B

upvoted 1 times

🗨️ 👤 **Festus365** 1 year, 1 month 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** 1 year, 1 month 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

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

Suggested Answer: B

Community vote distribution

B (100%)

 **EEMS700** 1 month, 3 weeks ago

Selected Answer: B

Correct

pass-through will not work if AD is down.

upvoted 3 times

 **imlearningstuffagain** 2 months, 1 week 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

Suggested Answer: A

Community vote distribution

A (100%)

 **Frank9020** 1 month, 2 weeks ago

Selected Answer: B

While password hash synchronization allows users to authenticate to Microsoft 365 services if Active Directory becomes unavailable, modifying the password settings from the Default Domain Policy in Active Directory DOES NOT ensure that the password policy is enforced in Entra ID. The password length requirement should be configured in Entra ID to ensure it applies to synchronized identities.

upvoted 1 times

 **LiamAzure** 6 months ago

Selected Answer: A

A, Synchronization lets you reset from 365

upvoted 1 times

 **Fran22** 10 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 3 times

 **PhoenixMan** 1 year, 1 month ago

Correct answer I had the question in today exam

upvoted 1 times

 **EEMS700** 1 year, 1 month ago

Selected Answer: A

Answer is correct

upvoted 3 times

 **Vincent1966** 1 year, 3 months 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

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:

Configure Azure AD Connect Health settings:

Answer Area

Suggested Answer:

View sync errors in Azure AD Connect Health:

Configure Azure AD Connect Health settings:

🗨️ **cb0900** Highly Voted 1 year, 3 months ago

View sync errors - user 2

Configure AADConnect - user 2

<https://www.examttopics.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 33 times

🗨️ **imlearningstuffagain** 1 year, 2 months ago

Source at Microsoft Site.

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-health-operations#roles>

upvoted 4 times

🗨️ **br99mlpt** Most Recent 2 months, 1 week ago

I think user 2 for both

upvoted 2 times

🗨️ **cc780eb** 2 months, 3 weeks ago

From my point of view, the answer is user 2 for both

upvoted 1 times

🗨️ **Fran22** 10 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** 11 months, 4 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** 1 year ago

View sync errors = User 1(Azure AD connect sync account)

Configure AADConnect health settings = User 2(Role: Contributor)

upvoted 1 times

🗨️ **NrdAlrt** 1 year, 1 month 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. It's 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

Suggested Answer: D

Community vote distribution

D (100%)

APK1 4 months, 3 weeks ago

Selected Answer: D

Answer D

upvoted 1 times

TonyManero 8 months, 1 week ago

Selected Answer: D

In a conditional access policy you can set a location

upvoted 1 times

DiligentSam 1 year, 2 months ago

correct

upvoted 1 times

Paul_white 1 year, 2 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

Suggested Answer: B

Community vote distribution

A (100%)

🗨️ **dado11** 3 months, 1 week ago

it's Yes

upvoted 2 times

🗨️ **Khattak3143** 4 months, 3 weeks ago

Selected Answer: A

Dear Admin please process APK1's request.

A final answer!

upvoted 1 times

🗨️ **APK1** 4 months, 3 weeks ago

Selected Answer: A

Dear Admin,

Please correct the answer as A

upvoted 2 times

🗨️ **oopspruu** 8 months, 1 week 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** 10 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

🗨️ **SBG12** 12 months 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** 1 year, 1 month ago

Selected Answer: A

Would agree with A

upvoted 2 times

🗨️ **NrdAlrt** 1 year, 1 month ago

Selected Answer: A

Just realized filters are also considered the part where you pick OU's. Oops. A it is.

upvoted 3 times

🗨️ **NrdAlrt** 1 year, 1 month 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** 1 year, 1 month ago

I meant B.

upvoted 1 times

🗨️ **jt2214** 1 year, 2 months ago

Selected Answer: A

<https://www.examttopics.com/discussions/microsoft/view/59313-exam-ms-100-topic-3-question-22-discussion/>

upvoted 2 times

🗨️ **Paul_white** 1 year, 2 months ago

ANSWER IS A !!!!!

upvoted 1 times

🗨️ **Sas2003** 1 year, 3 months ago

Selected Answer: A

No error just remove filtering or U exclusion

upvoted 4 times

🗨️ **jakke91** 1 year, 3 months ago

A indeed

<https://www.examttopics.com/discussions/microsoft/view/59313-exam-ms-100-topic-3-question-22-discussion/>

upvoted 2 times

🗨️ **vercracked_007** 1 year, 3 months ago

Should this not 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	<input type="text" value="Search this list"/>	
<input type="checkbox"/>	Members	Email address	Last sign-in	Member type		
<input type="checkbox"/>	User1	User1@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:25 PM	User		
<input type="checkbox"/>	User3	User3@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:27 PM	User		

The User Administrator role has the assignments shown in the following exhibit.

User Administrator


▶ Run As

General **Assigned** Permissions

You can assign this role to users and groups, and select users and groups to remove or manage them.

[Learn more about assigning admin roles](#)

 Add users  Add groups

<input type="checkbox"/>	Admin name	Last sign-in	Scope 
<input type="checkbox"/>	Group1	Unavailable for groups	Organization
<input type="checkbox"/>	Group2	Unavailable for groups	AU1

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

NOTE: Each correct selection is worth one point.

Answer Area

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

Answer Area

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

Suggested Answer:

 **aleksdj** Highly Voted 7 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