

SC-300 Microsoft Identity and Access Administrator

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

You have an Azure Active Directory (Azure AD) tenant that contains the following objects:

- A device named Device1
- Users named User1, User2, User3, User4, and User5
- Groups named Group1, Group2, Group3, Group4, and Group5

The groups are configured as shown in the following table.

Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group3
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Dynamic User	User5

To which groups can you assign a Microsoft Office 365 Enterprise E5 license directly?

- A. Group1 and Group4 only
- B. Group1, Group2, Group3, Group4, and Group5
- C. Group1 and Group2 only
- D. Group1 only
- E. Group1, Group2, Group4, and Group5 only

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>

Community vote distribution

B (51%) E (25%) C (24%)

✉  **sezza_blunt**  2 years, 5 months ago

There is not enough information in the question to provide a 100% correct answer. You can assign licences to any group created within the Azure AD portal. These can include security groups, Microsoft 365 groups, and either assigned or dynamic groups. You can even create a dynamic device security group and assign E5 licences to it, which doesn't make sense but is true (I've tested it).

However, the missing bit of information is whether the Microsoft 365 groups have the "SecurityEnabled" attribute set to True. Only M365 groups that have the "SecurityEnabled" attribute set to True can have licences assigned to them. If the group is created in the M365 Admin Centre, then the "SecurityEnabled" attribute is set to False and you can not assign licences to the group. But if the M365 group is created in the Azure AD portal, then the "SecurityEnabled" attribute is set to True and you can assign licences.

For the answer, I would make an assumption that because this is an Identity-related exam testing us on Azure AD topics, that the M365 groups were created in the Azure AD portal and therefore have the "SecurityEnabled" attribute set to True. Which means the correct answer is B - all groups.

upvoted 74 times

✉  **Leon1969** 2 months, 1 week ago

B is correct. The feature can be used with security groups, and Microsoft 365 groups that have securityEnabled = TRUE.
<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>

upvoted 2 times

✉  **JimboJones99** 1 month, 2 weeks ago

For anyone looking, this is in the Limitations and known issues section of the MS article Leon1969 posted
upvoted 1 times

✉  **jack987** 11 months, 2 weeks ago

I agree, the correct answer is B - all groups.

upvoted 3 times

✉  **HarishArul** 11 months, 2 weeks ago

No C is the right answer. You can assign licenses only to the Security Group, not Microsoft 365 Group. And Group 3 consists of a Device, not users. Only users can have a license, not a device. Microsoft 365 Group is basically used for shared mailboxes, which will only be possible if you already have a license. So Group 1 and Group 2 only can be assigned licenses.

upvoted 18 times

✉  **jack987** 11 months, 1 week ago

You're right. I just tested it in our environment. The license option won't show for Microsoft 365 Groups.
The correct answer is C.

Use group-based licensing with dynamic groups

You can use group-based licensing with any security group, which means it can be combined with Azure AD dynamic groups.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>

upvoted 11 times

□ **KrisDeb** 1 year ago

I agree with you, all groups but with the exception of M365 groups created in M365 Admin Center. The question should be more specific, especially that we are supposed to become the ACCESS and IDENTITY specialists with attention to detail...

upvoted 2 times

□ **someonehad** 2 years, 5 months ago

I agree, answer B is correct, here you can find info about group device licensing requirements: <https://docs.microsoft.com/en-us/deployoffice/device-based-licensing#steps-to-configure-device-based-licensing-for-microsoft-365-apps-for-enterprise>

Security, with dynamic device membership is supported.

upvoted 6 times

□ **eufdf12342** 2 years ago

I agree too, answer B

upvoted 2 times

□ **Beitran** **Highly Voted** 2 years, 7 months ago

Wrong, you can assign licenses to Microsoft 365 groups as well. The correct answer is E

upvoted 19 times

□ **Shaz** 2 years, 7 months ago

The answer is correct, there's only the two groups *users not devices* that marked as security.

upvoted 7 times

□ **Borbz** 2 years, 5 months ago

By default, M365 groups are marked as SecurityEnabled=True so they are considered security groups as well. therefore I think "Beitran" is correct and the answer is E.

upvoted 6 times

□ **researched_answer_boi** 2 years, 2 months ago

Correct, E

<https://docs.microsoft.com/en-us/graph/api/group-post-groups?view=graph-rest-1.0&tabs=http>

Set to true for security-enabled groups, including Microsoft 365 groups. Required. Note: Groups created using the Microsoft Azure portal always have securityEnabled initially set to true.

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>

The feature can only be used with security groups, and Microsoft 365 groups that have securityEnabled=TRUE.

upvoted 4 times

□ **Bulldozer** 1 year, 9 months ago

It is not possible to assign a license to an M365 group because this is not supported and neither are mail-enabled security groups.

upvoted 2 times

□ **J4U** 2 years, 1 month ago

Why can't it be Group 3 for answer B. The license assignment to groups is irrespective of group membership and can be assigned to any type of security groups.

upvoted 3 times

□ **kijken** **Most Recent** 3 weeks, 4 days ago

Selected Answer: B

I mean B

upvoted 1 times

□ **kijken** 3 weeks, 4 days ago

Selected Answer: C

The best way to test this question is to make a dynamic device sec group and assign a license.

I did this and it is possible, so the answer is C

upvoted 1 times

□ **kijken** 3 weeks, 2 days ago

I mean B of course. I wrote this in a separate message, but just to make sure I will put it here in a reply aswell

upvoted 1 times

□ **kijken** 1 month ago

Alot is unclear in this question.

I assume portal.azure.com interface is used.

I could not do it through Microsoft 365 portal, but I can do it with portal.azure.com interface and then azure ad.

Besides of that you need a P1 or P2 license.

Assuming that is the case aswell then answer would be B

upvoted 1 times

□ **Softeng** 2 months, 1 week ago

Selected Answer: B

Agree with sezza_blunt.

Link to documentation:

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced#:~:text=The%20feature%20can%20only%20be%20used%20with%20security%20groups%2C%20and%20Microsoft%20365%20groups%20that%20have%20securityEnabled%3DTRUE>

upvoted 2 times

 **sherifhamed** 2 months, 1 week ago

Selected Answer: B

In Microsoft Office 365, you can assign licenses directly to individual users or to groups. You can assign Microsoft Office 365 Enterprise licenses directly to the following groups:

Security Groups:

Distribution Lists (Mail-Enabled Groups)

Office 365 Groups (Microsoft 365 Groups)

Azure AD Groups: Azure Active Directory (Azure AD) groups can also be used for license assignment in Office 365. Assigning licenses to Azure AD groups works similarly to security groups.

Dynamic Distribution Lists: You can also use dynamic distribution lists based on user attributes to assign licenses automatically to users who meet specific criteria.

upvoted 2 times

 **Rhaider** 3 months ago

Selected Answer: B

I tested this and answer is B All groups can be assigned as long as it is created in Azure AD portal (Entra)

upvoted 4 times

 **syougun200x** 3 months ago

B (all the groups mentioned) is the answer. I tested on my test tenant.

Some people read into details too much. But I would answer simply to this question. When attempting to either of those groups, nothing blocks to assign a license.

upvoted 1 times

 **Logitech** 3 months, 1 week ago

Tested it, i can assigne it to all groups, but only M365 groups if i created theme in Azure Ad.

upvoted 1 times

 **JackLash96** 3 months, 3 weeks ago

I've tested this in a Azure environment. Whilst it is possible to assign licenses to all the groups here. I have no idea why you'd assign an O365 E5 license to a device but it is technically possible so B is Correct

upvoted 2 times

 **EmnCours** 3 months, 4 weeks ago

Selected Answer: B

the correct answer is B - all groups.

upvoted 3 times

 **RahulX** 4 months ago

Correct Ans: C (Group 1 and Group 2). You can assign licenses only to the Security Group, not Microsoft 365 Group.

upvoted 1 times

 **dule27** 5 months ago

Selected Answer: B

B. Group1, Group2, Group3, Group4, and Group5

upvoted 4 times

 **Tweety1972** 5 months ago

Can you explain please?

upvoted 2 times

 **dule27** 5 months ago

You can assign licences to any group created within the Azure AD portal. These can include security groups, Microsoft 365 groups, and either assigned or dynamic groups. You can even create a dynamic device security group and assign E5 licences to it, which doesn't make sense but is true (I've tested it).

upvoted 1 times

 **b233f0a** 5 months, 1 week ago

Selected Answer: B

All groups created via Azure Portal is the correct answer. Device groups can be assigned Microsoft 365 Apps for enterprise license so that it also a valid answer.

upvoted 2 times

 **kukushka** 6 months, 2 weeks ago

Selected Answer: B

B - all groups
upvoted 3 times

 **ShoaibPKDXB** 6 months, 3 weeks ago

Selected Answer: E

E is correct
upvoted 3 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

You have a Microsoft Exchange organization that uses an SMTP address space of contoso.com. Several users use their contoso.com email address for self-service sign-up to Azure Active Directory (Azure AD). You gain global administrator privileges to the Azure AD tenant that contains the self-signed users. You need to prevent the users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services.

Which PowerShell cmdlet should you run?

- A. Set-MsolCompanySettings
- B. Set-MsolDomainFederationSettings
- C. Update-MsolFederatedDomain
- D. Set-MsolDomain

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup>

Community vote distribution

A (100%)

✉  **julioglez88** Highly Voted 2 years, 5 months ago

The correct answer is A

As reference, Self-service sign-up: Method by which a user signs up for a cloud service and has an identity automatically created for them in Azure AD based on their email domain.

Azure AD cmdlet Set-MsolCompanySettings could help you to prevent creating user accounts with parameters:

AllowEmailVerifiedUsers (users can join the tenant by email validation)-->when is TRUE.

AllowAdHocSubscriptions (controls the ability for users to perform self-service sign-up)

e.g. Set-MsolCompanySettings -AllowEmailVerifiedUsers \$false -AllowAdHocSubscriptions \$false

upvoted 28 times

✉  **RahulX** Most Recent 6 days, 16 hours ago

A. Set-MsolCompanySettings.

upvoted 1 times

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

Selected Answer: A

The correct answer is A. Set-MsolCompanySettings.

To prevent users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services, you need to run the Set-MsolCompanySettings cmdlet with the -AllowAdHocSubscriptions parameter set to \$false. This will disable all self-service sign-ups for all Microsoft cloud-based apps and services in the contoso.com Azure AD tenant

upvoted 1 times

✉  **EmnCours** 4 months, 2 weeks ago

Selected Answer: A

A. Set-MsolCompanySettings

upvoted 1 times

✉  **dule27** 6 months, 2 weeks ago

Selected Answer: A

A. Set-MsolCompanySettings

upvoted 1 times

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

Selected Answer: A

The correct answer is A

upvoted 1 times

✉  **jack987** 11 months, 2 weeks ago

The correct answer is A.

upvoted 1 times

✉  **[Removed]** 12 months ago

Selected Answer: A

Answer is A. Set-MsolCompanySettings is the correct answer as per Microsoft documentation. <https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup#how-do-the-controls-work-together>

upvoted 1 times

□ **KrisDeb** 1 year ago

Selected Answer: A

<https://learn.microsoft.com/en-us/powershell/module/msonline/set-msolcompanysettings?view=azureadps-1.0>

upvoted 1 times

□ **den5_pepito83** 1 year ago

ON EXAM 14/11/2022

upvoted 2 times

□ **clem24** 1 year, 6 months ago

o control whether users can sign up for self-service subscriptions, use the Set-MsolCompanySettings PowerShell cmdlet with the AllowAdHocSubscriptions parameter

<https://docs.microsoft.com/en-us/microsoft-365/admin/misc/self-service-sign-up?view=o365-worldwide>

upvoted 2 times

□ **DemekeA** 1 year, 7 months ago

You can use group-based licensing with any security group, which means it can be combined with Azure AD dynamic groups. The feature can only be used with security groups, and Microsoft 365 groups that have securityEnabled=TRUE.

upvoted 2 times

□ **Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022

upvoted 2 times

□ **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 3 times

□ **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022.

upvoted 3 times

□ **xurxosan** 1 year, 9 months ago

Selected Answer: A

A is correct

upvoted 2 times

□ **stromnessian** 1 year, 9 months ago

Selected Answer: A

A is correct.

upvoted 2 times

You have a Microsoft 365 tenant that uses the domain named fabrikam.com. The Guest invite settings for Azure Active Directory (Azure AD) are configured as shown in the exhibit. (Click the Exhibit tab.)

Guest user access

Guest user access restrictions (Preview) ⓘ

[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

Admins and users in the guest inviter role can invite ⓘ

Yes No

Members can invite ⓘ

Yes No

Guests can invite ⓘ

Yes No

Email One-Time Passcode for guests ⓘ

[Learn more](#)

Yes No

Enable guest self-service sign up via user flows (Preview) ⓘ

[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)

A user named bsmith@fabrikam.com shares a Microsoft SharePoint Online document library to the users shown in the following table.

Name	Email	Description
User1	User1@contoso.com	A guest user in fabrikam.com
User2	User2@outlook.com	A user who has never accessed resources in fabrikam.com
User3	User3@fabrikam.com	A user in fabrikam.com

Which users will be emailed a passcode?

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

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode>

Community vote distribution

A (52%)

B (40%)

8%

 **Eltooth**  2 years, 6 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode#when-does-a-guest-user-get-a-one-time-passcode>

"When the email one-time passcode feature is enabled, newly invited users who meet certain conditions will use one-time passcode authentication. Guest users who redeemed an invitation before email one-time passcode was enabled will continue to use their same authentication method."

User 1 is already a registered guest user in fabrikan.com so will not receive additional OTP.
User 2 has never accessed fabrikam.com so WILL receive OTP each time they login.
User 3 (providing email addy is not a typo) will not receive a OTP as they are a domain user.

Answer is A.

upvoted 67 times

□ **pheb** 2 years, 3 months ago

idk why this has so many upvotes. it clearly states in the link you provided, that the user won't get OTP, if they have a microsoft account. User 2 has the domain "outlook.com". user 3 is a domain user and therefore won't receive an OTP. But User 1 (at least it does not say so anywhere) does not have a microsoft account, an azure ad account or a federation with another IP. he will always use OTP to authenticate not only once. so it has to be B.

upvoted 34 times

□ **JN_311** 5 months, 2 weeks ago

I agree, Answer should B. Reference Article: <https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode#when-does-a-guest-user-get-a-one-time-passcode>

upvoted 1 times

□ **wooyourdaddy** 10 months, 2 weeks ago

The link also contains this:

What happens to my existing guest users if I enable email one-time passcode?

Your existing guest users won't be affected if you enable email one-time passcode, as your existing users are already past the point of redemption. Enabling email one-time passcode will only affect future redemption activities where new guest users are redeeming into the tenant.

upvoted 1 times

□ **Holii** 5 months, 3 weeks ago

This is assuming you didn't already have these settings configured when you invited the guest accounts. It says no where in the question that they didn't already have these settings in place.

Seeing as how the default is to have OTP enabled for guest users, I would assume this activity is as Pheb suggests.

upvoted 1 times

□ **Kiano** 1 year, 6 months ago

Just because you have an Outlook.com account does not mean you have a Microsoft account. A Microsoft account is the account you associate with microsoft services at the time of need. It can be a gmail account or any kind of private account. I believe the right answer is A, Users2 only. Exactly as explained by Eltooth

upvoted 5 times

□ **itismadu** 11 months, 2 weeks ago

After reading the article and googling what is qualified as a Microsoft account, I agree with @pheb.

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode#when-does-a-guest-user-get-a-one-time-passcode>

upvoted 3 times

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

The answer should be B.

One-time passcodes are valid for 30 minutes. After 30 minutes, that specific one-time passcode is no longer valid, and the user must request a new one. User sessions expire after 24 hours. After that time, the guest user receives a new passcode when they access the resource. Session expiration provides added security, especially when a guest user leaves their company or no longer needs access.

upvoted 1 times

□ **jack987** 11 months, 2 weeks ago

I agree the correct answer is A.

upvoted 1 times

□ **Beitran** Highly Voted 2 years, 7 months ago

Uh, the conditions are:

They do not have an Azure AD account

They do not have a Microsoft account

The inviting tenant did not set up Google federation for @gmail.com and @googlemail.com users

So arguably none? Since User 1 has an AAD account, user 2 has a Microsoft account and User 3 has an AAD account as well.

upvoted 13 times

□ **asturmark** 1 year, 9 months ago

I agree with you. According to this question the answer should be "none". As someone else mentioned the answer option has been changed in the exam. The user3 now has a gmail account. In that case user3 will be the only one getting the one-time passcode.

upvoted 6 times

□ **lahl** 1 month, 1 week ago

yes, that's true! User3 has a Gmail account in the exam!

upvoted 1 times

□ **Jhill777** 1 year ago

As of 11-21-2022, I had to create a MSFT for my user@gmail.com in order to log in. No OTP required after that. Answer should be none without Google Federation.

upvoted 1 times

✉ **Jhill777** 1 year ago

MSFT account for my gmail.com account was then changed to @outlook.com, just to be clear.

upvoted 1 times

✉ **Reyain** 2 years, 7 months ago

just to clarify your absolutely valid comment, above are the conditions when a one-time passcode would be sent to a user according to the linked MS documentation. it does in fact require "negative" conditions to apply.

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode>

upvoted 2 times

✉ **xm3000** 2 years, 5 months ago

agree with you, checked out the example section under <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode#when-does-a-guest-user-get-a-one-time-passcode>

"Guest user teri@gmail.com is invited to Fabrikam, which does not have Google federation set up. Teri does not have a Microsoft account. They'll receive a one-time passcode for authentication."

upvoted 3 times

✉ **RahulX** Most Recent 6 days, 16 hours ago

User 2 will receive OTP each time for login.

upvoted 1 times

✉ **virgilpz** 1 week ago

Selected Answer: B

as per <https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode#when-does-a-guest-user-get-a-one-time-passcode>

I believe the answer to be B

upvoted 1 times

✉ **kijken** 3 weeks, 4 days ago

Selected Answer: B

outlook.com = Microsoft account and account is authenticated by MS

3rd option is member of MS Entra ID tenant itself

Contoso.com is the only option left. This can be an on prem environment for example that cannot be authenticated by MS or the own tenant.

So the answer is B

upvoted 1 times

✉ **Nyamnyam** 4 weeks, 1 day ago

Selected Answer: B

The reference is clear OTP is NOT sent to MSA accounts (aka not to Outlook.com = User2) accounts. The fact the user1 (from contoso.com) is invited as guest does NOT make him automatically Microsoft Entra account. Sorry, I know this was unfair question.

upvoted 1 times

✉ **VirtualJP** 1 month, 2 weeks ago

Selected Answer: B

I'm thinking User1.

<https://learn.microsoft.com/en-gb/azure/active-directory/external-identities/one-time-passcode>

upvoted 1 times

✉ **Softeng** 2 months, 1 week ago

Selected Answer: A

Answer is A. Just read the documentation.

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode#when-does-a-guest-user-get-a-one-time-passcode>

upvoted 2 times

✉ **marcoby** 2 months, 1 week ago

The answer should be A, User 2 only. The article linked to the answer states:

When does a guest user get a one-time passcode?

When a guest user redeems an invitation or uses a link to a resource that has been shared with them, they'll receive a one-time passcode if:

They don't have a Microsoft Entra account. (User 3 does because they are in the domain.)

They don't have a Microsoft account. (User3 does because they are in the domain.)

The inviting tenant didn't set up federation with social (like Google) or other identity providers. (Not relevant to question)

They don't have any other authentication method or any password-backed accounts. (User 1 is already registered as a guest meaning they have established some form of authentication already. OTP is the fallback option when no other form of authentication has been established for the user being shared to.)

Email one-time passcode is enabled.

upvoted 1 times

 **AleFerrillo** 3 months ago

Selected Answer: B

As per docs: "if...They don't have a Microsoft account." which user2 clearly has upvoted 2 times

 **EmnCours** 4 months, 2 weeks ago

Selected Answer: A

A. User2 only
upvoted 3 times

 **Mikael25** 5 months ago

Selected Answer: A

It's Answer A, because according to this link <https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode> and the answer on FAQ "What happens to my existing guest users if I enable email one-time passcode?

Your existing guest users won't be affected if you enable email one-time passcode, as your existing users are already past the point of redemption. Enabling email one-time passcode will only affect future redemption activities where new guest users are redeeming into the tenant.

upvoted 3 times

 **dule27** 5 months ago

Selected Answer: A

A. User2 only
upvoted 3 times

 **OK2020** 5 months, 1 week ago

Selected Answer: B

When does a guest user get a one-time passcode?

When a guest user redeems an invitation or uses a link to a resource that has been shared with them, they'll receive a one-time passcode if:

They don't have an Azure AD account.

They don't have a Microsoft account.

The inviting tenant didn't set up federation with social (like Google) or other identity providers.

They don't have any other authentication method or any password-backed accounts.

Email one-time passcode is enabled.

upvoted 3 times

 **pikey433** 5 months, 1 week ago

Selected Answer: B

As per pheb's explanation and after reading the Microsoft documentation

upvoted 3 times

 **OK2020** 7 months ago

Selected Answer: B

User1 Only

check the link details carefully:

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode>

1. it's for B2B with outside domains, so Fabricam user won't receive it.

2. user with "outlook" domain will not receive it too, Microsoft acct:

When does a guest user get a one-time passcode?

When a guest user redeems an invitation or uses a link to a resource that has been shared with them, they'll receive a one-time passcode if:

They don't have an Azure AD account.

They don't have a Microsoft account.

The inviting tenant didn't set up federation with social (like Google) or other identity providers.

They don't have any other authentication method or any password-backed accounts.

Email one-time passcode is enabled.

upvoted 4 times

 **Halwagy** 10 months, 3 weeks ago

Answer is B.

The email one-time passcode feature is a way to authenticate B2B collaboration users when they can't be authenticated through other means, such as Azure AD, Microsoft account (MSA)

upvoted 1 times

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users. From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users. You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort. What should you use?

- A. the Identity Governance blade in the Azure Active Directory admin center
- B. the Set-AzureAdUser cmdlet
- C. the Licenses blade in the Azure Active Directory admin center**
- D. the Set-WindowsProductKey cmdlet

Correct Answer: C

You can unassign licenses from users on either the Active users page, or on the Licenses page. The method you use depends on whether you want to unassign product licenses from specific users or unassign users licenses from a specific product.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1. the Licenses blade in the Azure Active Directory admin center
2. the Set-MsolUserLicense cmdlet

Other incorrect answer options you may see on the exam include the following:

- ☞ the Administrative units blade in the Azure Active Directory admin center
- ☞ the Groups blade in the Azure Active Directory admin center
- ☞ the Set-AzureAdGroup cmdlet

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/admin/manage/remove-licenses-from-users?view=o365-worldwide>

Community vote distribution

C (100%)

✉ **Jt909** Highly Voted 2 years, 2 months ago

In the exam the cmdlet was Set-MsolUserLicense, the right one!

upvoted 36 times

✉ **TJ001** 1 year, 10 months ago

just note it only works with Windows Power shell and not Powershell core..

upvoted 2 times

✉ **Beitran** Highly Voted 2 years, 7 months ago

Correct!

upvoted 12 times

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

Selected Answer: C

Correct Answer: C

upvoted 1 times

✉ **dule27** 5 months, 1 week ago

Selected Answer: C

C. the Licenses blade in the Azure Active Directory admin center

upvoted 1 times

✉ **[Removed]** 12 months ago

Selected Answer: C

C for this particular question and answer set. Set-MsolUserLicense cmdlet is also available to make the changes.

upvoted 1 times

✉ **Faheem2020** 1 year, 2 months ago

To remove licenses from an existing user account, use the following syntax:

```
Set-MgUserLicense -UserId "<Account>" -RemoveLicenses @("<AccountSkuId1>") -AddLicenses @{}
```

"The Set-MsolUserLicense and New-MsolUser (-LicenseAssignment) cmdlets are scheduled to be retired. Please migrate your scripts to the Microsoft Graph SDK's Set-MgUserLicense cmdlet as described above"

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/remove-licenses-from-user-accounts-with-microsoft-365-powershell?source=recommendations&view=o365-worldwide>
upvoted 4 times

POOUAGA 1 year, 7 months ago

The correct answer is B. Read the question carefully: The licenses are assigned to individual users from the Groups blade in the Azure Active Directory admin center.
That being said, we are talking about group based licensing. And the least amount of administrative effort is set-azureaduser cmdlet to change all the 25000 users to the new E5 licenses
upvoted 1 times

Geolem 1 year, 4 months ago

Per M\$ Documentation, you cannot change License stuff via Set-AzureADUser : <https://docs.microsoft.com/en-us/powershell/module/azuread/set-azureaduser?view=azureadps-2.0>

The command is Set-AzureADUserLicense but also deprecated :(

upvoted 1 times

Sh1rub10 1 year, 8 months ago

Selected Answer: C
The Set-MsolUserLicense cmdlet updates the license assignment for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.
<https://docs.microsoft.com/en-us/microsoft-365/enterprise/remove-licenses-from-user-accounts-with-microsoft-365-powershell?view=o365-worldwide>
upvoted 4 times

glazdub 1 year, 8 months ago

The Set-MsolUserLicense cmdlet updates the license assignment for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.
<https://docs.microsoft.com/en-us/microsoft-365/enterprise/remove-licenses-from-user-accounts-with-microsoft-365-powershell?view=o365-worldwide>
upvoted 2 times

stromnessian 1 year, 9 months ago

No correct answer here.
upvoted 1 times

TonytheTiger 1 year, 9 months ago

On the exam today - March 4, 2022. Look for " Set-MsolUserLicense " instead of answer listed here
upvoted 3 times

Benkyoujin 1 year, 6 months ago

That's deprecated now, though. I take it Set-MgUserLicense is the new one?
upvoted 2 times

Pravda 1 year, 10 months ago

On the exam 1/20/2022
upvoted 1 times

Sammy786 1 year, 10 months ago

Was the answer B?
upvoted 1 times

TP447 1 year, 11 months ago

If licenses are assigned using Group Membership then its a few clicks rather than manage for each user. Easy to set up and manage.
upvoted 1 times

AZ_Student 2 years, 1 month ago

Correct answer C, go to the Licenses blade in the Azure Active Directory admin center and uncheck the licenses that you want to remove.
upvoted 1 times

melatocaroca 2 years, 4 months ago

Set-AzureAdUser cannot be used to assign license you must use Set-AzureAdUserLicense
Adds or removes licenses for a Microsoft online service to the list of assigned licenses for a user.
upvoted 8 times

Ed2learn 2 years, 5 months ago

I agree the question as written is correct - however - watch on the test for the powershell command to be corrected. It is beyond a reasonable expectation to individually click 2500 users when powershell takes a few minutes. Point being - watch for the correction on the exam.
upvoted 4 times

Ailil 2 years, 5 months ago

B is not correct because set-azureaduser command individually cant be use license removal, in the other hand License blade not contains select all options for the users, so you have to tick every user individually
upvoted 2 times

HOTSPOT -

You have a Microsoft 365 tenant named contoso.com.

Guest user access is enabled.

Users are invited to collaborate with contoso.com as shown in the following table.

User email	User type	Invitation accepted	Shared resource
User1@outlook.com	Guest	No	Enterprise application
User2@fabrikam.com	Guest	Yes	Enterprise application

From the External collaboration settings in the Azure Active Directory admin center, you configure the Collaboration restrictions settings as shown in the following exhibit.

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)

 Delete

TARGET DOMAINS

Outlook.com

From a Microsoft SharePoint Online site, a user invites user3@adatum.com to the site.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	<input type="radio"/>	<input type="radio"/>
User2 can access the enterprise application.	<input type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access the enterprise application.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes -

Invitations can only be sent to outlook.com. Therefore, User1 can accept the invitation and access the application.

Box 2. Yes -

Invitations can only be sent to outlook.com. However, User2 has already received and accepted an invitation so User2 can access the application.

Box 3. No -

Invitations can only be sent to outlook.com. Therefore, User3 will not receive an invitation.

□  **Val_0** Highly Voted 2 years, 7 months ago

Yes/Yes/No - @Reyain - I replicated this in my lab as well, but don't have the requirement to have the domain "checked". User1 didn't accept the invitation, but their domain is in the allowed list so once they do, they'll be able to gain access to the Ent App. User2 probably accepted the invitation before the domain restriction was put into place so they should be able to access it as well. User3's domain is not allowed, so the invite will not be sent to them and they won't be able to access SharePoint.

upvoted 46 times

□  **reddevil01** 2 years, 6 months ago

User1:

In ideal scenario the box next to outlook.com in collaboration settings should be checked for the invitation to get to the user's mailbox

In this case , it says invitation is not accepted as per question ,(that means invitation is sent to user but not accepted.) So I believe the user settings for collaboration was changed after the invitation was sent.

Therefore User 1 should be able to to accept invitation and access the app

User2:

In question it says the user2 already accepted invitation hence again the user settings for external collaboration was changed after the invitation was sent.

Therefore User2 can access the app

User3:

The invitation wont even be sent to user 3 mailbox since user settings for collaboration doesn't allow invitation to be sent to adatum.com

upvoted 10 times

□  **f2bf85a** 7 months, 2 weeks ago

Checkboxes left to the domain and "Target Domains" are only there to select and delete the entries. They do not have to do with enabling or disabling the entries. So the domain is still active in the whitelist / blacklist even if unckecked.

upvoted 1 times

□  **TJ001** 1 year, 10 months ago

very straight forward question and answer

upvoted 2 times

□  **EmnCours** Most Recent 3 months, 4 weeks ago

YES

YES

No

upvoted 1 times

□  **Heshan** 4 months, 4 weeks ago

On the exam, 09/07/2023

upvoted 3 times

□  **AMZ** 5 months, 1 week ago

Question valid - 06/23

upvoted 2 times

□  **dule27** 6 months, 2 weeks ago

YES

YES

NO

upvoted 1 times

□  **JCKD4Ni3L** 6 months, 3 weeks ago

Is it just me or we can't see the email the invitation was sent ? Because of the . It kind of screws the question.... :(((
upvoted 2 times

□  **JunetGoyal** 7 months ago

Yes, yes, No.

Those who are confuse at 3rd by assuming that sharepoint n onedrive work different then B2B, please check the link
<https://learn.microsoft.com/en-us/sharepoint/sharepoint-azureb2b-integration>

upvoted 1 times

□  **m4rv1n** 7 months, 2 weeks ago

About the user3:

"This list works independently from OneDrive for Business and SharePoint Online allow/block lists. If you want to restrict individual file sharing in SharePoint Online, you need to set up an allow or blocklist for OneDrive for Business and SharePoint Online. For more information, see Restricted domains sharing in SharePoint Online and OneDrive for Business."

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure>

and

"If you have enrolled in the SharePoint and OneDrive integration with Azure AD B2B, invitations in SharePoint are also subject to any domain

restrictions configured in Azure Active Directory."

<https://learn.microsoft.com/en-us/sharepoint/restricted-domains-sharing?redirectSourcePath=%252farticle%252frestricted-domains-sharing-in-sharepoint-online-and-onedrive-for-business-5d7589cd-0997-4a00-a2ba-2320ec49c4e9>

upvoted 1 times

 **f2bf85a** 7 months, 2 weeks ago

<https://learn.microsoft.com/en-us/sharepoint/sharepoint-azureb2b-integration>

"SharePoint and OneDrive integration with the Azure AD B2B one-time passcode feature is currently not enabled by default."

Since the question does not mention that SharePoint and OneDrive integration with Azure AD B2B is enabled, we should assume that it is disabled, as the default setting is so...

So, the answer for User3 should also be Yes... But no one can know for sure what is counted as correct answer...

upvoted 1 times

 **f2bf85a** 7 months, 2 weeks ago

Correction: Just tested the exact scenario, and although SharePoint integration with B2B is disabled, the guest user not included in the allowed domains could not be invited from SharePoint Online.

So 3rd question for User3 should be NO

upvoted 1 times

 **itannajones** 8 months, 3 weeks ago

This scenario DOES NOT state that the Outlook.com domain restriction for guest invitations was enabled after User2 in the fabrikam domain already accepted the guest invitation. Soooo once the setting to allow only Outlook.com domain guest invitations is enabled in the tenant shouldn't that prevent the fabrikam.com domain guest users from accessing content? This seems like a security glitch to me...

upvoted 1 times

 **BB6919** 10 months, 3 weeks ago

This came in the exam today- 15.01.2023. I answered Y/Y/Y. I was a bit confused with the 3rd question. Mostly it should have been No.

upvoted 2 times

 **shoutiv** 11 months, 3 weeks ago

Yes, Yes, No

Checked in my tenant

upvoted 3 times

 **BTL_Happy** 1 year ago

this came out with some tweaks to the question and answers.

upvoted 1 times

 **Zubairr13** 1 year, 4 months ago

On the exam, 7/23/2022.

upvoted 2 times

 **ali_pin** 1 year, 5 months ago

User2 can access the application because they're already a guest user, so the @outlook.com domain only does not apply.

upvoted 2 times

 **Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022

upvoted 2 times

 **DemekeAd** 1 year, 7 months ago

YES

YES

No

upvoted 2 times

 **janshal** 1 year, 7 months ago

I think User3 CAN accept the invitation and gain access to the SharePoint site

"This list works independently from OneDrive for Business and SharePoint Online allow/block lists. If you want to restrict individual file sharing in SharePoint Online, you need to set up an allow or deny list for OneDrive for Business and SharePoint Online"

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/allow-deny-list>

check in my LAB...

upvoted 3 times

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to bulk invite Azure AD business-to-business (B2B) collaboration users.

Which two parameters must you include when you create the bulk invite? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. email address
- B. redirection URL
- C. username
- D. shared key
- E. password

Correct Answer: AB

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite>

Community vote distribution

AB (100%)

 **Ighobulu** Highly Voted 2 years, 7 months ago

correct

upvoted 16 times

 **RahulX** Most Recent 6 days, 16 hours ago

A. email address

B. redirection URL

upvoted 1 times

 **sherifhamed** 2 months, 2 weeks ago

Selected Answer: AB

When creating a bulk invite for Azure AD business-to-business (B2B) collaboration users, you must include the following parameters:

A. Email address: The email address is required to specify the email of the external user who will be invited to collaborate with your organization.

B. Redirection URL: The redirection URL is necessary to specify where the invited user will be redirected to after they accept the invitation. It typically leads to the sign-up or sign-in page for the external user's organization.

The other options (C, D, and E) are not typically part of the bulk invite process.

upvoted 1 times

 **EmnCours** 3 months, 4 weeks ago

Selected Answer: AB

A. email address

B. redirection URL

upvoted 1 times

 **dule27** 6 months, 2 weeks ago

Selected Answer: AB

A. email address

B. redirection URL

upvoted 1 times

 **ShoaibPKDXB** 6 months, 3 weeks ago

Selected Answer: AB

AB are correct.

upvoted 1 times

 **jojoseph** 10 months, 2 weeks ago

Selected Answer: AB

correct

upvoted 1 times

 **[Removed]** 12 months ago

Selected Answer: AB

Selected answer is correct.
upvoted 1 times

 **Jhill777** 1 year ago

Selected Answer: AB

AB. Column one is Email address to invite [inviteeEmail] Required
Column 2 is Redirection url [inviteRedirectURL] Required
upvoted 1 times

 **pikapin** 1 year, 2 months ago

In exam 29/Sep
upvoted 1 times

 **trxs1** 1 year, 4 months ago

Selected Answer: AB

correct
upvoted 1 times

 **Zubairr13** 1 year, 4 months ago

On the exam, 7/23/2022.
upvoted 1 times

 **shine98** 1 year, 5 months ago

On the exam - June 12, 2022
upvoted 1 times

 **Sh1rub10** 1 year, 8 months ago

Selected Answer: AB

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite#invite-guest-users-in-bulk>
upvoted 3 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.
upvoted 2 times

 **WS_21** 1 year, 8 months ago

Selected Answer: AB

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite#invite-guest-users-in-bulk>
upvoted 2 times

 **gwerin** 1 year, 10 months ago

Selected Answer: AB

Correct
upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant that contains the objects shown in the following table.

Name	Type	Directly assigned license
User1	User	<i>None</i>
User2	User	Microsoft Office 365 Enterprise E5
Group1	Security group	Microsoft Office 365 Enterprise E5
Group2	Microsoft 365 group	<i>None</i>
Group3	Mail-enabled security group	<i>None</i>

Which objects can you add as members to Group3?

- A. User2 and Group2 only
- B. User2, Group1, and Group2 only
- C. User1, User2, Group1 and Group2
- D. User1 and User2 only
- E. User2 only

店铺：专业认证88

Correct Answer: E

Reference:

<https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/>

Community vote distribution

E (4%)

U (26%)

✉  **Cheguevarax** Highly Voted 2 years, 6 months ago

The answer is Use2 only. I just tested. You can't assign the users with no license. 100%

upvoted 71 times

✉  **Arjanussie** 9 months, 1 week ago

Test it also You can't assign the users with no license / mailbox

upvoted 1 times

✉  **rsamant** 1 year, 7 months ago

Right. you need to have exchange service included in the license so E3 and E5 users can only be added

upvoted 3 times

✉  **Hot_156** 1 year, 2 months ago

Which objects can you add as members to Group3? - From Azure AD, you can add any user to a Mail-enabled Security Group (licensed or unlicensed)... You have to remember that a group is also a SECURITY GROUP! This exam is based on Azure AD IAM, so I would say D.

upvoted 3 times

✉  **Sashy** 2 years, 1 month ago

I agree with Discuss4cert! I just tested as well and you cannot add an unlicensed member to Group 3, but I was able to go to user's group membership tab and her from her profile to group 3.

upvoted 3 times

✉  **Diginomad** Highly Voted 1 year, 11 months ago

Selected Answer: E

The answer is E - User2 Only. When you try to add a member to a Mail-enabled Security Group, you won't be able to see unlicensed Users. I had to test this when I saw contradictory comments.

upvoted 15 times

✉  **xupiter** 1 year, 10 months ago

That's right, but only for Azure portal. Using Microsoft 365 admin center, you can add unlicensed users to a Mail-enabled Security Group. So answer is D.

upvoted 3 times

✉  **zol95** 1 year, 2 months ago

You are incorrect. Tested in Lab environment:

In the M365 admin center, only users can be added to the mail-enabled security group.

You can only add licensed users to the group, unlicensed users won't even show up on the member select page. Correct answer is definitely E.

upvoted 2 times

✉  **Chris7910** 6 months, 2 weeks ago

But you can go to O365 Admin Center -> Users -> Active Users, select the user -> Account -> Manage groups and assign the group to the user.

So technically you added the user to the group.
upvoted 1 times

✉ **zol95** 1 year, 2 months ago

Sorry xupiter you are correct. If you open the mail enabled SG, then you won't be able to add the user, but if you open the unlicensed users from Users/Active Users/"user"/Groups/Manage groups then you can add the unlicensed user to the mail-enabled SG... Correct answer is D.

upvoted 1 times

✉ **Fcnet** 1 year, 1 month ago

no you can't from portal.azure.com / it's not permitted (may be it was possible 1 year ago but not now)
upvoted 3 times

✉ **RahulX** Most Recent 6 days, 15 hours ago

The Correct ans is User 2.
User 2 has valid exol license, thus having smtp address.
Tested on Lab: Only user and DL can be added into M365 Mail enabled security group.
upvoted 2 times

✉ **JCKD4Ni3L** 1 month, 4 weeks ago

Selected Answer: D

Add user to the domain contacts in the admin center, then you will be able to add it to your mail-enabled SG. I do this on a regular basis.. answer is « D ».
upvoted 1 times

✉ **Softeng** 2 months, 1 week ago

Selected Answer: E

Tested in lab, you can't assign security/m365 groups, neither an unlicensed group.
upvoted 2 times

✉ **Bear4** 2 months, 1 week ago

I can add a other mail enabled security group? So User 2 and Group 3.
upvoted 1 times

✉ **syougun200x** 3 months ago

As of today, when I tested in my tenant, User 1 and user 2 can be added. No groups appear to choose from in the list.
upvoted 1 times

✉ **edmca** 3 months, 2 weeks ago

D is correct. I tried to add to create a test mail-enabled sec group and tried to add an unlicensed user from Exchange admin center but the system would not let me, however, you can go to O365 Admin Center -> Users -> Active Users, select the user -> Account -> Manage groups and assign the group to the user. The unlicensed user won't be able to receive the mail since it doesn't have any mail related license
upvoted 1 times

✉ **EmnCours** 3 months, 3 weeks ago

Selected Answer: E

It's E: User 2 only
The Identity needs to have a mailbox.
So only Users with a mailbox, shared mailbox identities and Mail-Enabled security groups can be added.

- Mail-enabled security groups cannot contain M365 groups or Security groups, but they can contain other Mail-Enabled Security Groups.
- M365 Groups cannot contain other groups in general.
upvoted 3 times

✉ **zyhke** 5 months, 2 weeks ago

This is an exam for Azure, they don't want you touching admin center for this...The answer is E
upvoted 3 times

✉ **Holii** 6 months ago

Why is it not A?
I tried unlicensed users. Couldn't add them. So it's definitely either A or E.

I tried unlicensed Microsoft 365 Groups. It worked. I tried sending out an email to the mail-enabled security group and it sent the email out to all the users part of the Microsoft 365 group.

The question says "Directly assigned license", you can definitely have a Microsoft 365 group without a license directly assigned, but have users with licenses and the flow will work as expected...

Are we to assume they mean an unlicensed Microsoft 365 Group *with* unlicensed users?

upvoted 1 times

✉ **Holii** 6 months ago

Update: These were groups that were additionally registered as Distribution Groups, not solely Microsoft 365 Groups.

Answer is E.

upvoted 1 times

✉ **dule27** 6 months, 2 weeks ago

Selected Answer: E

E. User2 only
upvoted 2 times

 **ShoaibPKDXB** 6 months, 3 weeks ago

Selected Answer: E

E is correct
upvoted 3 times

 **OK2020** 7 months ago

Selected Answer: E

Which Microsoft 365 plans include groups?

Any Microsoft 365 subscription that has Exchange Online and SharePoint Online will support groups. That includes the Business Essentials and Business Premium plans, and the Enterprise E1, E3, and E5 plans. The group takes on the licensing of the person who creates the group (also known as the "organizer" of the group). As long as the organizer has the proper license for whatever features you want the group to have, that license will convey to the group.

<https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/office-365-groups?view=o365-worldwide>
upvoted 3 times

 **f2bf85a** 7 months, 2 weeks ago

Selected Answer: E

It's E: User 2 only
The Identity needs to have a mailbox.
So only Users with a mailbox, shared mailbox identities and Mail-Enabled security groups can be added.

- Mail-enabled security groups cannot contain M365 groups or Security groups, but they can contain other Mail-Enabled Security Groups.
- M365 Groups cannot contain other groups in general.

upvoted 2 times

 **ccadenasa** 9 months ago

User2 only. Tested in my lab
upvoted 1 times

 **ra1paul** 9 months, 2 weeks ago

D is the correct answer.
You can add a shared mailbox without license to a Mail enabled security group from EAC.
upvoted 1 times

DRAG DROP -

You have an on-premises Microsoft Exchange organization that uses an SMTP address space of contoso.com.

You discover that users use their email address for self-service sign-up to Microsoft 365 services.

You need to gain global administrator privileges to the Azure Active Directory (Azure AD) tenant that contains the self-signed users.

Which four 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.

Select and Place:

Actions

Sign in to the Microsoft 365 admin center.

Create a self-signed user account in the Azure AD tenant.

From the Microsoft 365 admin center, add the domain name.

Respond to the Become the admin message.

From the Microsoft 365 admin center, remove the domain name.

Create a TXT record in the contoso.com DNS zone.

Answer Area**Correct Answer:****Actions**

Sign in to the Microsoft 365 admin center.

Create a self-signed user account in the Azure AD tenant.

From the Microsoft 365 admin center, add the domain name.

Respond to the Become the admin message.

From the Microsoft 365 admin center, remove the domain name.

Create a TXT record in the contoso.com DNS zone.

Answer Area

Create a self-signed user account in the Azure AD tenant.

Sign in to the Microsoft 365 admin center.

Respond to the Become the admin message.

Create a TXT record in the contoso.com DNS zone.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover>

Beitran Highly Voted 2 years, 7 months ago

Seems correct judging by the link.

upvoted 20 times

slayer78 Highly Voted 2 years, 1 month ago

So after doing some research on this, the correct answer is:

1. Create a self signed user account
2. Sign into the admin center
3. Become an Admin
4. Create TXT record

This doesn't seem right, but that's how it's spelled out here:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover>

upvoted 14 times

casti 2 years, 1 month ago

To create the TXT record you have to register the domain in the administrator portal and obtain the value of the TXT record, IMHO is not correct

upvoted 2 times

 **007Ali** 1 year, 10 months ago

It would appear this question is getting at the "Internal admin takeover" process described here: <https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover>

That process provides a way to add a TXT record to your domain before registering the domain in the Azure Portal. So I think @slayer78 has the correct sequence.

upvoted 7 times

 **Jhill777** 1 year ago

Yessir. Had to do this many times.

upvoted 1 times

 **EmnCours** Most Recent 3 months, 3 weeks ago

1. Create a self signed user account
2. Sign into the admin center
3. Respond to the Become an Admin message
4. Create TXT record

upvoted 1 times

店铺：专业认证88

 **dule27** 6 months, 2 weeks ago

1. Create a self signed user account
2. Sign into the admin center
3. Respond to the Become an Admin message
4. Create TXT record

upvoted 2 times

 **ShoaibPKDXB** 6 months, 3 weeks ago

- correct:
1. Create a self signed user account
 2. Sign into the admin center
 3. Become an Admin
 4. Create TXT record

upvoted 1 times

 **Zubairr13** 1 year, 4 months ago

On the exam, 7/23/2022.

upvoted 3 times

 **sapien45** 1 year, 5 months ago

So many questions about Microsoft 365 services .., not even in the exam Syllabus

upvoted 3 times

 **stromnessian** 1 year, 8 months ago

Given answer is correct IMO.

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022

upvoted 1 times

 **saadnadir** 1 year, 10 months ago

Create a Self Signed user account in azure AD tenant
Sign in to the Microsoft 365 admin center
respond to the become the admin message
create a txt record in the contoso.com DNS zone

upvoted 1 times

店铺：专业认证88

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

 **casti** 2 years, 1 month ago

i think:

- 1 sing in in the admin center
- 2 Create a self signed user account
- 3 Create TXT record
- 4 From the 365 admin center add the domain name

upvoted 1 times

 **casti** 2 years, 1 month ago

After thinking about it again, I think that:

i think:

- 1 Create a self signed user account
- 2 sing in the admin center
- 3 From the 365 admin center add the domain name
- 4 Create TXT record

upvoted 3 times

✉ **Mohammad_Aломари** 1 year, 4 months ago

Nope, the question about the unmanaged directory/tenant, so, the answer is correct.

upvoted 1 times

✉ **Ibukun** 1 year, 11 months ago

This is a mistake

upvoted 1 times

✉ **Domza** 2 years, 5 months ago

Does not really say anything abt "Take over an unmanaged directory"

Ooof, these kinda questions

upvoted 3 times

✉ **jilly78** 1 year, 6 months ago

yes it lacks context

upvoted 1 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1 and the groups shown in the following table.

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned

In the tenant, you create the groups shown in the following table.

Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

Which members can you add to GroupA and GroupB? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

GroupA:

- User1 only
- User1 and Group1 only
- User1, Group1, and Group2 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group3 only
- User1, Group1, Group2, Group3, and Group4

GroupB:

- User1 only
- User1 and Group4 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group4 only
- User1, Group1, Group2, Group3, and Group4

Answer Area

GroupA:

- User1 only
- User1 and Group1 only
- User1, Group1, and Group2 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group3 only
- User1, Group1, Group2, Group3, and Group4

Correct Answer:

GroupB:

- User1 only
- User1 and Group4 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group4 only
- User1, Group1, Group2, Group3, and Group4

Reference:

<https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/>

 **Val_0** Highly Voted  2 years, 7 months ago

Group A - User1, Group1, Group2 and Group3. Group A cannot contain M365 groups.

Group B - User1 only; M365 groups cannot contain other groups.

upvoted 78 times

 **AmazingKies** 2 years, 2 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-membership-azure-portal>

upvoted 6 times

lime568 1 year, 8 months ago

We don't currently 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.
Assigning apps to nested groups.
Applying licenses to nested groups.
Adding distribution groups in nesting scenarios.
Adding security groups as members of mail-enabled security groups

upvoted 19 times

syougun200x [Most Recent] 3 months ago

As of today when I tested with my tenant.
Group A: can include users and security groups but no MS365 groups.
Group B: can include only users but no groups.

upvoted 1 times

EmnCours 3 months, 3 weeks ago

Group A - User1, Group1, Group2 and Group3. Group A cannot contain M365 groups.
Group B - User1 only; M365 groups cannot contain other groups.

upvoted 1 times

dule27 6 months, 2 weeks ago

Group A - User1, Group1, Group2 and Group3
Group B - User1 only

upvoted 2 times

ShoaibPKDXB 6 months, 3 weeks ago

Correct
Group A - User1, Group1, Group2 and Group3
Group B - User1 only

upvoted 1 times

anaSH 12 months ago

Answer is correct, tested in my tenant

upvoted 4 times

cameron0485 1 year ago

Question #13 Topic 1 shows a security group in a M365 group

upvoted 1 times

ANDRESCB1988 1 year ago

Correct.
GroupA allow add users, Dynamic User, Dynamic Devices.
GroupB only permit add users.

upvoted 2 times

pikapin 1 year, 2 months ago

In exam 29/Sep

upvoted 1 times

GryffindorOG 1 year, 3 months ago

Answer:
Group A: User 1 and Group 1 Only
Group B: User 1 Only

Dynamic and M365 Groups CANNOT be added to security groups so Group A can only add User 1 (users can be added to any group) Group 1 (security groups can be added to security groups)

Group B: Only users can be added to M365 groups

Tested this in my tenant

upvoted 4 times

Jhill777 1 year ago

No, you didn't test because I just assigned dynamic user and dynamic device groups to the Security group.

upvoted 3 times

AZ_Guru_Wannabe 1 year, 3 months ago

This is wrong - you CAN add a dynamic assigned group to another group.

upvoted 3 times

Zubairr13 1 year, 4 months ago

On the exam, 7/23/2022.

upvoted 1 times

 **sapien45** 1 year, 5 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-membership-azure-portal>

We don't currently support:
Adding Microsoft 365 groups to Security groups or other Microsoft 365 groups.

Group A - User1, Group1, Group2 and Group3. Group A cannot contain M365 groups.
Group B - User1 only; M365 groups cannot contain other groups
upvoted 1 times

 **observador081** 1 year, 6 months ago

You have an Azure AD (Azure Active Directory) tenant that contains the following users:

User1 has a Department set to Sales and a Country set to US
User2 has a Department set to Marketing and a Country set to US
User3 has a Department set to Sales and a Country set to Germany
User4 has a Department set to Marketing and a Country set to Germany
You create a group called Group1 that has the following dynamic membership rule.

user.country -eq "USA" -and user.department -eq "Marketing" -or user.department -eq "Sales"
Which users are members of Group1?

Please select only one answer.

A-User1 and User2 only

B-User1 and User3 only

C-Only User2 and User3

D-User1, User2, User3 and User4

upvoted 1 times

 **BTL_Happy** 1 year ago

To answer your question above - B

upvoted 1 times

 **bleedinging** 1 year, 6 months ago

The Reference link at the bottom of the Answer is a broken link.

upvoted 2 times

 **thiennp1982** 1 year, 6 months ago

Correct

upvoted 1 times

 **Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022

upvoted 1 times

 **DemekeAd** 1 year, 7 months ago

correct answer

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-membership-azure-portal>

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 an Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.

You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.

Solution: You configure password writeback.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference:

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

Community vote distribution

B (100%)

 **melatocaroca** Highly Voted 2 years, 4 months ago

Answer NO

Password writeback is a feature of Azure AD Connect which ensures that when a password changes in Azure AD (password change, self-service password reset, or an administrative change to a user password) it is written back to the local AD – if they meet the on-premises AD password policy.

Technically, a password write-back operation is a password “reset” action. Password writeback removes the need to set up an on-premises solution for users to reset their password. It all happens in real time, and so users are notified immediately if their password could not be reset or changed for any reason.

upvoted 15 times

 **glazdub** 1 year, 8 months ago

Answer is NO. <https://docs.microsoft.com/en-us/answers/questions/3221/disable-account-sync.html>

upvoted 1 times

 **BaderJ** Highly Voted 2 years, 2 months ago

Passed the exam today 23/09/2021

This question came in the exam.

upvoted 8 times

 **EmnCours** Most Recent 3 months, 3 weeks ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

 **AMZ** 5 months, 1 week ago

Question valid - 06/23

upvoted 2 times

 **dule27** 6 months, 2 weeks ago

Selected Answer: B

B. No is correct

upvoted 1 times

 **ShoaibPKDXB** 6 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

 **[Removed]** 12 months ago

Selected Answer: B

Correct answer given.

upvoted 1 times

 **ANDRESCB1988** 1 year ago

correct, answer is No

upvoted 1 times

 **shine98** 1 year, 5 months ago

On the exam - June 12, 2022

upvoted 1 times

 **bleedinging** 1 year, 6 months ago

Objection, your honor: Irrelevant.

upvoted 3 times

 **Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022

upvoted 1 times

 **WMG** 1 year, 8 months ago

Selected Answer: B

Password reset has nothing to do with what the question is asking.

upvoted 2 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 1 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 2 times

 **Iamjudeicon** 1 year, 11 months ago

Congratulations @BaderJ for success. I am preparing for mine that's scheduled this week Friday 17th December. My concern is, do Microsoft reshuffle their questions every year especially after every year's ignite?.

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 an Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.

You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.

Solution: You configure pass-through authentication.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Reference:

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

Community vote distribution

A (100%)

melatocaroca Highly Voted 2 years, 4 months ago

YES

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications by using the same passwords. Pass-through Authentication signs users in by validating their passwords directly against on-premises Active Directory.
upvoted 15 times

EmnCours Most Recent 3 months, 3 weeks ago

Selected Answer: A

Correct Answer: A

upvoted 2 times

Heshan 4 months, 4 weeks ago

On the exam, 09/07/2023

upvoted 1 times

AMZ 5 months, 1 week ago

Question valid - 06/23

upvoted 1 times

dule27 6 months, 2 weeks ago

Selected Answer: A

A: YES - pass-through authentication.

upvoted 1 times

[Removed] 12 months ago

Selected Answer: A

Correct answer given.

upvoted 1 times

ANDRESCB1988 1 year ago

correct, answer is yes

upvoted 2 times

pikapin 1 year, 2 months ago

In exam 29/Sep

upvoted 1 times

[Removed] 1 year, 4 months ago

Selected Answer: A

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn#comparing-methods>

Consideration: What user account states are supported?

Password hash synchronization + Seamless SSO: Disabled accounts (up to 30-minute delay)

Pass-through Authentication + Seamless SSO: Disabled accounts

Federation with AD FS: Disabled accounts

upvoted 2 times

□ **shine98** 1 year, 5 months ago

On the exam - June 12, 2022

upvoted 1 times

□ **DemekeAd** 1 year, 7 months ago

Correct

Pass-through Authentication enforces the on-premises account policy at the time of sign-in. 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 3 times

□ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 1 times

□ **TJ001** 1 year, 10 months ago

pass through is right

upvoted 1 times

□ **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

□ **Iamjudeicon** 1 year, 11 months ago

Congratulations @BaderJ for your success. I am preparing to take mine this coming week. I need every encouragement Lol

upvoted 1 times

□ **BaderJ** 2 years, 2 months ago

Passed the exam today 23/09/2021

This question came in the exam.

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.

You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.

You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.

Solution: You configure conditional access policies.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference:

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

Community vote distribution

B (100%)

melatocaroca [Highly Voted] 2 years, 5 months ago

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign into both on-premises and cloud-based applications using the same passwords

It uses a lightweight on-premises agent that listens for and responds to password validation requests. If disabled user can not login
upvoted 8 times

MajorUrs [Highly Voted] 2 years, 6 months ago

Correct (B - No)

upvoted 7 times

Stevo74 [Most Recent] 3 months, 2 weeks ago

Basically, you can configure a conditional policy for every disabled acc or group of acc (if you're disabling more of them at once). In policy you can block access to all cloud apps for this specific user or users and that will do, but this is not a permanent solution because you will need to do this every time, so that's why answer is B.

upvoted 1 times

EmnCours 3 months, 3 weeks ago

Selected Answer: B

Correct (B - No)

upvoted 1 times

Heshan 4 months, 4 weeks ago

On the exam, 09/07/2023

upvoted 1 times

dule27 6 months, 2 weeks ago

Selected Answer: B

B. No is the correct answer

upvoted 1 times

[Removed] 12 months ago

Selected Answer: B

No is the correct answer.

upvoted 1 times

ANDRESCB1988 1 year ago

correct, answers is NO

upvoted 1 times

Tokiki 1 year, 5 months ago

B is correct
upvoted 1 times

 **shine98** 1 year, 5 months ago

On the exam - June 12, 2022
upvoted 1 times

 **Fico** 1 year, 6 months ago

Selected Answer: B
has been verified <https://docs.microsoft.com/en-us/answers/questions/3221/disable-account-sync.html>
upvoted 1 times

 **Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022
upvoted 1 times

 **WMG** 1 year, 8 months ago

Selected Answer: B
Conditional Access will not help.
upvoted 1 times

店铺：专业认证88

 **glazdub** 1 year, 8 months ago

<https://docs.microsoft.com/en-us/answers/questions/3221/disable-account-sync.html>
as per this thread answer is NO.
upvoted 1 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022
upvoted 2 times

 **BaderJ** 2 years, 2 months ago

Passed the exam today 23/09/2021
This question came in the exam.
upvoted 3 times

 **Eltooth** 2 years, 6 months ago

Agreed - answer is no.
upvoted 3 times

店铺：专业认证88

店铺：专业认证88

You have an Azure Active Directory (Azure AD) tenant that contains the following objects.

- A device named Device1
- Users named User1, User2, User3, User4, and User5
- Five groups named Group1, Group2, Group3, Group4, and Group5

The groups are configured as shown in the following table.

Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group4
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Assigned	User5

How many licenses are used if you assign the Microsoft 365 Enterprise E5 license to Group1?

- A. 0
- B. 2
- C. 3
- D. 4

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>

Community vote distribution

0 (0%)

 **gills** Highly Voted 2 years, 4 months ago

The answer is simple. Answer is correct. Why? Because nested group do not inherit licenses.

upvoted 57 times

 **jt63** 1 year, 11 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced#limitations-and-known-issues>
upvoted 4 times

 **Dobby_41** Highly Voted 2 years, 6 months ago

Group 4 cannot be a member of group 1.

upvoted 21 times

 **sapien45** 1 year, 5 months ago

Good catch
upvoted 4 times

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

Selected Answer: B
2 licenses
upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

Selected Answer: B
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

 **EmnCours** 4 months, 2 weeks ago

Selected Answer: B
Answer is correct.
upvoted 1 times

 **AMZ** 5 months, 1 week ago

Question valid - 06/23
upvoted 1 times

 **dule27** 6 months, 2 weeks ago

Selected Answer: B

B: 2 licenses

upvoted 2 times

 **f2bf85a** 8 months ago

Selected Answer: B

It doesn't affect the correct answer, but M365 Groups (Group4) cannot be contained to other groups. This example showing that Group1 contains Group4 is wrong.

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/how-to-manage-groups#add-or-remove-a-group-from-another-group>

upvoted 3 times

 **broncobucks** 9 months, 2 weeks ago

Selected Answer: B

agree it is b

upvoted 1 times

 **jojoseph** 10 months, 2 weeks ago

B. nested group do not inherit licenses

upvoted 3 times

 **[Removed]** 11 months, 4 weeks ago

Selected Answer: B

As Gills suggested, nested groups do not support nested groups.

upvoted 2 times

 **den5_pepito83** 1 year ago

On Exam 14/11/2022

upvoted 1 times

 **ANDRESCB1988** 1 year ago

correct, nesting is not support to assing license

upvoted 1 times

 **Lion007** 1 year, 4 months ago

Selected Answer: B

Correct, answer is B.

"Group-based licensing currently does not 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."

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced#limitations-and-known-issues>

upvoted 3 times

 **Tokiki** 1 year, 5 months ago

agree, B

upvoted 1 times

 **Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022

upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1.

A contractor uses the credentials of user1@outlook.com.

You need to ensure that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com.

What should you do?

- A. Run the New-AzADUser cmdlet.
- B. Configure the External collaboration settings.
- C. Add a WS-Fed identity provider.
- D. Create a guest user account in contoso.com.**

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal>

Community vote distribution

D (90%)	10%
---------	-----

 **Jt909** Highly Voted 2 years, 2 months ago

Probably in the exam the cmdlet New-AzureADMSInvitation is proposed and correct
upvoted 21 times

 **AS007** Highly Voted 2 years, 6 months ago

Looks good given external collaboration is allowed/ default settings
upvoted 5 times

 **WMG** 1 year, 8 months ago

Unless noted, all MS questions assume default settings.
upvoted 2 times

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

Selected Answer: D
Answer is correct.
upvoted 1 times

 **dule27** 6 months, 2 weeks ago

Selected Answer: D
D. Create a guest user account in contoso.com.
upvoted 2 times

 **LOEG** 6 months, 3 weeks ago

Hi Admin, why is the email not visible. The email is protected. how do we able to answer questions when/ if the email in the question is protected
upvoted 1 times

 **kanew** 7 months, 1 week ago

Selected Answer: B
B for me. D has to be incorrect as you can't create a Guest User with external Identity via AAD or PowerShell. You can invite one but not create one unless they have a tenancy (contoso.com etc) address. That rules out A and D. C is not correct as Outlook is a configured Identity provider by default so no action is required. With A you can use the external collaboration settings to enable Guest self-sign up via user flows and add the application to the self service flow. It's exactly what they need.
upvoted 1 times

 **kanew** 6 months, 4 weeks ago

Sorry, that 2nd to last sentence should read... "With B you can use the external collaboration settings to enable Guest self-sign up via user flows and add the application to the self service flow."
upvoted 1 times

 **Holii** 6 months ago

1.) Configure External Collaboration Settings
2.) Create a User Flow
That's 2 operations.
Answer D can do this in 1 operation assuming default External Collaboration Settings.
upvoted 2 times

 **Holii** 6 months ago

I'd like to note that while this would be the (most ideal) solution when considering PoLP/Zero-Trust, it's too many steps in a process when you're just trying to add an account to access an app.

That's the problem with these exams. It tests you getting the right answer, regardless if it's bad process for the long run.
upvoted 2 times

 **DorelPopKun** 7 months, 3 weeks ago

Correct answer is D.
New-AzADUser is used to create a new active directory user as work/school account
upvoted 1 times

 **Taigr** 10 months, 2 weeks ago

Hi guys, so correct answer is D, not A? (This cmdlet is used to invite a new external user to your directory.)
upvoted 2 times

 **Holii** 6 months ago

New-AzureADUser is just a generic 'Add an Azure AD user'
It can be used to create an Azure AD user inside your tenant.

Funny thing is though, you can specify -UserType "Guest" and make an external guest account the same as D.
I assume since it's not specifying the -UserType flag, it's not considering it.
D is specifically talking about creating a guest account.
upvoted 1 times

 **[Removed]** 11 months, 4 weeks ago

Selected Answer: D

Correct answer. B2B is required.
upvoted 3 times

 **Jhill777** 1 year ago

Selected Answer: D
Correct, given external collaboration is set to defaults
upvoted 1 times

 **ANDRESCB1988** 1 year ago

correct option D
upvoted 1 times

 **Magis** 1 year, 1 month ago

Selected Answer: D
Correct. B2B is the only option in this scenario.
upvoted 2 times

 **shine98** 1 year, 5 months ago

On the exam - June 12, 2022
upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022
upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022
upvoted 1 times

Your network contains an Active Directory forest named contoso.com that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com by using Azure AD Connect.

You need to prevent the synchronization of users who have the extensionAttribute15 attribute set to NoSync. What should you do in Azure AD Connect?

- A. Create an inbound synchronization rule for the Windows Azure Active Directory connector.
- B. Configure a Full Import run profile.
- C. Create an inbound synchronization rule for the Active Directory Domain Services connector.**
- D. Configure an Export run profile.

Correct Answer: C

Reference:

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

Community vote distribution

C (100%)

 **EmnCours** 3 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 2 times

 **Heshan** 4 months, 4 weeks ago

On the exam, 09/07/2023

upvoted 1 times

 **AMZ** 5 months, 1 week ago

Question valid - 06/23

upvoted 1 times

 **dule27** 6 months, 2 weeks ago

Selected Answer: C

C. Create an inbound synchronization rule for the Active Directory Domain Services connector.

upvoted 1 times

 **ShoaibPKDXB** 6 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

 **m4rv1n** 7 months, 2 weeks ago

Selected Answer: C

Right answer <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#negative-filtering-do-not-sync-these>
upvoted 1 times

 **OrangeSG** 10 months, 4 weeks ago

Selected Answer: C

The connector name is Active Directory Domain Services connector (AD DS connector)

Reference

Azure AD Connect: Configure AD DS Connector Account Permissions

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-configure-ad-ds-connector-account>

upvoted 2 times

 **purek77** 11 months, 1 week ago

Selected Answer: C

For all who suggests something else than C - please read below:

<https://www.microsoftpressstore.com/articles/article.aspx?p=2861445&seqNum=3>

upvoted 1 times

 **[Removed]** 11 months, 4 weeks ago

Selected Answer: C

C is the correct answer.

upvoted 1 times

 **BTL_Happy** 1 year ago

this came out in my test.

upvoted 2 times

 **palito1980** 1 year, 1 month ago

Selected Answer: C

Following <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#negative-filtering-do-not-sync-these>.

Answer C is correct. You create an inbound rule because information is taken from Active Directory to Metaverse object.

upvoted 3 times

 **DeepMoon** 1 year, 2 months ago

Given answer C: is incorrect because it is talking AAD DS connector not AAD connector (sneaky!)

It should be A.

upvoted 3 times

 **DeepMoon** 1 year, 1 month ago

Active Directory Domain Service is an entirely different service that is not part of the question.

upvoted 1 times

 **Geolem** 1 year, 4 months ago

Would it be possible that the M\$ Documentation has a screenshot error ?

Why on the step 4, it is an OUTBOUND Sync Rule and on the step 5, it is an inbound ?

upvoted 1 times

 **DeepMoon** 1 year, 2 months ago

See diagram on

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

AD -> Connector -> Metaverse -> AAD

Inbound is from AD Connector to metaverse.

Outbound means from metaverse to AAD.

upvoted 2 times

 **Tokiki** 1 year, 5 months ago

C is correct

upvoted 1 times

 **Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022

upvoted 2 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 2 times

 **Sh1rub10** 1 year, 8 months ago

Selected Answer: C

Corret, configure in *Azure AD Connect* in question means configure something in *Active Directory Domain Services* side

upvoted 1 times

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

Name	Type	Directory synced
User1	User	No
User2	User	Yes
User3	Guest	No

All the users work remotely.

Azure AD Connect is configured in Azure AD as shown in the following exhibit.

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	Disabled	0 domains
Pass-through authentication	Enabled	2 agents

Connectivity from the on-premises domain to the internet is lost.

Which users can sign in to Azure AD?

A. User1 and User3 only

B. User1 only

C. User1, User2, and User3

D. User1 and User2 only

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-current-limitations>

Community vote distribution

A (100%)

examkid Highly Voted 2 years, 4 months ago

I think the answer is correct.

When the connection to on-premise is lost, PTA will not work anymore. The failover to

Password Hash Synchronization is not automatic and needs to be configured manually in AD Connect. If the connection to on-premise is lost, and the AD Connect server runs un-premise, user 2 cannot login.

~~~~~

Enabling Password Hash Synchronization gives you the option to failover authentication if your on-premises infrastructure is disrupted. This failover from Pass-through Authentication to Password Hash Synchronization is not automatic. You'll need to switch the sign-in method manually using Azure AD Connect. If the server running Azure AD Connect goes down, you'll require help from Microsoft Support to turn off Pass-through Authentication.

upvoted 32 times

AmazingKies Highly Voted 2 years, 2 months ago

Pass-through authentication is configured, Sync user will try to authenticate on local AD and unable to authenticate due to internet outage only cloud users ( User 1 and User 3) can be authenticated

Correct Answer : A

upvoted 13 times

 **EmnCours** Most Recent 3 months, 3 weeks ago

**Selected Answer: A**

Correct Answer : A

upvoted 3 times

 **Sango** 5 months ago

Answer A is correct. PTA is enabled which means no AD synced user auth will work until the issue is resolved. If both PHS and PTA are enabled (as per config) it is still a manual process (not mentioned in the question) to roll back to PHS. Microsoft: "Enabling Password Hash Synchronization gives you the option to failover authentication if your on-premises infrastructure is disrupted. This failover from Pass-through Authentication to Password Hash Synchronization is not automatic. You'll need to switch the sign-in method manually using Azure AD Connect. If the server running Azure AD Connect goes down, you'll require help from Microsoft Support to turn off Pass-through Authentication."

upvoted 1 times

 **dule27** 6 months, 2 weeks ago

**Selected Answer: A**

A. User1 and ~~User3~~ only

upvoted 1 times

 **f2bf85a** 7 months, 2 weeks ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-ptc-current-limitations#unsupported-scenarios>

Read the Note:

Enabling Password Hash Synchronization gives you the option to failover authentication if your on-premises infrastructure is disrupted. This failover from Pass-through Authentication to Password Hash Synchronization is not automatic. You'll need to switch the sign-in method manually using Azure AD Connect. If the server running Azure AD Connect goes down, you'll require help from Microsoft Support to turn off Pass-through Authentication.

Since the Password Hash sync failover is not automatic, in this case the answer is A. User2 that is directory sync will need Pass-Through Authentication, which will be unavailable at that moment.

upvoted 1 times

 **simonseztech** 11 months, 2 weeks ago

**Selected Answer: A**

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.

upvoted 1 times

 **[Removed]** 11 months, 4 weeks ago

**Selected Answer: A**

Answer A is correct. PTA cannot be used for directory synchronised objects when the connectivity is lost.

upvoted 1 times

 **den5\_pepito83** 1 year ago

ON EXAM 14/11/2022

upvoted 2 times

 **ANDRESCB1988** 1 year ago

answer A is correct

upvoted 1 times

 **estyj** 1 year, 1 month ago

Correct A. <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-ptc-current-limitations>

upvoted 1 times

 **pikapin** 1 year, 2 months ago

In exam 29/Sep

upvoted 1 times

 **Zubairr13** 1 year, 4 months ago

On the exam, 7/23/2022.

upvoted 1 times

 **rachee** 1 year, 4 months ago

C. Per <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-ptc-current-limitations>, Enabling Password Hash Synchronization gives you the option to failover authentication if your on-premises infrastructure is disrupted.

The diagram shows Pasword Hash Synchronization is enabled.

upvoted 5 times

 **Tokiki** 1 year, 5 months ago

Agree .A

upvoted 1 times

 **bleedinging** 1 year, 6 months ago

Correct. Only domain-synced users will be affected. Cloud users can still access cloud resources.

upvoted 1 times

 **Sh1rub10** 1 year, 8 months ago

**Selected Answer: A**  
only cloud users ( User 1 and User 3) can be authenticated  
upvoted 1 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

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 an Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.

You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.

Solution: You configure Azure AD Password Protection.

Does this meet the goal?

A. Yes

B. No

#### Correct Answer: B

##### Community vote distribution

B (100%)

 **melatocaroca** Highly Voted 2 years, 4 months ago

Answer NO

Azure AD Password Protection

With this feature, you can use the same checks for passwords in AzureAD on your on-premises Active Directory implementation.

You can enforce both the Microsoft Global Banned Passwords and Custom banned-passwords list stored in Azure AD tenant.

The DC agent software must be installed on all DCs in a domain.

upvoted 5 times

 **kijken** Most Recent 3 weeks, 3 days ago

just a general tip on yes/no questions. If you are not sure, always say no.

There are more questions with no as correct answer then yes

upvoted 2 times

 **kalyankrishna1** 2 months, 2 weeks ago

**Selected Answer: B**

PTA is the only thing that'll work

upvoted 1 times

 **Heshan** 4 months, 4 weeks ago

On the exam, 09/07/2023

upvoted 2 times

 **dule27** 6 months, 2 weeks ago

**Selected Answer: B**

B: NO is the correct answer

upvoted 1 times

 **OrangeSG** 11 months ago

**Selected Answer: B**

Answer is No.

Correct solution shall be Azure Active Directory (Azure AD) Pass-through Authentication.

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications by using the same passwords. Pass-through Authentication signs users in by validating their passwords directly against on-premises Active Directory.

upvoted 1 times

 **[Removed]** 11 months, 4 weeks ago

**Selected Answer: B**

B is the correct answer. Password Protection isn't the solution.

upvoted 1 times

 **ANDRESCB1988** 1 year ago

correct, is NO

upvoted 1 times

 **Jawad1462** 1 year, 1 month ago

**Selected Answer: B**

Is the correct answer

upvoted 1 times

 **shine98** 1 year, 5 months ago

On the exam - June 12, 2022

upvoted 1 times

 **Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022

upvoted 1 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 1 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

 **ShoaibNasr** 1 year, 8 months ago

and what is the correct answer

upvoted 1 times

 **Iamjudeicon** 1 year, 11 months ago

NO NO NO

The Given Answer Is Correct!!!

upvoted 2 times

 **sapien45** 1 year, 5 months ago

How about you explain why Azure AD Password Protection do not do the trick ... instead of ... being useless.

With this feature, you can use the same checks for passwords in AzureAD on your on-premises Active Directory implementation. You can enforce both the Microsoft Global Banned Passwords and Custom banned-passwords list stored in Azure AD tenant.

upvoted 2 times

 **Ed2learn** 2 years, 5 months ago

very clearly no - the given answer is correct

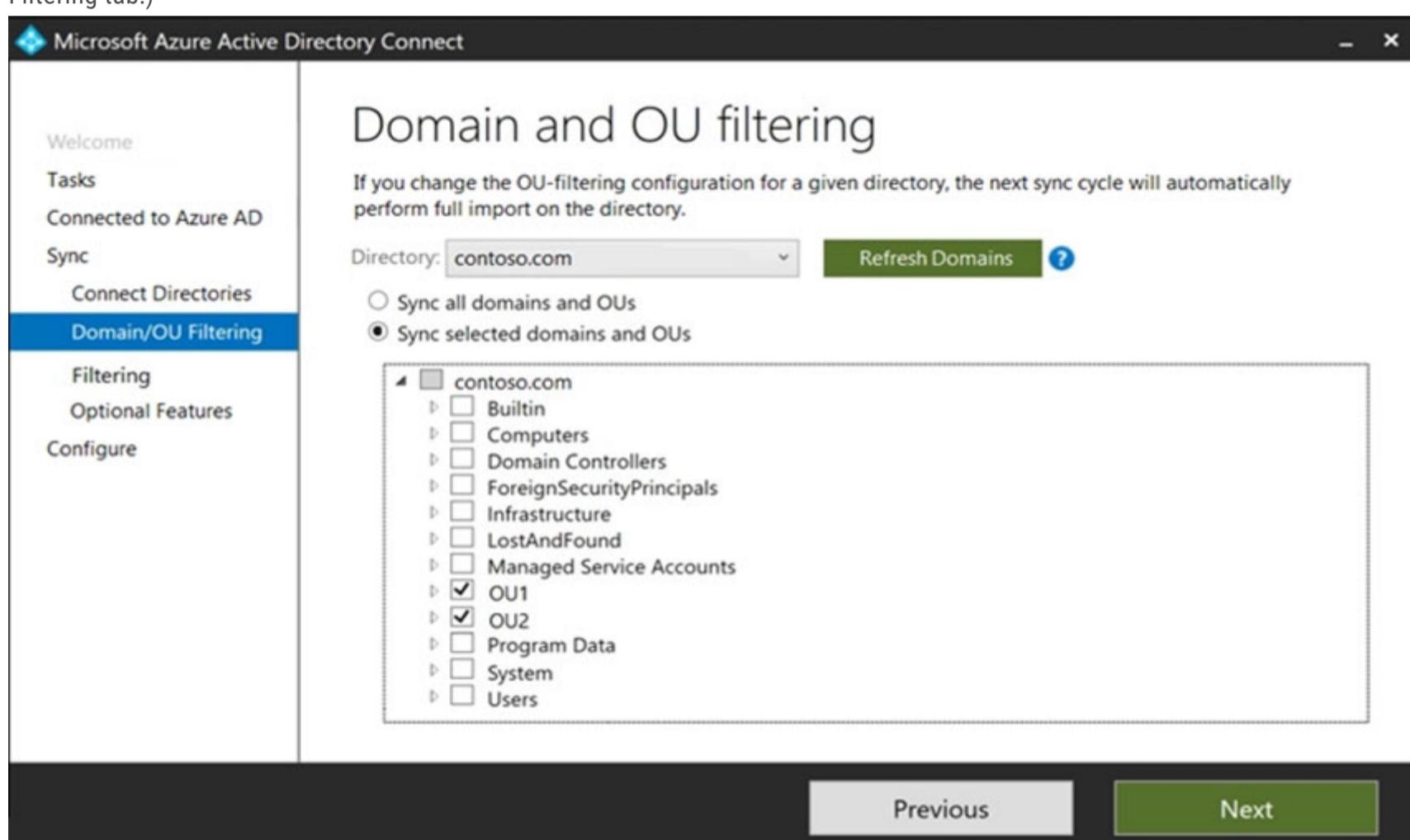
upvoted 1 times

**HOTSPOT -**

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

| Name   | Type           | In organizational unit (OU) | Description                             |
|--------|----------------|-----------------------------|-----------------------------------------|
| User1  | User           | OU1                         | User1 is a member of Group1.            |
| User2  | User           | OU1                         | User2 is not a member of any groups.    |
| Group1 | Security group | OU2                         | User1 and Group2 are members of Group1. |
| Group2 | Security group | OU1                         | Group2 is a member of Group1.           |

You install Azure AD Connect. You configure the Domain and OU filtering settings as shown in the Domain and OU Filtering exhibit. (Click the Domain and OU Filtering tab.)



You configure the Filter users and devices settings as shown in the Filter Users and Devices exhibit. (Click the Filter Users and Devices tab.)

Microsoft Azure Active Directory Connect

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

Filter users and devices

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

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

FOREST GROUP  
contoso.com  Resolve

Previous Next

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

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

### Answer Area

| Statements                | 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"/> |

Correct Answer:

Only direct members of Group1 are synced. Group2 will sync as it is a direct member of Group1 but the members of Group2 will not sync.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom>

□  **DrMe** Highly Voted 2 years, 1 month ago

Correct:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom#:~:text=When%20you%20add%20a%20group%20as%20a%20member%2C%20only%20the%20group%20itself%20is%20added.%20Its%20members%20aren%27t%20added>.

upvoted 21 times

□  **Jhill777** Highly Voted 1 year ago

This is a dumb question that only some dude at MSFT would write. Tested in lab because you'll never do something this dumb in real life. The answer is correct even though the wizard specifically states "Nested groups are not supported and will be ignored." They are not ignored. User1, Group1 and Group2 were created in Azure AD. User2 was not.

upvoted 17 times

□  **its\_tima** 10 months, 2 weeks ago

well depends on what type of group: Security or Office 365? If not them. perhaps the question makes you assume it's a Dynamic Group.

upvoted 1 times

□  **its\_tima** 10 months, 2 weeks ago

I take my word back, it's security so the question should get blame

upvoted 2 times

□  **Nivos23** Most Recent 1 month ago

YES

NO

YES

upvoted 1 times

□  **EmnCours** 3 months, 3 weeks ago

Correct:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom#:~:text=When%20you%20add%20a%20group%20as%20a%20member%2C%20only%20the%20group%20itself%20is%20added.%20Its%20members%20aren%27t%20added>

upvoted 1 times

□  **dule27** 6 months, 2 weeks ago

YES

NO

YES

upvoted 1 times

□  **roberto314** 1 year ago

ON EXAM 15/11/2022

upvoted 5 times

□  **den5\_pepito83** 1 year ago

ON EXAM 14/11/2022

upvoted 3 times

□  **pikapin** 1 year, 2 months ago

In exam 29/Sep

upvoted 1 times

□  **lme** 1 year, 2 months ago

on the exam 09222022, i answered the same. Passed the exam, btw.

upvoted 3 times

□  **Efficia** 1 year, 5 months ago

The given answer is correct.

Group 2 is a member of Group 1, so only Group 2 will sync, its members won't sync.

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom#sync-filtering-based-on-groups>

"All objects that you want to synchronize must be direct members of the group. Users, groups, contacts, and computers or devices must all be direct members. Nested group membership isn't resolved. \*\*When you add a group as a member, only the group itself is added. Its members aren't added.\*\*"

upvoted 4 times

□  **Tokiki** 1 year, 5 months ago

Correct, YNY

upvoted 1 times

□  **rachee** 1 year, 5 months ago

In the "Filter Users and Devices" exhibit it states "Nested groups are not supported and will be ignored." So does this mean only the users and devices in a nested group won't sync, or the group won't sync either?

upvoted 2 times

□  **Cybermystg** 1 year, 5 months ago

In the test today 6/15/2022

upvoted 1 times

□ **RandomNickname** 1 year, 6 months ago

See articles pasted by other members and on answer sections for reference as to why.

1:Y - User1 is a member of Group 1, and a direct member so as the group is synced, so will this.

2:N - User 2 is not a member of group1, and filtering is in place for G1.

3:Y - G2 will be synced because it's a direct member of G1, however any nested, for example, members of G2 will not be synced, so direct users or groups of G1 will.

For reference see below excerpt from MS article

"All objects that you want to synchronize must be direct members of the group. Users, groups, contacts, and computers or devices must all be direct members. Nested group membership isn't resolved. When you add a group as a member, only the group itself is added. Its members aren't added."

upvoted 8 times

□ **TP447** 1 year, 8 months ago

At first I thought this should be Y/N/N but having confirmed in the article, Group 2 will sync as a Direct Member of Group 1 delegated for the pilot. Therefore Y/N/Y is correct.

upvoted 4 times

□ **SnottyPudding** 1 year, 8 months ago

Q3 is NO: "When using OU-based filtering in conjunction with group-based filtering, the OU(s) where the group and its members are located must be included." Synchronization is selected only for OU2, and Group2 is in OU1. Therefore, Group2 WILL NOT sync to Azure AD.

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

upvoted 2 times

□ **kanew** 7 months, 1 week ago

I initially thought that but on reflection agree with the Y,N,Y. Think of the group filter as a subset of the OU's selected. So all members of OU1 and OU2 are in scope then the filter removes (filters!) anyone not in Group 1. It doesn't matter which OU Group 2 is in. It syncs as is part of the OUs in scope and not filtered out as is a first level member of Group1. Jeez I did a bad job of explaining that. terrible scenario - it was talked about many years ago but I've never seen any organization ever use it!

upvoted 1 times

□ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You need to ensure that Azure AD External Identities pricing is based on monthly active users (MAU).

What should you configure?

- A. a user flow
- B. the terms of use
- C. a linked subscription**
- D. an access review

**Correct Answer: C**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing>

Community vote distribution

C (100%)

 **jt63** Highly Voted 1 year, 11 months ago

Correct.

To take advantage of MAU billing, your Azure AD tenant must be linked to an Azure subscription.

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing#what-do-i-need-to-do>

upvoted 6 times

 **WS\_21** Highly Voted 1 year, 8 months ago

**Selected Answer: C**

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing#what-do-i-need-to-do>

upvoted 5 times

 **haazybanj** Most Recent 4 weeks ago

**Selected Answer: C**

The correct answer is C. a linked subscription.

Azure AD External Identities pricing is based on monthly active users (MAU) when your tenant is linked to a subscription. This means that you will only be charged for the number of users who actively use Azure AD External Identities in a given month.

upvoted 1 times

 **sherifhamed** 2 months, 2 weeks ago

**Selected Answer: C**

To ensure that Azure AD External Identities pricing is based on monthly active users (MAU), you should configure:

C. a linked subscription

You need to link your Azure AD External Identities to a billing subscription that supports monthly active users (MAU) billing. This allows you to pay based on the number of unique users who access your applications or services each month.

Options A (a user flow), B (the terms of use), and D (an access review) are not related to configuring billing for Azure AD External Identities based on MAU.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: C**

C. a linked subscription

upvoted 1 times

 **dule27** 6 months, 2 weeks ago

**Selected Answer: C**

C. a linked subscription

upvoted 1 times

 **ShoaibPKDXB** 6 months, 3 weeks ago

C Linked Subscription

upvoted 1 times

 **Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022

upvoted 3 times

□ **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 3 times

□ **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022

upvoted 3 times

□ **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

□ **KennethYY** 1 year, 11 months ago

When I study from Microsoft learning, doesn't see this feature need cost ..... :>\_<:

upvoted 2 times

□ **BaderJ** 2 years, 2 months ago

Passed the exam today 23/09/2021

This question came in the exam.

upvoted 2 times

□ **zaqwsx** 2 years, 3 months ago

it looks correct, from docs:

An Azure AD tenant already linked to a subscription?

"Do nothing. When you use External Identities features to collaborate with guest users, you'll be automatically billed using the MAU model."

upvoted 3 times

## DRAG DROP -

You have a new Microsoft 365 tenant that uses a domain name of contoso.onmicrosoft.com.

You register the name contoso.com with a domain registrar.

You need to use contoso.com as the default domain name for new Microsoft 365 users.

Which four 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.

Select and Place:

**Actions**

Delete the contoso.onmicrosoft.com domain.

Add a custom domain name of contoso.com.

Set the domain to primary.

Create a new TXT record in DNS.

Successfully verify the domain name.

**Answer Area**

店铺：专业认证88

**Actions**

Delete the contoso.onmicrosoft.com domain.

**Correct Answer:****Answer Area**

Add a custom domain name of contoso.com.

Create a new TXT record in DNS.

Successfully verify the domain name.

Set the domain to primary.

Reference:

<https://practical365.com/configure-a-custom-domain-in-office-365/>

 casti Highly Voted 2 years, 1 month ago

Correct!!!

upvoted 23 times

 EmnCours Most Recent 4 months, 2 weeks ago

Correct!!!

upvoted 1 times

 EmnCours 3 months, 3 weeks ago

1. Add a custom domain name of contoso.com
2. Create a new TXT record in DNS
3. Successfully verify the domain name
4. Set the domain to primary

upvoted 2 times

 dule27 6 months, 2 weeks ago

1. Add a custom domain name of contoso.com
2. Create a new TXT record in DNS
3. Successfully verify the domain name
4. Set the domain to primary

upvoted 4 times

 [Removed] 11 months, 4 weeks ago

Sequence given is correct.

upvoted 1 times

 ANDRESCB1988 1 year ago

correct

店铺：专业认证88

upvoted 1 times

□ **pete26** 1 year, 1 month ago

The answer given is correct!

upvoted 1 times

□ **rachee** 1 year, 4 months ago

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

upvoted 1 times

□ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 1 times

□ **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 3 times

□ **TJ001** 1 year, 10 months ago

Correct !!

upvoted 1 times

□ **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 2 times

□ **Iamjudeicon** 1 year, 11 months ago

CORRECT!!!

upvoted 2 times

**HOTSPOT -**

You have an Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium Plan 2 license. The tenant contains the users shown in the following table.

| Name   | Role                       |
|--------|----------------------------|
| Admin1 | Cloud device administrator |
| Admin2 | Device administrator       |
| User1  | <b>None</b>                |

You have the Device Settings shown in the following exhibit.

User1 has the devices shown in the following table.

| Name    | Operating system | Device identity     |
|---------|------------------|---------------------|
| Device1 | Windows 10       | Azure AD joined     |
| Device2 | iOS              | Azure AD registered |
| Device3 | Windows 10       | Azure AD registered |
| Device4 | Android          | Azure AD registered |

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

User1 can join four additional Windows 10 devices to Azure AD.

Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to Yes.

Admin2 is a local administrator on Device3.

**Yes** **No**






**Correct Answer:****Answer Area****Statements**

**Yes** **No**

User1 can join four additional Windows 10 devices to Azure AD.



Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to Yes.



Admin2 is a local administrator on Device3.

Users may join 5 devices to Azure AD.

Box 2: No -

Cloud device administrator can enable, disable, and delete devices in Azure AD and read Windows 10 BitLocker keys in the Azure portal. The role does not grant permissions to manage any other properties on the device.

Box 3: No -

An additional local device administrator has not been applied

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

□  **DrMe** Highly Voted 2 years, 1 month ago

Looks like the max devices applies to registered and joined (just not hybrid), so I'm thinking

- 1) No
- 2) Yes
- 3) No

<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal#:~:text=Maximum%20number%20of%20devices%20setting%20applies%20to%20devices%20that%20are%20either%20Azure%20AD%20joined%20or%20Azure%20AD%20registered>

upvoted 66 times

□  **AleFerrillo** 2 months, 4 weeks ago

I just tried to change the "MFA Settings" in the Device Settings page with a Cloud Device Admin and it saved the changes. So it is definitely NO, YES, NO.

upvoted 1 times

□  **Nilz76** 1 year, 8 months ago

Correct: 1) = NO

Maximum number of devices: This setting enables you to select the maximum number of Azure AD joined OR Azure AD registered devices that a user can have in Azure AD. If users reach this limit, they can't add more devices until one or more of the existing devices are removed. The default value is 50. You can increase the value up to 100. If you enter a value above 100, Azure AD will set it to 100. You can also use Unlimited to enforce no limit other than existing quota limits.

Link to the MS article below:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal#configure-device-settings>

upvoted 3 times

□  **sergioandresiq** 1 year, 5 months ago

100% agreed and tested, these answers are correct:

- 1) No
- 2) Yes
- 3) No

upvoted 11 times

□  **phony** 1 year, 9 months ago

for 3) it's hard to tell, because a part of the picture is not available. see example here: <https://docs.microsoft.com/en-us/mem/intune/enrollment/device-limit-intune-azure#azure-device-limit-restriction>

upvoted 1 times

□  **phony** 1 year, 9 months ago

but 3) it is NO because the device is AD Registered, not AD Joined.

upvoted 10 times

□  **kanew** 7 months, 1 week ago

exactly!

upvoted 1 times

□  **xurxosan** Highly Voted 1 year, 9 months ago

<https://docs.microsoft.com/en-gb/azure/active-directory/devices/device-management-azure-portal#configure-device-settings>

1. No

Maximum number of devices: This setting enables you to select the maximum number of Azure AD joined or Azure AD registered devices that a user can have in Azure AD

2. Yes

You must be assigned one of the following roles to view or manage device settings in the Azure portal:

Global Administrator  
Cloud Device Administrator  
Global Reader  
Directory Reader

3. No

Only Azure AD joined devices

upvoted 21 times

jack987 11 months, 2 weeks ago

I agree, correct answer is:

1. No -

<https://learn.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal#configure-device-settings>

The Maximum number of devices setting applies to devices that are either Azure AD joined or Azure AD registered. This setting doesn't apply to hybrid Azure AD joined devices.

2. Yes

3. No

upvoted 1 times

Nyamnyam [Most Recent] 4 weeks, 1 day ago

I also support the 1.No, 2.Yes, 3.No community here.

upvoted 2 times

amurp35 3 months, 2 weeks ago

Seems the real correct answer is 1-No, 2-Yes, 3-No, and not what is shown

upvoted 1 times

EmnCours 3 months, 3 weeks ago

Correction:

NO

YES

NO

upvoted 1 times

dule27 6 months, 2 weeks ago

NO

NO

NO

upvoted 1 times

dule27 5 months ago

Correction:

NO

YES

NO

upvoted 1 times

kanew 7 months, 1 week ago

The correct answers are No, No, No . There was quite a lot to think about in this question but it wasn't that hard to prove so I'm not sure why all the disagreement.

1) No. The set limit is 5. We have 4 and Microsoft state that both AZure AD registered and Azure AD joined devices count (not hybrid-joined). Here is the reference: <https://learn.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

2) No. It's easy to test and I did.

3) No. This was a bit trickier. I nearly said yes before realizing this only applies to Win 10/11 Azure AD JOINED devices. This device is only registered. "Additional local administrators on Azure AD joined devices: This setting allows you to select the users who are granted local administrator rights on a device. These users are added to the Device Administrators role in Azure AD. Global Administrators in Azure AD and device owners are granted local administrator rights by default."

<https://learn.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

upvoted 1 times

Holii 5 months, 4 weeks ago

No/Yes/No

Test again, Cloud Device Administrator gives the appropriate control.

<https://learn.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

You must be assigned one of the following roles to view or manage device settings in the Azure portal:

Global Administrator

Global Reader

Cloud Device Administrator

Intune administrator

Windows 365 administrator

Directory reviewer

upvoted 2 times

dobriv 7 months, 2 weeks ago

The Second question answer is 100 % YES. You can find the reason here : "You must be assigned one of the following roles to view or manage device settings in the Azure portal:

Global Administrator

Cloud Device Administrator

Global Reader

Directory Reader"

<https://learn.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

The First question is NO - The Maximum number of devices setting applies to devices that are either Azure AD joined or Azure AD registered. This setting doesn't apply to hybrid Azure AD joined devices. - same link !

upvoted 1 times

✉ **rajbne** 7 months, 3 weeks ago

can the answer to question be updated based on the discussion to No, Yes, NO ?

upvoted 2 times

✉ **eleazarrd** 7 months, 3 weeks ago

Número máximo de dispositivos : esta configuración le permite seleccionar el número máximo de dispositivos unidos a Azure AD o registrados en Azure AD que un usuario puede tener en Azure AD. Si los usuarios alcanzan este límite, no pueden agregar más dispositivos hasta que se eliminen uno o más de los dispositivos existentes. El valor predeterminado es 50 . Puede aumentar el valor hasta 100. Si ingresa un valor superior a 100, Azure AD lo establecerá en 100. También puede usar Ilimitado para aplicar ningún límite más que los límites de cuota existentes.

Mi respuesta sería N,N,N

upvoted 1 times

✉ **iwantmyexamsobad** 8 months ago

Answer is NO, NO, NO.

Try for yourself: create a cloud device admin and try modifying the device settings. You won't be able to! impossible to save the modifications.

upvoted 6 times

✉ **kanew** 7 months, 1 week ago

Agree 100%. My comment above has the reasons and references

upvoted 1 times

✉ **217f3c9** 7 months, 2 weeks ago

Nice ... just want to write that I can modify the settings. 2) is No 100%

upvoted 1 times

✉ **itismadu** 7 months, 4 weeks ago

I think i agree with you. <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#cloud-device-administrator>

upvoted 1 times

✉ **mayleni** 9 months, 3 weeks ago

2) No, cloud device admin doesn't have permission for any MFA action <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#cloud-device-administrator>

upvoted 4 times

✉ **Holii** 5 months, 4 weeks ago

You're trolling.

Your link states:

"microsoft.directory/deviceRegistrationPolicy/basic/update - Update basic properties on device registration policies"

Quite literally gives the correct level of access to Device Settings at the tenant-level:

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

upvoted 1 times

✉ **mayleni** 9 months, 3 weeks ago

In this question we don't have Hybrid devices so 1) No.

The docs say "The Maximum number of devices setting applies to devices that are either Azure AD joined or Azure AD registered. This setting doesn't apply to hybrid Azure AD joined devices."

upvoted 1 times

✉ **Garito** 10 months ago

N

Y

N

The Maximum number of devices setting applies to devices that are either Azure AD joined or Azure AD registered. This setting doesn't apply to hybrid Azure AD joined devices.

<https://learn.microsoft.com/en-gb/azure/active-directory/devices/device-management-azure-portal#configure-device-settings>

upvoted 1 times

✉ **Netromoni** 10 months, 1 week ago

Answer is correct!!! I guess the confusion part is number 1--> it is YES because only 1 device is AD joined (Azure AD joined is for corporate owned devices. It works only for Windows computers BESIDE Azure AD registered is for non-corporate ("bring your own device") scenarios. It enables single sign-on access to Azure AD managed resources such as Teams, Microsoft365, etc. This registration is what happens when you add a work or school account in Windows:)

upvoted 1 times

✉ **jojoseph** 10 months, 2 weeks ago

1) No

2) Yes

3) No

upvoted 2 times

✉ **den5\_pepito83** 1 year ago

YES

NO

NO

There is no user selected so the rules don't apply to nobody

upvoted 3 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

## DRAG DROP -

You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3.

You need to configure the users as shown in the following table.

| User  | Configuration                                                                                                                                                 |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User1 | <ul style="list-style-type: none"> <li>User administrator role</li> <li>Device Administrators role</li> <li>Identity Governance Administrator role</li> </ul> |
| User2 | <ul style="list-style-type: none"> <li>Records Management role</li> <li>Quarantine Administrator role group</li> </ul>                                        |
| User3 | <ul style="list-style-type: none"> <li>Endpoint Security Manager role</li> <li>Intune Role Administrator role</li> </ul>                                      |

Which portal should you use to configure each user? To answer, drag the appropriate portals to the correct users. Each portal 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.

Select and Place:

**Portals****Answer Area**

Azure Active Directory admin center

User1:

Exchange admin center

User2:

Microsoft 365 compliance center

User3:

Microsoft Endpoint Manager admin center

SharePoint admin center

Correct Answer:

**Portals****Answer Area**

Azure Active Directory admin center

User1: Azure Active Directory admin center

Exchange admin center

User2: Exchange admin center

Microsoft 365 compliance center

User3: Microsoft Endpoint Manager admin center

Microsoft Endpoint Manager admin center

SharePoint admin center

 **sergioandreslq** Highly Voted 1 year, 5 months ago

Answer:

User 1: Azure AD Admin center

User 2: Microsoft Purview admin center (legacy Microsoft Compliance Admin center), these roles came from Exchange, Microsoft is not enforcing the roles permission from Exchange, Microsoft is recommending using Microsoft Purview Admin center. I believe this answer is too old. it could be true years ago, however, Microsoft today is with MS purview to assign these roles. Record management and Quarantine role are known as SCC (security and compliance center) SCC roles have evolved from Exchange role groups design to MS Purview.

User 3: Endpoint Manager/Tenant administration/Roles/ you will see these two roles in the endpoint admin center.

upvoted 29 times

✉  **f2bf85a** 8 months ago

I agree... Also, although Records Management role can be selected in both Exchange Admin and Microsoft Purview, Quarantine Administrator can be only selected on Microsoft Purview... It is not listed in Exchange Admin Center.

upvoted 1 times

✉  **jack987** 11 months, 2 weeks ago

I agree with sergioandreslq

The correct answer is:

User 1: Azure AD Admin Center

User 2: Microsoft Compliance Admin Center

User 3: Microsoft Endpoint Manager Admin Center

upvoted 9 times

✉  **Nyamnyam** 4 weeks, 1 day ago

Meanwhile "Device Administrator" role is not existing anymore: <https://dirteam.com/sander/2020/08/31/knowledgebase-the-device-administrator-role-is-not-available-on-the-roles-and-administrators-pane-in-the-azure-portal/>

So the question is obsoleted. Hope to not come in an exam.

upvoted 1 times

✉  **dhenrique1555** Highly Voted 1 year, 7 months ago

The second user is ambiguous, as you can do it both from Exchange and Compliance center.

upvoted 13 times

✉  **Holii** 5 months, 4 weeks ago

Quarantine Administrator is no longer a role in Exchange Admin Center.

upvoted 2 times

✉  **jilly78** 1 year, 6 months ago

currently true

upvoted 3 times

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

New names:

User 1: Entra ID Admin center

User 2: Microsoft Purview admin center

User 3: Intune admin center

upvoted 4 times

✉  **EmnCours** 3 months, 3 weeks ago

The correct answer is:

User 1: Azure AD Admin Center

User 2: Microsoft Compliance Admin Center

User 3: Microsoft Endpoint Manager Admin Center

upvoted 2 times

✉  **EmnCours** 4 months, 2 weeks ago

Correct Answer

upvoted 1 times

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

for records management role - can be granted from both portals (Exchange admin center and Microsoft Purview)

But for Quarantined administrator role , you can assign it from Microsoft Purview.

upvoted 2 times

✉  **dule27** 6 months, 2 weeks ago

User 1: Azure AD Admin Center

User 2: Exchange Admin Center

User 3: Microsoft Endpoint Manager Admin Center

upvoted 2 times

✉  **dule27** 5 months ago

User 2: Microsoft Purview Compliance portal

upvoted 1 times

✉  **Holii** 5 months, 4 weeks ago

If this answer follows today's logic,

It would be 2.) Microsoft Purview Compliance Center.

Quarantine was shifted to be a compliance feature. As such, Exchange Admin Center no longer has a Quarantine Administrator role, it was moved to Compliance.

upvoted 2 times

✉  **AmplifiedStitches** 7 months, 3 weeks ago

The Quarantine Administrator role assignment option does appear to be located in the Purview admin center:

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

□ **doch** 10 months, 2 weeks ago

Strangely enough, the quarantine administrator role group is in the Exchange Admin Center.

upvoted 1 times

□ **ANDRESCB1988** 1 year ago

correct

upvoted 1 times

□ **VinciTheTechnic1an** 1 year, 5 months ago

If you practice this you know the answer. I also agree with bleedinging. Exchange is not mentioned here but the Purview is the correct answer.

upvoted 2 times

□ **bleedinging** 1 year, 6 months ago

For the second user, with Microsoft Purview now the naming for M365 Compliance Portal, I think this was meant to trip us up. If we can't choose the M365 Compliance Portal, the remaining correct answer is technically Microsoft Exchange Admin Center.

upvoted 4 times

□ **kanew** 7 months, 1 week ago

surely this is just out of date. The branding is now Purview but the link is still <https://compliance.microsoft.com>

upvoted 1 times

□ **slick\_orange** 1 year, 3 months ago

Or maybe the question was not up to date.

upvoted 2 times

□ **Nilz76** 1 year, 7 months ago

Answer is partly wrong:

Correct answers below:

- 1) Azure AD Admin Center
- 2) Microsoft Purview Portal > Permissions & Roles > Purview Roles (Old name was "Microsoft 365 Compliance Portal")
- 3) Microsoft Endpoint Manager Admin Center

upvoted 4 times

You have an Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant. The tenant uses pass-through authentication.

A corporate security policy states the following:

- Domain controllers must never communicate directly to the internet.
- Only required software must be installed on servers.

The Active Directory domain contains the on-premises servers shown in the following table.

| Name    | Description                               |
|---------|-------------------------------------------|
| Server1 | Domain controller (PDC emulator)          |
| Server2 | Domain controller (infrastructure master) |
| Server3 | Azure AD Connect server                   |
| Server4 | Unassigned member server                  |

You need to ensure that users can authenticate to Azure AD if a server fails.

On which server should you install an additional pass-through authentication agent?

- A. Server4
- B. Server2
- C. Server1
- D. Server3

#### Correct Answer: A

Reference:

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

Community vote distribution

A (91%) 9%

□  **Nilz76** Highly Voted 1 year, 7 months ago

**Selected Answer: A**

Server 4

The standalone Authentication Agents can be installed on any Windows Server 2016 or later, with TLS 1.2 enabled. The server needs to be on the same Active Directory forest as the users whose passwords you need to validate.

upvoted 14 times

□  **EmnCours** Most Recent 4 months, 2 weeks ago

**Selected Answer: A**

Answer A.

upvoted 1 times

□  **dule27** 6 months, 2 weeks ago

**Selected Answer: A**

A: Server 4

upvoted 1 times

□  **yakuzasm** 9 months, 2 weeks ago

server 4 is correct, tested and worked

upvoted 2 times

□  **ANDRESCB1988** 1 year ago

Server 4 is correct

upvoted 1 times

□  **slick\_orange** 1 year, 3 months ago

Agree. A. Server 4. Although it got me confused a bit because I didn't check the answer properly. I always imagine, A. Server 1, B. Server 2, etc. So, be careful during the exam.

upvoted 2 times

□  **Cis** 1 year, 4 months ago

**Selected Answer: A**

Answer A.

upvoted 1 times

□  **Zubairr13** 1 year, 4 months ago

On the exam, 7/23/2022.

upvoted 2 times

 **Tokiki** 1 year, 5 months ago

Agree. A

upvoted 2 times

 **shine98** 1 year, 5 months ago

On the exam - June 12, 2022

upvoted 1 times

 **bleedinging** 1 year, 6 months ago

Gotta be A. Server 3 has it already and if it goes down they won't be able to authenticate.

upvoted 4 times

 **Xyz\_40** 1 year, 5 months ago

correct...

upvoted 1 times

 **Davidf** 1 year, 6 months ago

Server 4 since DCs cannot talk to the internet and server 3 already has it presumably

upvoted 3 times

 **Nilz76** 1 year, 7 months ago

**Selected Answer: A**

This question was in the exam 28/April/2022

upvoted 3 times

 **Nilz76** 1 year, 7 months ago

**Selected Answer: D**

Server 4

The standalone Authentication Agents can be installed on any Windows Server 2016 or later, with TLS 1.2 enabled. The server needs to be on the same Active Directory forest as the users whose passwords you need to validate.

upvoted 2 times

 **Nilz76** 1 year, 7 months ago

Correction, wrong vote on Selected Answer, Should be Selected Answer A.

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1. A contractor uses the credentials of user1@outlook.com. You need to ensure that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com. What should you do?

- A. Run the New-AzureADMSInvitation cmdlet.
- B. Configure the External collaboration settings.
- C. Add a WS-Fed identity provider.
- D. Implement Azure AD Connect.

**Correct Answer: A**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal>

<https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0>

*Community vote distribution*

A (83%)      B (17%)

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

**Selected Answer: A**

A is the answer, they are looking for you to invite the user to azure ad. Assume that unless stated otherwise, default config in Azure AD is set, so collaboration settings are already on. "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." <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure>  
upvoted 15 times

 **Hot\_156** Highly Voted 1 year, 2 months ago

**Selected Answer: A**

This is the same question as 14. There you answer that "create a guest account" but here you all are saying "you need to configure collaboration settings". Think about it, if that would be the correct answer you shouldn't have it as an option on question number 14 but you have it there...

It is A

upvoted 12 times

 **acsoma** 3 months, 3 weeks ago

You are right in Question the cmd-let creates a new AZ Ad user account... the difference is that between the cmd-lets.

current question's answer is: A

upvoted 1 times

 **haazybanj** Most Recent 4 weeks ago

**Selected Answer: A**

The best answer is A. Run the New-AzureADMSInvitation cmdlet.

The New-AzureADMSInvitation cmdlet is used to invite a guest user to your Azure AD tenant. To use the New-AzureADMSInvitation cmdlet, you will need the contractor's email address and the name of the Azure AD application that you want to give them access to.

upvoted 1 times

 **EmnCours** 4 months, 2 weeks ago

**Selected Answer: A**

A. Run the New-AzureADMSInvitation cmdlet.

upvoted 1 times

 **vietnam** 4 months, 2 weeks ago

The wording say not "invite user" but "make sure you can invite user" therefore B

upvoted 1 times

 **dule27** 6 months, 2 weeks ago

**Selected Answer: A**

A. Run the New-AzureADMSInvitation cmdlet.

upvoted 1 times

 **AMDF** 11 months, 4 weeks ago

**Selected Answer: A**

A is correct  
upvoted 3 times

**pikapin** 1 year, 2 months ago

In exam 29/Sep  
upvoted 1 times

**DeepMoon** 1 year, 2 months ago

Key words are: "You need to ensure that you can provide the contractor with access to App1." Which means you need to setup the following screen for @outlook account to work. Under collaboration settings.  
<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/self-service-sign-up-user-flow#create-the-user-flow-for-self-service-sign-up>

upvoted 1 times

**Holii** 5 months, 4 weeks ago

- 1.) Configure External Collaboration Settings
- 2.) Create a User Flow
- 3.) Link user flow to the application

While this would achieve the long-term best practice of the solution, it is too many steps and doesn't achieve the "What should you do"

Running New-AzureADMSInvitation will provide an external user account that they can use to start authenticating immediately.

The other solution, although 'correct', has too many steps not included by just saying "Configure the settings"

upvoted 1 times

**Seed001** 1 year, 4 months ago

**Selected Answer: B**

Question is asking the prerequisite of A, so I'll go for B.  
upvoted 3 times

**kangtamo** 1 year, 4 months ago

**Selected Answer: A**

I would go with A.  
upvoted 1 times

**Tokiki** 1 year, 5 months ago

A is answer  
upvoted 1 times

**Mike8899** 1 year, 5 months ago

B:  
By default all users can invite guest users.  
To access to App1. Add applications to the self-service sign-up user flow under configure external collaboration settings.  
upvoted 2 times

**kanew** 7 months, 1 week ago

A) because guest self-sign up via user flow (i.e. for apps ) is disabled by default but it states if it is then the guest must be invited. A) will therefore work no matter this setting  
upvoted 1 times

**RandomNickname** 1 year, 5 months ago

**Selected Answer: A**

A looks correct.  
By default all users can invite guest users, since the question doesn't state otherwise.  
A: is correct, since you just need to invite the user.  
upvoted 5 times

**shine98** 1 year, 5 months ago

On the exam - June 12, 2022  
upvoted 1 times

**GioGio** 1 year, 5 months ago

Which was your answer?  
upvoted 1 times

**Benkyoujin** 1 year, 6 months ago

**Selected Answer: B**

Isn't it B? The question asks that you need to ensure that you can add the user. Doesn't that imply you should check the settings first, and only run the powershell after? Poorly worded.  
upvoted 5 times

**slick\_orange** 1 year, 3 months ago

I agree with you. i guess that's the trick. "You need to ENSURE that you CAN provide". And it's not "You need to provide." So, I'd go with B.

upvoted 2 times

✉️ **sapien45** 1 year, 5 months ago

Perfectly worded question, you are just very confused, my friend

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 5 times

✉️ **Nilz76** 1 year, 7 months ago

Or... if you have the Microsoft Graph Identity Sign-ins PowerShell Module Installed, you can use:

Invitation:

```
New-MgInvitation -InvitedUserDisplayName "User 1" -InvitedUserEmailAddress user1@outlook.com -InviteRedirectUrl  
"https://myapplications.microsoft.com" -SendInvitationMessage:$true
```

To verify:

```
Get-MgUser -Filter "Mail eq 'user1@outlook.com'"
```

upvoted 2 times

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users. From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users. You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort. What should you use?

- A. the Administrative units blade in the Azure Active Directory admin center
- B. the Set-AzureAdUser cmdlet
- C. the Groups blade in the Azure Active Directory admin center
- D. the Set-MsolUserLicense cmdlet

**Correct Answer: D**

The Set-MsolUserLicense cmdlet updates the license assignment for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

- 1. the Licenses blade in the Azure Active Directory admin center
- 2. the Set-MsolUserLicense cmdlet

Other incorrect answer options you may see on the exam include the following:

- ☞ the Identity Governance blade in the Azure Active Directory admin center
- ☞ the Set-WindowsProductKey cmdlet
- ☞ the Set-AzureAdGroup cmdlet

Reference:

<https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0>

*Community vote distribution*

D (100%)

✉  **bleedinging**  1 year, 6 months ago

The Set-MsolUserLicense cmdlet is deprecated. You'd use Set-MgUserLicense now.  
upvoted 10 times

✉  **sapien45** 1 year, 5 months ago

Not yet deprecated

The Set-MsolUserLicense and New-MsolUser (-LicenseAssignment) cmdlets are scheduled to be retired. Please migrate your scripts to the Microsoft Graph SDK's Set-MgUserLicense cmdlet as described above  
upvoted 4 times

✉  **JimboJones99**  1 month, 2 weeks ago

**Selected Answer: D**

Although Set-MsolUserLicense is set to be retired, it is still valid at the time of writing this comment.

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/remove-licenses-from-user-accounts-with-microsoft-365-powershell?view=o365-worldwide>  
upvoted 2 times

✉  **sherifhamed** 2 months, 2 weeks ago

But isn't it true that,  
The Set-MsolUserLicense cmdlet is a valid PowerShell cmdlet used for managing license assignments for individual users in Microsoft 365. It allows you to add, remove, or modify licenses for a specific user.  
upvoted 2 times

✉  **EmnCours** 3 months, 3 weeks ago

**Selected Answer: D**

D. the Set-MsolUserLicense cmdlet  
upvoted 1 times

✉  **dule27** 5 months, 1 week ago

**Selected Answer: D**

D. the Set-MsolUserLicense cmdlet  
upvoted 1 times

ShoaibPKDXB 6 months, 3 weeks ago

**Selected Answer: D**

D: Set-MsolUserLicense  
upvoted 2 times

[Removed] 11 months, 4 weeks ago

**Selected Answer: D**

D is the correct answer here, although MS documentation suggests the cmdlet is deprecated.  
upvoted 1 times

giver 1 year, 4 months ago

Q % - same question. community selected remove from license from the blade.  
upvoted 1 times

Dimonchik 12 months ago

For 2500 users? Well... the community like a million of flies- they can't make a mistake.  
upvoted 1 times

martinods 1 year, 2 months ago

in the question 4 "use the Licenses blade in the Azure Active Directory admin center" is the only plausible solutions. in this question we have also Set-MsolUserLicense cmdlet  
upvoted 2 times

rachee 1 year, 4 months ago

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/remove-licenses-from-user-accounts-with-microsoft-365-powershell?view=o365-worldwide>  
upvoted 1 times

Tokiki 1 year, 5 months ago

D is correct  
upvoted 1 times

Benkyoujin 1 year, 6 months ago

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365-powershell?view=o365-worldwide>  
upvoted 1 times

**HOTSPOT -**

You have an Azure Active Directory (Azure AD) tenant and an Azure web app named App1.

You need to provide guest users with self-service sign-up for App1. The solution must meet the following requirements:

- ⇒ Guest users must be able to sign up by using a one-time password.
- ⇒ The users must provide their first name, last name, city, and email address during the sign-up process.

What should you configure in the Azure Active Directory admin center for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

One-time password:

- A linked subscription
- An identity provider
- Azure AD Privileged Identity Management (PIM)**
- The External collaboration settings

User details:

- A user flow**
- Access reviews
- An access package
- The tenant properties

Correct Answer:

**Answer Area**

One-time password:

- A linked subscription
- An identity provider**
- Azure AD Privileged Identity Management (PIM)**
- The External collaboration settings

User details:

- A user flow**
- Access reviews
- An access package
- The tenant properties

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/identity-providers> <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/self-service-sign-up-overview>

IMO it's more of a tricky wording and manipulative question, but the answer is correct. In simple word:

1. is about OTP setting: which comes under "External Identities" > All identity providers, Select Email one-time passcode. Link:

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure#configure-settings-in-the-portal>

2. Question is about self service sign in setting: which comes under External Identities > External collaboration settings---Under Enable guest self-service sign up via user flows, select Yes. Link: <https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure#configure-settings-in-the-portal>

Honestly with more than 27 years in the field, I don't get why some vendors put such memory-specific questions rather than testing concepts and engineers ability to find the required detail when from documentations

upvoted 18 times

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

- 1.) External Collaboration Settings - We need to verify that the self-service sign up via user flows is enabled.
- 2.) User Flow - Email one-time passcode is already a selectable option.

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/self-service-sign-up-user-flow#enable-self-service-sign-up-for-your-tenant>

upvoted 1 times

✉ **EmnCours** 3 months, 3 weeks ago

One-Time Password: an Identity Provider  
User Details: a user flow  
upvoted 3 times

✉ **venumurki** 5 months, 3 weeks ago

- 1) One-time passcode will be configured as one of the IDP which is under "All Identity Providers" blade and 2) User Flow
- upvoted 3 times

✉ **dule27** 5 months, 3 weeks ago

One-Time Password: an Identity Provider  
User Details: a user flow  
upvoted 2 times

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

Correct. An Identity provider and User flow  
upvoted 1 times

✉ **f2bf85a** 8 months ago

Why Box 1 should be "An Identity Provider"??  
You first have to enable self-service sign-up from the "External Collaboration Settings".  
If you do that, "Email one-time passcode" identity provider is already added and enabled by default...  
upvoted 2 times

✉ **Holii** 5 months, 4 weeks ago

This. No idea why people are suggesting an IdP.  
No where in this is it suggested that we require/the users are using a third-party IdP that isn't currently registered...

Email one-time passcode is already an established IdP by default...

- 1.) External Collaboration Settings - We need to verify that the self-service sign up via user flows is enabled.
- 2.) User Flow - Email one-time passcode is already a selectable option.

upvoted 2 times

✉ **Holii** 5 months, 4 weeks ago

The only thing I hate is how it's a dual question.

"What do you need to configure One-Time password?"  
"What do you need to configure User details?"

Technically, you don't modify the External Collaboration Settings for One-time Password, you would modify it for the end-goal of user flow...the only place you modify its settings is in the Identity Providers blade.

Context of this question is terrible, but I thought about it some more and I think it's

- 1.) an Identity Provider

2.) User Flow

upvoted 2 times

✉ **ccaitlab** 1 year ago

The given answer is correct. <https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode#to-enable-or-disable-email-one-time-passcodes>

upvoted 3 times

✉ **Magis** 1 year, 1 month ago

Correct.

- First you'll enable self-service sign-up for your tenant and federate with the identity providers you want to allow external users to use for sign-in. Then you'll create and customize the sign-up user flow and assign your applications to it.

upvoted 2 times

□ **TheMCT** 1 year, 2 months ago

The given answer is correct. The Email one-time passcode is now moved to All Identity Providers:

Box 1 -> Identity Provider

Box 2 -> User Flow

upvoted 4 times

□ **Moezey** 1 year, 2 months ago

aNSWER IS WRONG. tHE ANSWER IS EXTERNAL COLLABORATION SETTINGS AND USER FLOW

upvoted 1 times

□ **Holii** 5 months, 3 weeks ago

It's a dual-part question..

"What do you need to configure One-Time Password:"

You need an Identity Provider. You don't configure OTP through the External Collaboration Settings.

"What do you need to configure User Details:"

You need a user flow to configure all the appropriate attributes.

It's a bit confusing, but break it down into the two parts that the question is asking.

upvoted 1 times

□ **nhmh90** 12 months ago

I think guest setting, refer question 3

upvoted 2 times

□ **taer** 1 year, 2 months ago

correct

upvoted 1 times

You have an Azure Active Directory (Azure AD) Azure AD tenant.

You need to bulk create 25 new user accounts by uploading a template file.

Which properties are required in the template file?

- A. displayName, identityIssuer, usageLocation, and userType
- B. accountEnabled, givenName, surname, and userPrincipalName
- C. accountEnabled, displayName, userPrincipalName, and passwordProfile**
- D. accountEnabled, passwordProfile, usageLocation, and userPrincipalName

**Correct Answer: C**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-add>

Community vote distribution

C (100%)

 **Nyamnyam** 4 weeks, 1 day ago

Has anyone payed attention to the accountEnabled attribute? It should be set to \$True. But in the CSV-file it is referred as "block sign in", which should be "No". So No = \$True? What have MSFT employees smoked when developing the CSV upload interface? ;)

upvoted 1 times

 **amurp35** 3 months, 2 weeks ago

The correct answer is C, but according to the CSV in the Microsoft doc, the column names are a bit different: "The only required values are Name, User principal name, Initial password and Block sign in (Yes/No)."

upvoted 1 times

 **EmnCours** 4 months, 2 weeks ago

**Selected Answer: C**

Correct Answer: C

upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: C**

C. accountEnabled, displayName, userPrincipalName, and passwordProfile

upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: C**

Correct. C

upvoted 1 times

 **kerimnl** 1 year, 1 month ago

**Selected Answer: C**

Correct Answer is: C

Name [displayName] -> Required

User name [userPrincipalName] -> Required

Initial password [passwordProfile] -> Required,

Block sign in (Yes/No) [accountEnabled] -> Required

upvoted 3 times

 **TheMCT** 1 year, 2 months ago

Given answer , C, is correct. The required fields in the template include Name [displayName] Required User name [userPrincipalName] Required Initial password [passwordProfile] Required Block sign in (Yes/No) [accountEnabled] Required

upvoted 1 times

 **DeepMoon** 1 year, 2 months ago

None of the 4 possible answers have all the selections as mentioned in @zed026 's link.

But C is the most likely given the answer choices.

This is a question that may evolve over time to have the correct answers.

upvoted 1 times

 **birrach** 1 year, 2 months ago

**Selected Answer: C**

You can see it in the Template  
upvoted 2 times

✉ **zed026** 1 year, 3 months ago

Open the CSV file and add a line for each user you want to create. The only required values are Name, User principal name, Initial password and Block sign in (Yes/No). Then save the file. <https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-add#to-create-users-in-bulk>

upvoted 3 times

✉ **Cepheid** 11 months, 1 week ago

So basically, none of the provided answers is correct.

upvoted 1 times

✉ **ThotSlayer69** 10 months, 2 weeks ago

C has all of them though? (Name, user name, password and block sign-in) Why would you say this?

upvoted 1 times

✉ **ThotSlayer69** 10 months, 2 weeks ago

That last part sounds aggressive upon reread, apologies. Didn't mean for it to come off like that

upvoted 2 times

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant.

Users sign in to computers that run Windows 10 and are joined to the domain.

You plan to implement Azure AD Seamless Single Sign-On (Azure AD Seamless SSO).

You need to configure the Windows 10 computers to support Azure AD Seamless SSO.

What should you do?

- A. Configure Sign-in options from the Settings app.
- B. Enable Enterprise State Roaming.
- C. Modify the Intranet Zone settings.**
- D. Install the Azure AD Connect Authentication Agent.

**Correct Answer: C**

Reference:

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

*Community vote distribution*

C (100%)

 **jcano** Highly Voted 2 years, 1 month ago

Answer is C.

You can gradually roll out Seamless SSO to your users using the instructions provided below. You start by adding the following Azure AD URL to all or selected users' Intranet zone settings by using Group Policy in Active Directory:

<https://autologon.microsoftazuread-sso.com>

In addition, you need to enable an Intranet zone policy setting called Allow updates to status bar via script through Group Policy.  
more information in:

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

upvoted 17 times

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

20% of the questions coming from this dump, the rest of the questions are new even the case study. Please read through the discussions and understand how it works so you can still answer even if the question is new.

upvoted 15 times

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

**Selected Answer: C**

Correct Answer: C

upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: C**

C. Modify the Intranet Zone settings.

upvoted 2 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: C**

Correct: C

upvoted 1 times

 **Zubairr13** 1 year, 4 months ago

On the exam, 7/23/2022.

upvoted 3 times

 **ali\_pin** 1 year, 5 months ago

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

upvoted 2 times

 **shine98** 1 year, 5 months ago

On the exam - June 12, 2022

upvoted 3 times

 **petercorn** 1 year, 6 months ago

**Selected Answer: C**

Answer in Step 3: Roll out the feature

upvoted 1 times

 **POOUAGA** 1 year, 7 months ago

Agree the answer is C

upvoted 1 times

 **Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022

upvoted 1 times

 **Miguelin11** 1 year, 8 months ago

Hi all, I completed the exam on 31/03/2022. Keep in mind that if you don't have a background in Azure Identity Access management and you rely entirely on the questions presented here you will be disappointed. There are several questions in the exam from this. However, they are new business cases as well as other questions and even answers are different. You may want to consult other training material if this is your only reference to study or learn the questions here but also study the Microsoft material which is offered for free.

upvoted 7 times

 **Silent\_Muzinde** 1 year, 8 months ago

ANSWER C: <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start#step-3-roll-out-the-feature>  
upvoted 2 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

 **Sh1rub10** 1 year, 8 months ago

**Selected Answer: C**

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

upvoted 1 times

 **WMG** 1 year, 8 months ago

**Selected Answer: C**

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

upvoted 1 times

 **WS\_21** 1 year, 8 months ago

**Selected Answer: C**

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

upvoted 1 times

**DRAG DROP -**

You need to resolve the recent security incident issues.

What should you configure for each incident? To answer, drag the appropriate policy types to the correct issues. 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.

Select and Place:

**Policy Types**

An authentication method policy

A Conditional Access policy

A sign-in risk policy

A user risk policy

**Answer Area**

Leaked credentials:

A sign-in from a suspicious browser:

Resources accessed from an anonymous IP address:

**Correct Answer:****Policy Types**

An authentication method policy

A Conditional Access policy

A sign-in risk policy

A user risk policy

**Answer Area**

Leaked credentials:

A user risk policy

A sign-in from a suspicious browser:

A sign-in risk policy

Resources accessed from an anonymous IP address:

A sign-in risk policy

Box 1: A user risk policy -

User-linked detections include:

Leaked credentials: This risk detection type indicates that the user's valid credentials have been leaked. When cybercriminals compromise valid passwords of legitimate users, they often share those credentials.

User risk policy.

Identity Protection can calculate what it believes is normal for a user's behavior and use that to base decisions for their risk. User risk is a calculation of probability that an identity has been compromised. Administrators can make a decision based on this risk score signal to enforce organizational requirements. Administrators can choose to block access, allow access, or allow access but require a password change using Azure AD self-service password reset.

Box 2: A sign-in risk policy -

Suspicious browser: Suspicious browser detection indicates anomalous behavior based on suspicious sign-in activity across multiple tenants from different countries in the same browser.

Box 3: A sign-in risk policy -

A sign-in risks include activity from anonymous IP address: This detection is discovered by Microsoft Defender for Cloud Apps. This detection identifies that users were active from an IP address that has been identified as an anonymous proxy IP address.

Note: The following three policies are available in Azure AD Identity Protection to protect users and respond to suspicious activity. You can choose to turn the policy enforcement on or off, select users or groups for the policy to apply to, and decide if you want to block access at sign-in or prompt for additional action.

\* User risk policy

Identifies and responds to user accounts that may have compromised credentials. Can prompt the user to create a new password.

\* Sign in risk policy

Identifies and responds to suspicious sign-in attempts. Can prompt the user to provide additional forms of verification using Azure AD Multi-Factor Authentication.

\* MFA registration policy

Makes sure users are registered for Azure AD Multi-Factor Authentication. If a sign-in risk policy prompts for MFA, the user must already be registered for Azure AD Multi-Factor Authentication.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

□  **0byte** Highly Voted 1 year, 1 month ago

The given answer is correct.

Currently supported risk detections are

Sign-in risk detections:

Activity from anonymous IP address

Additional risk detected

Admin confirmed user compromised

Anomalous Token

Anonymous IP address

Atypical travel

Azure AD threat intelligence

Impossible travel

Malicious IP address

Malware linked IP address

Mass Access to Sensitive Files

New country

Password spray

Suspicious browser

Suspicious inbox forwarding

Suspicious inbox manipulation rules

Token Issuer Anomaly

Unfamiliar sign-in properties

User risk detections:

Additional risk detected

Anomalous user activity

Azure AD threat intelligence

Leaked credentials

Possible attempt to access Primary Refresh Token (PRT)

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

upvoted 17 times

□  **chikorita** 8 months, 1 week ago

why "Azure AD threat intelligence" is part of both?

upvoted 1 times

□  **Holii** 5 months, 4 weeks ago

Azure AD Threat Intelligence are real-time detections on user behavior using machine learning. It's not tied to one type of "User Risk" vs "Sign-in Risk", it scans all sorts of behaviors for anything that may be illegitimate/malicious traffic.

No link to provide, just look it into it yourself.

upvoted 1 times

□  **EmnCours** Most Recent 3 months, 3 weeks ago

1. A user risk policy

2. A sign-in risk policy

3. A sign-in risk policy

upvoted 2 times

□  **dule27** 5 months, 1 week ago

1. A user risk policy

2. A sign-in risk policy

3. A sign-in risk policy

upvoted 3 times

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

Correct

upvoted 1 times

□  **chzon** 8 months, 2 weeks ago

Today I would solve all over Conditional Access.

upvoted 4 times

□  **syougun200x** 2 months, 3 weeks ago

I would go for conditional access policy for all the choices, too. When I open user risk policy or sign in risk policy, the below appears at the top of the page.

We recommend migrating user risk policy (or sign in risk policy) to Conditional access policy for more conditions and controls.

Maybe you're the only one who bothered to go hands on here.

upvoted 1 times

 den5\_pepito83 1 year ago

ON EXAM 14/11/2022

upvoted 3 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

## HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name  | User type | Directory synced |
|-------|-----------|------------------|
| User1 | Member    | Yes              |
| User2 | Member    | No               |
| User3 | Guest     | No               |

For which users can you configure the Job title property and the Usage location property in Azure AD? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Job title property:

- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Usage location property:

- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Correct Answer:

Job title property:

- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Usage location property:

- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Box 1: User1 and User2 only.

You can add or update a user's profile information using Azure Active Directory.

Add user profile information, including a profile picture, job-specific information, and some settings using Azure Active Directory (Azure AD).

The user profile includes:

Job info. Add any job-related information, such as the user's job title, department, or manager.

Box 2: User1, User2, and User3 -

Invite users with Azure Active Directory B2B collaboration, Update user's name and usage location.

To assign a license, the invited user's Usage location must be specified. Admins can update the invited user's profile on the Azure portal.

1. Go to Azure Active Directory > Users and groups > All users. If you don't see the newly created user, refresh the page.

2. Click on the invited user, and then click Profile.
3. Update First name, Last name, and Usage location.
4. Click Save, and then close the Profile blade.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-profile-azure-portal>

<https://docs.microsoft.com/en-us/power-platform/admin/invite-users-azure-active-directory-b2b-collaboration#update-users-name-and-usage-location>

✉ **Faheem2020** Highly Voted 1 year, 2 months ago

Option to edit job title appears greyed out for on-premise synced users, usage location can be modified  
I would go for the following answers

1. User2 and User3 only
2. User1, User2 and user3

upvoted 62 times

✉ **jack987** 11 months, 2 weeks ago

I agree. The correct answer is:

1. User2 and User3 only
2. User1, User2 and User3

I tested it in our environment. The option to edit the job title for an on-premise synced user is greyed out. You will have to change the job title for an on-premise synced user from on-prem AD.

Usage location is available for all types of users.

upvoted 8 times

✉ **kanew** 7 months ago

Agree 100% and tested.

upvoted 4 times

✉ **Silusha** 2 months, 1 week ago

Did you try to change the job title of User3?

upvoted 1 times

✉ **sbnpj** 8 months ago

agree with above answers. you cannot modify directory synced user's properties in azure ad.

upvoted 3 times

✉ **Magis** 1 year, 1 month ago

Agree. This answer is correct for sure.

upvoted 5 times

✉ **referme** Highly Voted 1 year, 3 months ago

Tested this in my lab. Job title property for directory synched users cannot be updated from Azure AD. So correct answer for the same is user 2 and user 3.

upvoted 15 times

✉ **Fcnet** 1 year, 1 month ago

Job Title : only user2 & user3  
Usage Location can be changed for U1,U2,U3  
upvoted 1 times

✉ **SvenHorsheim** 1 year ago

If they are directory synced, sure you can change usage location in AAD portal, but it will change back after a directory sync if it differs from what is in AD users and computers. I have personally run into this in our tenant at work where the telecom guys needed to change a usage to the US from another country in order to assign a license to allow for teams calling. They would change it in AAD and then find it had reverted within 30 min.

So that said I don't know where this answer actually falls in Microsoft's perspective because sure you can manipulate the setting in AAD, but it won't stick past the next directory sync.

upvoted 6 times

✉ **Holii** 5 months, 4 weeks ago

This, I have run into the same with my work... but the people at MSFT running the exams probably don't work with this.

So;

- 1.) 2/3
- 2.) 1/2/3

upvoted 1 times

✉ **JckD4Ni3L** Most Recent 1 month, 3 weeks ago

I do this often,

1. User2/user3 only, you can't modify job title on synced user in Entra ID.
2. User1/user2/user3

upvoted 3 times

✉ **Silusha** 2 months, 1 week ago

"Job Title" property for Azure Active Directory guest users through standard settings in the Azure portal.

I would go for the following answers

1. User2 only
2. User1, User2 and user3

upvoted 1 times

□ **AK\_1234** 1 month, 3 weeks ago

Correct answer:

- U2 and U3
- U1, U2 and U3

upvoted 1 times

□ **StarMe** 3 months, 2 weeks ago

The correct answer is

1. User 2 and User 3
2. User 1, User 2 and User 3

I have checked the above in my Azure AD tenant.

upvoted 1 times

□ **EmnCours** 3 months, 3 weeks ago

1. User2 and User3 only
2. User1, User2 and User3

upvoted 1 times

□ **Heshan** 4 months, 4 weeks ago

On the exam, 09/07/2023

upvoted 3 times

□ **Sango** 5 months ago

User 2 and 3 only. This is because User 1 is Directory Synchronized and can only be changed from Local AD, not Azure AD. The Second part is User1, User2 and User3.

upvoted 1 times

□ **dule27** 6 months ago

Job Title : User2 and User3 only  
Usage Location: User1,User2 and User3  
upvoted 1 times

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

Correct: 1. User2 and User3 only  
2. User1, User2 and user3  
upvoted 1 times

□ **ShoaibPKDXB** 6 months, 4 weeks ago

1. User and User 3 only
2. User1, User2 and User3

upvoted 1 times

□ **ShoaibPKDXB** 6 months, 4 weeks ago

Correct  
upvoted 1 times

□ **rajbne** 7 months, 3 weeks ago

Please update the final answer as per discussion ?  
upvoted 1 times

□ **raymond2018** 9 months, 2 weeks ago

The statement does not mentioned that it has AD On Premise.  
The provided answers are correct..  
upvoted 1 times

Yes it does. The first account is directory synced and therefore connected to an AD on-prem. Correct answer is:

Job Title - User 2 and 3

Usage Location - User 1,2 and 3

upvoted 3 times

□ **wsrudmen** 10 months, 2 weeks ago

JobTitle: User1 and User3 only

You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory.

UsageLocation: User1, User2, and User3

Usage location is an Azure property that can only be modified from Azure AD (for all users including Windows Server AD users synced via Azure AD Connect).

upvoted 1 times

□ **wsrudmen** 10 months, 2 weeks ago

Typo issue. For JobTitle => User 2 and User3  
upvoted 1 times

 **Vlako** 10 months, 3 weeks ago

Just tested, Usage location can be modified on dirsynced user.  
upvoted 2 times

 **Nazir97** 10 months, 4 weeks ago

Correct answer is

1. User 2 and User 3 only
2. All users

See a similar question from AZ-104: <https://www.examtopics.com/discussions/microsoft/view/38424-exam-az-104-topic-2-question-32-discussion/>

upvoted 3 times

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.  
You need to ensure that User1 can create new catalogs and add resources to the catalogs they own.  
What should you do?

- A. From the Roles and administrators blade, modify the Groups administrator role.
- B. From the Roles and administrators blade, modify the Service support administrator role.
- C. From the Identity Governance blade, modify the Entitlement management settings.**
- D. From the Identity Governance blade, modify the roles and administrators for the General catalog.

**Correct Answer: C**

Create and manage a catalog of resources in Azure AD entitlement management.

Create a catalog.

A catalog is a container of resources and access packages. You create a catalog when you want to group related resources and access packages. A user who has been delegated the catalog creator role can create a catalog for resources that they own. Whoever creates the catalog becomes the first catalog owner. A catalog owner can add more users, groups of users, or application service principals as catalog owners.

Prerequisite roles: Global administrator, Identity Governance administrator, User administrator, or Catalog creator.

Incorrect:

\* Groups Administrator - Members of this role can create/manage groups, create/manage groups settings like naming and expiration policies, and view groups activity and audit reports.

\* Service Support Administrator

Users with this role can create and manage support requests with Microsoft for Azure and Microsoft 365 services, and view the service dashboard and message center in the Azure portal and Microsoft 365 admin center.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-catalog-create>

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

Community vote distribution

|         |    |
|---------|----|
| C (95%) | 5% |
|---------|----|

 **Hot\_156** Highly Voted 1 year, 2 months ago

**Selected Answer: C**

Delegate entitlement management

By default, only Global Administrators and User Administrators can create and manage catalogs, and can manage all catalogs. Users added to entitlement management as Catalog creators can also create catalogs and will become the owner of any catalogs they create.

upvoted 14 times

 **syougun200x** 2 months, 3 weeks ago

Thank you. As of today, the same sentence can be seen in the setting section.

upvoted 1 times

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

Correct link with reasoning: <https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-delegate-catalog#as-an-it-administrator-delegate-to-a-catalog-creator>

upvoted 6 times

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

**Selected Answer: C**

[https://portal.azure.com/#view/Microsoft\\_AAD\\_ERM/DashboardBlade/~/elmSetting](https://portal.azure.com/#view/Microsoft_AAD_ERM/DashboardBlade/~/elmSetting)

Correct. C

upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: C**

C. From the Identity Governance blade, modify the Entitlement management settings.

upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: C**

Correct. C  
upvoted 1 times

 **eleazarrrd** 7 months, 2 weeks ago

**Selected Answer: D**  
La respuesta correcta es D. Desde la hoja Identity Governance, modifique los roles y administradores para el catálogo general.

Para permitir que el usuario Usuario1 pueda crear nuevos catálogos y agregar recursos a los catálogos que posee, debemos conceder los permisos necesarios a través de los roles y administradores del catálogo. La opción correcta para esto es la D. Desde la hoja Identity Governance, modifique los roles y administradores para el catálogo general.

En la hoja de Identity Governance, podemos administrar los derechos de acceso y los permisos de los usuarios para diferentes recursos en Azure AD. Al modificar los roles y administradores para el catálogo general, podemos agregar a Usuario1 como administrador del catálogo o asignarle un rol que le permita crear y administrar los recursos en el catálogo.

Las opciones A y B no son relevantes para el objetivo dado y la opción C es para la administración de derechos de acceso en general, pero no específicamente para los catálogos y recursos en Azure AD.

upvoted 1 times

 **francescoc** 8 months, 1 week ago

**Selected Answer: C**  
C is correct  
"Prerequisite roles: Global administrator, Identity Governance administrator, User administrator, or Catalog creator"  
<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-catalog-create>  
upvoted 1 times

 **[Removed]** 11 months, 4 weeks ago

**Selected Answer: C**  
Correct answer is C.  
upvoted 1 times

 **lme** 1 year, 2 months ago

on the exam 09222022, i answered the same. Passed the exam, btw.  
upvoted 3 times

 **Hot\_156** 1 year, 2 months ago

roles and administrators for the General catalog can manage catalogs but not create them so the answer is C  
upvoted 2 times

 **Kamal\_SriLanka** 1 year, 2 months ago

The Answer is D my Friend  
upvoted 1 times

 **Hot\_156** 1 year, 2 months ago

test it and then come back and tell us what was the result :)  
upvoted 3 times

 **Ltf** 1 year, 2 months ago

Seems it's D  
upvoted 3 times

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant.

Users sign in to computers that run Windows 10 and are joined to the domain.

You plan to implement Azure AD Seamless Single Sign-On (Azure AD Seamless SSO).

You need to configure the Windows 10 computers to support Azure AD Seamless SSO.

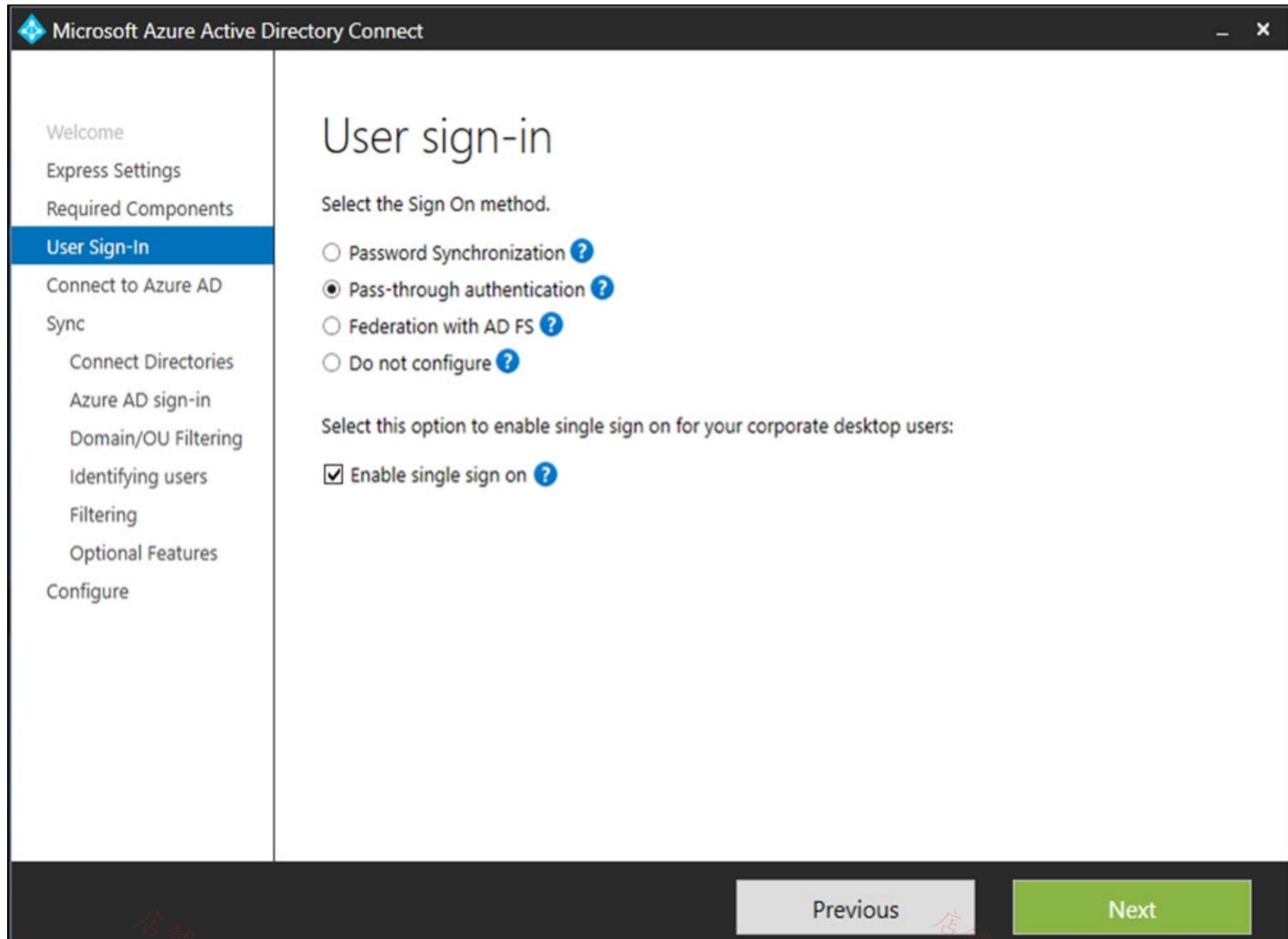
What should you do?

- A. Configure Sign-in options from the Settings app.
- B. Enable Enterprise State Roaming.
- C. Modify the Local intranet Zone settings.
- D. Install the Azure AD Connect Authentication Agent.

**Correct Answer: A**

Enable Seamless SSO through Azure AD Connect.

At the User sign-in page, select the Enable single sign on option.



Note:

The option will be available for selection only if the Sign On method is Password Hash Synchronization or Pass-through Authentication.

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods.

Reference:

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

Community vote distribution

C (100%)

Shinolgarashi Highly Voted 1 year, 3 months ago

The question states: You need to configure the Windows 10 computers to support Azure AD Seamless SSO.

The catch is, "configure the Windows 10 computers."

The answer is C.

This is also a repeated question on the previous page.

upvoted 20 times

 **jack987** 11 months, 2 weeks ago

I agree, the correct answer is C.

upvoted 2 times

 **Taigr** 9 months, 2 weeks ago

Question is same, but possible answers are different. Here is LOCAL zone, and it is different than Intranet zone settings. So set answer si right I think.

upvoted 1 times

 **Taigr** 9 months, 2 weeks ago

OK, back. I found

If your organization is planning to use Seamless SSO, then the following URLs need to be reachable from the computers inside your organization and they must also be added to the user's local intranet zone:

<https://autologon.microsoftazuread-sso.com> (enable with GPO)

<https://aadg.windows.net.nsatc.net> (enable with GPO)

Also, the following setting should be enabled in the user's intranet zone: "Allow status bar updates via script." Use GPO for this operation.

upvoted 1 times

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

Answer is C

upvoted 1 times

 **BenLam** 1 month, 1 week ago

The link for the quick start shows the answer which is C. Scroll down to the Roll out the feature section.

upvoted 1 times

 **MrMicrosoft** 1 month, 2 weeks ago

**Selected Answer: C**

As in the previous page, answer is C.

upvoted 1 times

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: C**

C. Modify the Local intranet Zone settings.

To configure the Windows 10 computers to support Azure AD Seamless SSO, you need to modify the Local intranet Zone settings in Internet Explorer or Microsoft Edge. You need to add the following URL to the Local intranet Zone: <https://autologon.microsoftazuread-sso.com>. This will allow the browser to send the Kerberos ticket to Azure AD and enable Seamless SSO

upvoted 1 times

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: C**

ChatGPT Answer:

To configure Windows 10 computers to support Azure AD Seamless Single Sign-On (Azure AD Seamless SSO), you should:

C. Modify the Local intranet Zone settings.

upvoted 1 times

 **amurp35** 3 months, 2 weeks ago

**Selected Answer: C**

Answer is C

upvoted 1 times

 **EmnCours** 4 months, 2 weeks ago

**Selected Answer: C**

I agree, the correct answer is C.

upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: C**

C. Modify the Local intranet Zone settings.

upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **DCT** 9 months ago

walao, answer is C la, sohai

upvoted 1 times

 **mayleni** 10 months, 2 weeks ago

**Selected Answer: C**

C is correct also a similar question has the similar answer. Local intranet zone  
upvoted 2 times

 **Halwagy** 10 months, 3 weeks ago

**Selected Answer: C**

Modify the Local intranet Zone settings. as the question asking what you should do over Windows 10 device  
upvoted 2 times

 **chrisp1992** 11 months, 3 weeks ago

**Selected Answer: C**

Correct answer is C  
upvoted 2 times

 **hodkin** 12 months ago

**Selected Answer: C**

Agree, option is C. You need to modify the intranet setting to allow sign on for trusted locations  
upvoted 2 times

 **Kamal\_SriLanka** 1 year, 2 months ago

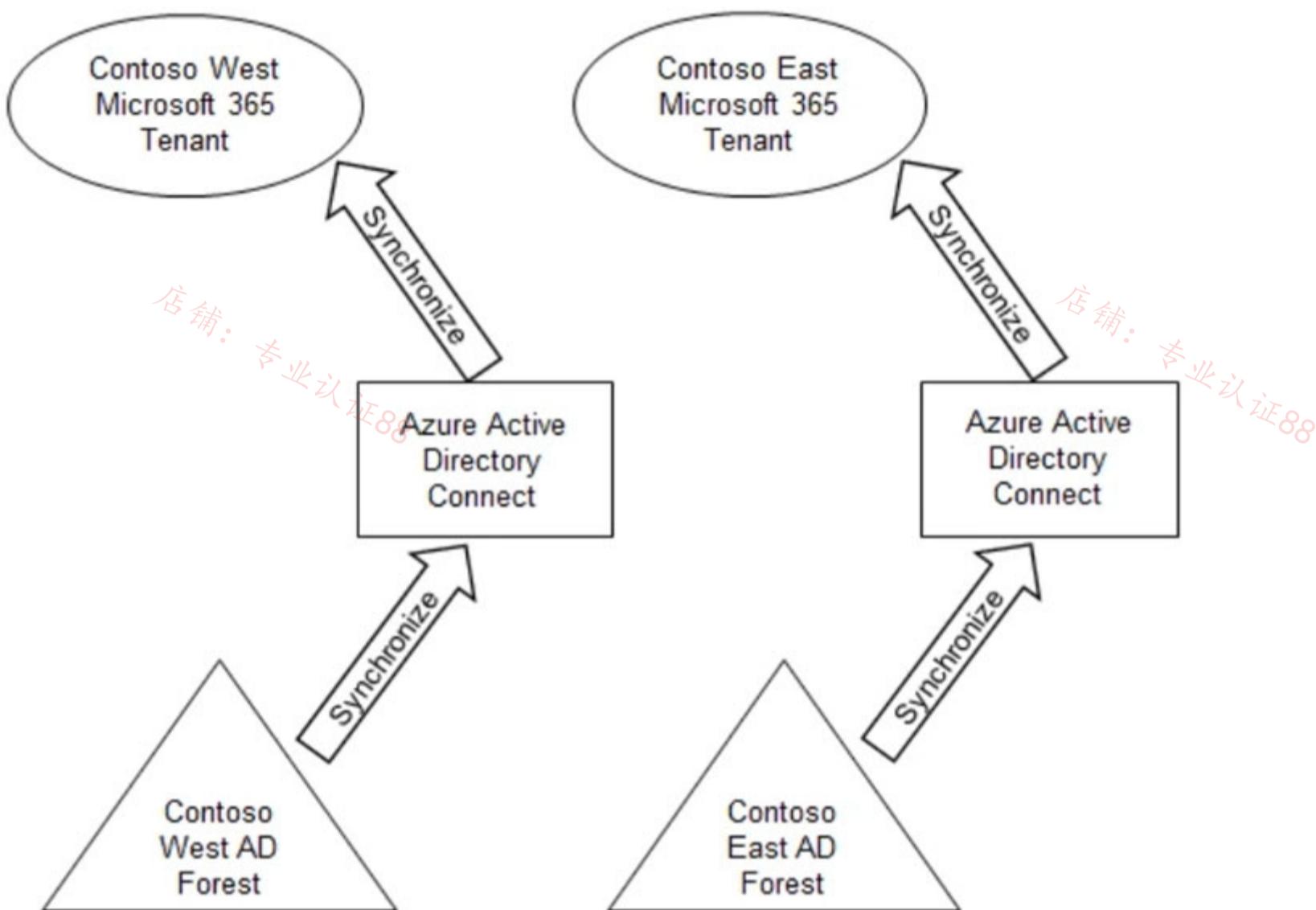
Modify the Local intranet Zone settings.  
upvoted 2 times

 **taer** 1 year, 2 months ago

**Selected Answer: C**

Correct answer is C  
upvoted 2 times

Your company has two divisions named Contoso East and Contoso West. The Microsoft 365 identity architecture for both divisions is shown in the following exhibit.



You need to assign users from the Contoso East division access to Microsoft SharePoint Online sites in the Contoso West tenant. The solution must not require additional Microsoft 365 licenses.

What should you do?

- A. Configure Azure AD Application Proxy in the Contoso West tenant.
- B. Invite the Contoso East users as guests in the Contoso West tenant.**
- C. Deploy a second Azure AD Connect server to Contoso East and configure the server to sync the Contoso East Active Directory forest to the Contoso West tenant.
- D. Configure the existing Azure AD Connect server in Contoso East to sync the Contoso East Active Directory forest to the Contoso West tenant.

**Correct Answer: B**

Before any of your users can grant SharePoint Online team site access to external guests, you will have to enable guest sharing from within Azure Active Directory.

Reference:

<https://redmondmag.com/articles/2020/03/11/guest-access-sharepoint-online-team-sites.aspx> <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/multi-tenant-common-considerations>

*Community vote distribution*

B (100%)

**LHADUK** Highly Voted 1 year ago

it should be stated as answer: configure cross-tenant access settings

upvoted 6 times

**Holii** 5 months, 4 weeks ago

This. Cross-tenant access settings is built specifically for this.

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/cross-tenant-access-overview>

upvoted 1 times

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

Correct Answer: B

upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: B**

B. Invite the Contoso East users as guests in the Contoso West tenant.

upvoted 1 times

 **haskelatchi** 6 months, 3 weeks ago

B for Bob

upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **[Removed]** 11 months, 4 weeks ago

**Selected Answer: B**

B is the correct answer. No further licensing is required here. As LHADUK suggested though, cross-tenant access should be configured.

upvoted 3 times

 **taer** 1 year, 2 months ago

**Selected Answer: B**

Correct Answer: B

upvoted 4 times

## DRAG DROP

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You need to ensure that User1 can create access reviews for groups, and that User2 can review the history report for all the completed access reviews. The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

| Roles                | Answer Area                 |
|----------------------|-----------------------------|
| Global administrator | User1: <input type="text"/> |
| Global reader        | User2: <input type="text"/> |
| Reports reader       |                             |
| Security operator    |                             |
| Security reader      |                             |
| User administrator   |                             |

User1: Global administrator

Correct Answer:

User2: Global reader

Halwagy Highly Voted 10 months, 3 weeks ago

User 1 : User Administrator

User 2 : Security Reader

upvoted 26 times

oscarpopi 10 months, 1 week ago

Correct

upvoted 3 times

doch Highly Voted 10 months, 2 weeks ago

User Admin

Security Reader

Ref: <https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task>

upvoted 11 times

oscarpopi 10 months, 1 week ago

Correct, that's a nice article, I'll bookmark it

upvoted 2 times

poesklap Most Recent 1 week ago

<https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-downloadable-review-history>

Global Admin  
Global Reader  
upvoted 1 times

✉ **haazybanj** 3 weeks, 1 day ago

User1: User Admin  
User 2: security Reader  
<https://learn.microsoft.com/en-us/azure/active-directory/governance/deploy-access-reviews#who-will-create-and-manage-access-reviews>  
upvoted 1 times

✉ **LanceMatt** 1 month, 2 weeks ago

Trick question If you read the question correctly, it does not say that User1 needs to create the groups. If User1 needed to create groups it would need the User Administrator roles, but because the groups are already created and follow the least privilege rule, then the Security operator role is sufficient. User2 is correct as the Security Reader  
upvoted 1 times

✉ **Nyamnyam** 4 weeks, 1 day ago

Sorry but no. Pls read <https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task> again. Search for "Create, update, or delete access review of a group or of an app". It is the User Administrator role.  
upvoted 2 times

✉ **AK\_1234** 1 month, 3 weeks ago

To access an access review, it needs following roles:  
- Global Administrator  
- Identity Governance Administrator  
- Privileged Role Administrator  
- Review Administrator  
So, Global Admin and Global reader is correct.  
upvoted 2 times

✉ **SumitSahoo** 2 months ago

correct!!  
To create access reviews for Azure resources, you must be assigned to the Owner or the User Access Administrator role for the Azure resources. To create access reviews for Microsoft Entra roles, you must be assigned to the Global Administrator or the Privileged Role Administrator role.  
upvoted 2 times

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

To ensure that User1 can create access reviews for groups and User2 can review the history report for all the completed access reviews while following the principle of least privilege, you should assign the following roles:

User1:

Role: User administrator (to create access reviews for groups)  
User2:

Role: Report reader (to review the history report for completed access reviews)  
These role assignments provide the necessary permissions for each user to perform their respective tasks without granting them excessive privileges.  
upvoted 1 times

✉ **StarMe** 3 months, 2 weeks ago

It should be User administrator and Security Reader role considering Least privilege permissions  
upvoted 1 times

✉ **dule27** 6 months ago

User 1: User Administrator  
User 2: Global Reader  
upvoted 2 times

✉ **dule27** 6 months ago

correction:  
User 1: User Administrator  
User 2: Security Reader  
upvoted 3 times

✉ **ccadenasa** 6 months, 2 weeks ago

User1: User Admin  
User 2: security Reader  
<https://learn.microsoft.com/en-us/azure/active-directory/governance/deploy-access-reviews#who-will-create-and-manage-access-reviews>  
upvoted 2 times

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

Correct  
upvoted 1 times

✉ **rajbne** 7 months, 3 weeks ago

Please update the final answer to reflect the answers below  
upvoted 2 times

 **lokylook** 8 months, 3 weeks ago

User 2: Security Reader because has least privileges  
upvoted 1 times

 **tarroka** 9 months, 3 weeks ago

User 1: User Administrator Create, update, or delete access review of a group or of an app User Administrator  
User 2: Security Reader Read access review of an Azure AD role Security Reader  
upvoted 4 times

 **tarroka** 10 months, 1 week ago

User Administrator and Security Reader  
upvoted 6 times

 **Akakentavr** 10 months, 2 weeks ago

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review>

The keyword is to create access reviews for AD roles or Azure resources as for resources we need to be To create access reviews for Azure resources, you must be assigned to the Owner or the User Access Administrator role for the Azure resources.

For Azure AD roles - Global Administrator.

So the first answer is about groups - Azure resources - the User Access Administrator role for the Azure resources  
upvoted 1 times

店铺：专业认证88

店铺：专业认证88

**HOTSPOT**

You have an Azure subscription.

You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

- Users that are assigned Role1 can create or delete instances of Azure Container Apps.
- Users that are assigned Role2 can enforce adaptive network hardening rules.

Which resource provider permissions are required for each role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area****Role1:**

Microsoft.App  
Microsoft.Compute  
Microsoft.Management  
Microsoft.Security

**Role2:**

Microsoft.App  
Microsoft.Compute  
Microsoft.Network  
Microsoft.Security

Correct Answer:  
Role1: Microsoft.Compute

Role2: Microsoft.Security

dejo Highly Voted 10 months, 2 weeks ago

I think it's:

Role1: Microsoft.App  
<https://learn.microsoft.com/en-us/azure/container-apps/quickstart-portal#prerequisites>

Role2: Microsoft.Security  
<https://learn.microsoft.com/en-ie/rest/api/defenderforcloud/adaptive-network-hardenings/enforce?tabs=HTTP>  
upvoted 17 times

ThotSlayer69 Highly Voted 10 months, 2 weeks ago

Role1: Microsoft.App (for containers)

Role2: Microsoft.Security

Microsoft.Security controls the Security Center (renamed Defender for Cloud) (<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-services-resource-providers>), which handles Adaptive Network Hardening (<https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-network-hardening#what-is-adaptive-network-hardening>)  
upvoted 5 times

marcoby Most Recent 2 months, 1 week ago

For Role1, the key word is Azure Container Apps. Compute is for Virtual Machines, App is for Azure Container Apps.

Role 2 is Security as mentioned before.

upvoted 2 times

StarMe 3 months, 2 weeks ago

It shoud be Microsoft.App and Microsoft.Security

<https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftapp>

upvoted 2 times

EmnCours 4 months, 2 weeks ago

Role 1: Microsoft.App

Role 2 : Microsoft.Security

upvoted 2 times

dule27 6 months ago

Role 1: Microsoft.App

Role 2 : Microsoft.Security

upvoted 2 times

ShoaibPKDXB 6 months, 4 weeks ago

Correct: 1. Microsoft.Apps

2. Microsoft.Security

upvoted 3 times

kanew 7 months ago

Role 1: Microsoft.App [microsoft.app/containerapps/delete](https://microsoft.app/containerapps/delete) [microsoft.app/containerapps/write](https://microsoft.app/containerapps/write)

Role 2: Microsoft.Security [Microsoft.Security/adaptiveNetworkHardenings/enforce/action](https://microsoft.security/adaptiveNetworkHardenings/enforce/action)

upvoted 3 times

sbnpj 7 months, 3 weeks ago

Role 1: Microsoft.App

<https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftapp>

Role2: Microsoft.Security

<https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftsecurity>

upvoted 2 times

byproduct 8 months ago

ChatGPT says its:

Role 1: Compute

Role 2: Network

upvoted 1 times

Holii 5 months, 4 weeks ago

Do some research. This is a trick question as "Compute" is the title term for Microsoft.app, since it encompasses the Compute stack. However, Microsoft.app literally has a resource definition to handle Creation and Deletion of Azure Container Apps.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#compute>

upvoted 2 times

thadeus 8 months ago

Seriously? Because it told me ".App" for Role1 and ".Network" for Role2.

upvoted 1 times

Arjanussie 9 months, 1 week ago

It is Microsoft.compute.....ask chatgpt what is in graph microsoft.compute and what is in graph microsoft.app

upvoted 1 times

Holii 5 months, 4 weeks ago

You know the graph documentation is listed here:

<https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#compute>

[microsoft.app/containerapps/write](https://microsoft.app/containerapps/write) Create or update a Container App

[microsoft.app/containerapps/delete](https://microsoft.app/containerapps/delete) Delete a Container App

upvoted 1 times

jojoseph 10 months, 2 weeks ago

Role 1: Microsoft.App

Role 2 : Microsoft.Security

upvoted 3 times

exmITQS 7 months, 3 weeks ago

Role1 needs permission to create and delete instances of Azure Container Apps. Azure Container Apps are built on top of Azure Web Apps and Azure Functions, which use the underlying compute resources provided by Azure Virtual Machines. Therefore, Role1 should be assigned the Microsoft.Compute/virtualMachines/write and Microsoft.Compute/virtualMachines/delete permissions. Additionally, Role1 needs permission to create or delete Azure Container Apps. Azure Container Apps are deployed to managed hosting environments, so Role1 should be assigned the Microsoft.Web/hostingEnvironments/managedHostingEnvironments/write permission.

upvoted 1 times

 **Halwagy** 10 months, 3 weeks ago

Correct Answer:

Role 1: Microsoft.App

Role 2 : Microsoft.Network

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-services-resource-providers>

upvoted 4 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

**HOTSPOT**

You have a Microsoft 365 tenant that has 5,000 users. One hundred of the users are executives. The executives have a dedicated support team.

You need to ensure that the support team can reset passwords and manage multi-factor authentication (MFA) settings for only the executives. The solution must use the principle of least privilege.

Which object type and Azure Active Directory (Azure AD) role should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area****Object type:**

- An administrative unit
- A custom administrator role
- A dynamic group
- A Microsoft 365 group

**Role:**

- Authentication administrator
- Groups administrator
- Helpdesk administrator
- Password administrator

**Correct Answer:** Object type: A custom administrator role

Role: Helpdesk administrator

**Halwagy** Highly Voted 10 months, 3 weeks ago

Correct Answer:

Object Type: Administrative Unit

Role: Authentication administrator

upvoted 42 times

**skbudhram** Highly Voted 9 months, 2 weeks ago

Sheesh this site has a lot of wrong answers, what's the point even ..

upvoted 14 times

**b0tag** Most Recent 3 months, 2 weeks ago

Should be

Administrative Unit

Helpdesk administrator - The Authentication Administrator role is less privileged than the Helpdesk Administrator role

The Authentication Administrator role has permissions to manage authentication methods and password reset whereas the Helpdesk Administrator role has permissions to manage passwords, groups, and users.

upvoted 2 times

**DasChi\_chicken** 1 month, 3 weeks ago

You are right regarding the difference between helpdesk and authentication Admin.... Therefore the answer is:  
Administrative unit  
Authentication Admin

The Support Team shall only reset MFA and Passwords and regarding least privilege this IS the best role  
upvoted 5 times

□ **EmnCours** 4 months, 2 weeks ago

Object Type: Administrative Unit  
Role: Authentication administrator  
upvoted 3 times

□ **dule27** 5 months ago

Object Type: An Administrative Unit  
Role: Authentication Administrator  
upvoted 2 times

□ **b233f0a** 6 months ago

Role: Authentication Administrator - <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#authentication-administrator> - "Set or reset any authentication method (including passwords) for non-administrators"  
upvoted 1 times

□ **dule27** 6 months ago

Object Type: An administrative unit  
Role: Authentication administrator  
upvoted 5 times

□ **ShoaibPKDXB** 6 months, 4 weeks ago

Correct: Object Type: An Administrative Unit  
Role: Authentication Administrator  
upvoted 1 times

□ **rajbne** 7 months, 3 weeks ago

Please update final answer  
upvoted 2 times

□ **Remus999** 7 months, 3 weeks ago

Authentication Administrator is the least privileged role to manage MFA as per <https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#multi-factor-authentication>  
upvoted 1 times

□ **Akakentavr** 10 months, 2 weeks ago

As well regarding the Authentication administrator or Helpdesk administrator options pay attention to "executives" in our case and Helpdesk administrator -Can reset passwords for non-administrators and Helpdesk Administrators.

So Authentication administrator is our choice  
upvoted 6 times

□ **jojoseph** 10 months, 2 weeks ago

Object Type: Administrative Unit  
Role: Authentication administrator  
upvoted 1 times

□ **ExamStudy68** 7 months, 3 weeks ago

Maybe it's by design to force discussion and make you think about it or look it up... Not sure really.  
upvoted 1 times

□ **dejo** 10 months, 2 weeks ago

Object type: An administrative unit  
Role: Helpdesk administrator

Helpdesk admin has less power in resetting passwords than Auth admin and others <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords>  
upvoted 4 times

□ **Halwagy** 10 months, 2 weeks ago

Helpdesk administrator cannot reset MFA settings only password reset, then Authentication administrator will be the right one  
upvoted 5 times

□ **dejo** 10 months, 2 weeks ago

well that's true :)  
upvoted 2 times

□ **natazar** 10 months, 3 weeks ago

admin unit way to go  
upvoted 4 times



You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name  | Group  |
|-------|--------|
| User1 | Group1 |
| User2 | Group1 |
| User3 | Group2 |
| User4 | Group2 |
| User5 | None   |

You have an administrative unit named Au1. Group1, User2, and User3 are members of Au1.

User5 is assigned the User administrator role for Au1.

For which users can User5 reset passwords?

- A. User1, User2, and User3
- B. User1 and User2 only
- C. User3 and User4 only
- D. User2 and User3 only

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **Halwagy** Highly Voted 10 months, 3 weeks ago

**Selected Answer: D**

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 (unless those users and devices are separately added as members of the administrative unit).

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

upvoted 21 times

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

Why is User1 not included?

upvoted 2 times

 **Nyamnyam** 4 weeks, 1 day ago

Because of what Halwagy has quoted and referenced above ;)

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: D**

User2 and User3 only

upvoted 1 times

 **Husterix** 5 months, 1 week ago

**Selected Answer: D**

D is the correct answer: the admin role only works on directly added members to the AU.

upvoted 3 times

 **dule27** 6 months ago

**Selected Answer: D**

User2 and User3 only

upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: D**

D is correct

upvoted 1 times

 **oscarpopi** 10 months, 1 week ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#operator-precedence>

upvoted 1 times

 **CloudRat** 10 months, 3 weeks ago

D. Is the correct answer. The User administrative role assigned, will only grant permission to reset passwords for Directly assigned members to the AU. Members of Groups, which is assigned to the AU, is not affected by this.

Tested this in Own Environment just to be sure :)

upvoted 4 times

 **divyakanth** 10 months, 3 weeks ago

can i say that AU is also a Group and since adding a group in to an existing group will not make the root users a set of the master group(nested group). and hence the user1 will not be added and the other users were directly added and so the admin can act on them

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name  | Usage location | Department | Job title |
|-------|----------------|------------|-----------|
| User1 | United States  | Sales      | Associate |
| User2 | Finland        | Sales      | SalesRep  |
| User3 | Australia      | Sales      | Manager   |

You create a dynamic user group and configure the following rule syntax.

user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager") -or (user.jobTitle -eq "SalesRep")

Which users will be added to the group?

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

**Correct Answer:** D

*Community vote distribution*

D (75%)

A (25%)

✉ **ydecac** Highly Voted 10 months, 3 weeks ago

```
user.usageLocation -in ["US","AU"] == User 1 & User 3
-and (user.department -eq "Sales") == User 1 & User 3
-and -not (user.jobTitle -eq "Manager") == User 1
-or (user.jobTitle -eq "SalesRep")
```

upvoted 21 times

✉ **keanwvegas** 7 months, 3 weeks ago

Just to further explain this...

1. Think of everything up to the OR as 1 big 'if, and if, and if' statement (statement 1). In this case, that'd leave only User 1 to be selected.
2. Think of everything after the OR as a separate statement (statement 2), meaning 'statement 1 OR statement 2', now including user2 who is a salesrep.

upvoted 11 times

✉ **Nyamnyam** 4 weeks, 1 day ago

well, that's basically what happens when admins or devs don't use parentheses.

OR is outside of the AND statement, so User 1 and User 2 are the correct answer.

upvoted 1 times

✉ **meself7** Highly Voted 10 months, 3 weeks ago

**Selected Answer: D**

D is correct

always resolve according to precedence, first all the -and operators, only after that the -or operators.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#operator-precedence>

upvoted 18 times

✉ **BRoald** 9 months ago

D is wrong because User 2 is located in Finland and cannot be added to the dynamic group. I tested this and im 100% sure ONLY user 1 gets added.

I tested this dynamic rule and got the result by validating an user that has an usage location set on Finland:

RED CROSS: user.usagelocation -in ["US","AU"] [UsageLocation = "FI"]

So again, only User 1 gets added to this group 100%

upvoted 11 times

✉ **Holii** 5 months, 4 weeks ago

Wrong. test again. You completely ditched the -or flag by testing only user.usagelocation...obviously you're going to get different results.

Proper order of precedence is as follows:

-or  
-and  
-and  
user.usageLocation -in ["US", "AU"]  
user.department -eq "Sales"  
-not  
user.jobTitle -eq "Manager"  
user.jobTitle -eq "SalesRep"

the -or flag trumps all other conditionals.

upvoted 1 times

□ **Alscoran** Most Recent 1 week, 4 days ago

**Selected Answer: D**

Because of the Or statement

upvoted 1 times

□ **BenLam** 1 month, 1 week ago

If people read it out loud it makes sense.

Filter the user's location by US or AU AND their department is SALES  
AND their job title is NOT Manager or SalesRep.

upvoted 1 times

□ **curtmcgirt** 3 weeks ago

nah.

(Filter the user's location by US or AU AND their department is SALES AND their job title is NOT Manager)

(OR their job title is SalesRep.)

upvoted 1 times

□ **haazybanj** 1 month, 1 week ago

**Selected Answer: D**

D is right

upvoted 2 times

□ **JimboJones99** 1 month, 2 weeks ago

**Selected Answer: A**

It's an OR at the end

upvoted 1 times

□ **JimboJones99** 1 month, 2 weeks ago

My bad, it's D because of the OR. Not A

upvoted 2 times

□ **SumitSahoo** 2 months ago

{ user.usageLocation -in ["US", "AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager") } -or { (user.jobTitle -eq "SalesRep") }

{user 1 } -or {User 2}

So and is both u1 and u2.

upvoted 2 times

□ **amurp35** 3 months, 2 weeks ago

**Selected Answer: D**

this is a question to test your knowledge of the order of operations or precedence. There are two main statements, a string of ands and then an or. User 2 does not get included in the first statement but does in the last. Therefore User 2 does get included. ANDs are like multiplication for math. They get done first, and grouped into one arithmetical operation, the result of which is then compared to the next group or singular statement, which is the OR.

upvoted 3 times

□ **TeresaCN** 3 months, 3 weeks ago

user.usageLocation -in ["US", "AU"] == User 1 & User 3  
-and (user.department -eq "Sales") == User 1 & User 3  
-and -not (user.jobTitle -eq "Manager") == User 1  
-or (user.jobTitle -eq "SalesRep") (no)

Answer is : A. User 1

upvoted 2 times

□ **stev\_au** 4 months, 1 week ago

**Selected Answer: D**

Answer D (User 1 and User 2) is 100% correct. Tested in lab.

upvoted 4 times

□ **ServerBrain** 3 months ago

I dispute that test.

user.usageLocation -in ["US","AU"] excludes User2

upvoted 1 times

□ **EmnCours** 4 months, 2 weeks ago

**Selected Answer: D**

Correct Answer: D

upvoted 2 times

□ **Tiagofv** 4 months, 3 weeks ago

Resposta: D

A primeira parte da regra "user.usageLocation -in ["US","AU]" verifica se o campo "Usage Location" do usuário está definido como "US" (United States) ou "AU" (Australia);

A segunda parte da regra "user.department -eq "Sales"" verifica se o campo "Department" do usuário está definido como "Sales";

A terceira parte da regra "-not (user.jobTitle -eq "Manager")" verifica se o campo "Job Title" do usuário não está definido como "Manager" e neste caso está negando a participação de quem tem o Job Title definido como Manager;

A última parte da regra "-or (user.jobTitle -eq "SalesRep")" verifica se o campo "Job Title" do usuário está definido como "SalesRep";

Com base nessa lógica, apenas User1 e User2 satisfazem todas as condições da regra e serão adicionados ao grupo.

upvoted 1 times

□ **Tiagofv** 4 months, 3 weeks ago

Estive lendo novamente e agora mudei minha opinião. O user2 é da Finlândia e não atende o início do comando. Acho que a resposta seria Apenas USER1 mesmo.

upvoted 1 times

□ **latoupi** 5 months, 1 week ago

The global filter term filters users who are located in the United States or Australia, who belong to the sales department, who are not responsible, or who have the job title "SalesRep."

So it is "User1"

upvoted 1 times

□ **dule27** 5 months, 3 weeks ago

**Selected Answer: D**

D. User1 and User2 only

upvoted 2 times

□ **penatuna** 6 months ago

**Selected Answer: D**

D is the right answer. Tested it with Dynamic membership rules -> Validate Rules (Preview).

BTW the syntax in the question is wrong. There is one extra space in the last user.jobTitle.

upvoted 2 times

□ **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: D**

D is correct

upvoted 2 times

□ **sbnpj** 7 months, 3 weeks ago

**Selected Answer: D**

Tested in my lab.

upvoted 2 times

You have an Azure AD tenant that contains a user named User1.

User1 needs to manage license assignments and reset user passwords.

Which role should you assign to User1?

- A. Helpdesk administrator
- B. Billing administrator
- C. License administrator
- D. User administrator

**Correct Answer: D**

*Community vote distribution*

D (100%)

✉ **EmnCours** 4 months, 2 weeks ago

Correct Answer: D

upvoted 1 times

✉ **dule27** 6 months ago

**Selected Answer: D**

D. User administrator

upvoted 1 times

✉ **JN\_311** 6 months ago

**Selected Answer: D**

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

upvoted 1 times

✉ **SwitchKat** 6 months, 3 weeks ago

I work on a least privilege when it comes to roles. User Administrator has much more access than this user seems to need. I would assign both the Help Desk Administrator role and the License Administrator role to the user. This allows them to do exactly what they need to and nothing more.

upvoted 3 times

✉ **Holii** 5 months, 3 weeks ago

Personally, this would be a custom role or what you were suggesting.

No way would we be granting User Administrator for a role that only needs these permissions. This looks like a slightly higher-privileged helpdesk administrator requirement.

upvoted 2 times

✉ **Holii** 5 months, 3 weeks ago

Answer is still D. though, because we can't select multiple.

upvoted 1 times

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

**Selected Answer: D**

correct D

upvoted 1 times

✉ **itismadu** 7 months, 4 weeks ago

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

upvoted 1 times

✉ **chikorita** 8 months, 1 week ago

correct cuz only User Access Admin fits in both the requirement : manage license assignments and reset user passwords.

upvoted 2 times

✉ **Aquintero** 10 months, 1 week ago

Administrador de Usuarios

upvoted 2 times

✉ **jojoseph** 10 months, 2 weeks ago

**Selected Answer: D**

User Administrator  
upvoted 2 times

 **Halwagy** 10 months, 3 weeks ago

**Selected Answer: D**  
User Administrator  
upvoted 3 times

 **CloudRat** 10 months, 3 weeks ago

D. Is Correct - Neither of the other Roles have permissions to handle all of the statements.  
upvoted 3 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the Set-MsolUserLicense cmdlet
- B. the Set-AzureADGroup cmdlet
- C. the Set-WindowsProductKey cmdlet
- D. the Administrative units blade in the Azure Active Directory admin center

**Correct Answer: D**

*Community vote distribution*

A (84%)      B (16%)

 **Nyamnyam** 4 weeks, 1 day ago

**Selected Answer: A**

A. is the correct answer  
upvoted 1 times

 **Sandipmcr** 1 month, 3 weeks ago

**Selected Answer: A**

Set-MsolUserLicense is the only way between the proposed answers  
upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

You can unassign licenses from users on either the Active users page, or on the Licenses page. The method you use depends on whether you want to unassign product licenses from specific users or unassign users licenses from a specific product.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1. the Licenses blade in the Azure Active Directory admin center

2. the Set-MsolUserLicense cmdlet

Other incorrect answer options you may see on the exam include the following:

- the Administrative units blade in the Azure Active Directory admin center
- the Groups blade in the Azure Active Directory admin center
- the Set-AzureAdGroup cmdlet

upvoted 2 times

 **morit2578** 3 months, 1 week ago

**Selected Answer: A**

Set-MsolUserLicense is the only way between the proposed answers  
upvoted 1 times

 **amurp35** 3 months, 2 weeks ago

I don't understand why some of these answers are highlighted as correct when they are plainly and obviously incorrect. The correct answer is A. The answer indicated as correct is D, but it is not correct. The reason? There is no such 'Administrative Units' blade in Azure AD.

upvoted 3 times

 **StarMe** 3 months, 2 weeks ago

Please update your answer to 'A' the Set-MsolUserLicense cmdlet.  
The Administrative Unit is for restriction, setting boundary.  
upvoted 2 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: B**

A. the Set-MsolUserLicense cmdlet  
upvoted 2 times

 **mali1969** 5 months, 2 weeks ago

You can use the Set-MsolUserLicense cmdlet to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort. You can use this cmdlet to remove licenses from one or more users at a time. Here is an example of how to remove the litwareinc:ENTERPRISEPACK (Office 365 Enterprise E3) license from the user account BelindaN@litwareinc.com:

```
Set-MsolUserLicense -UserPrincipalName belindan@litwareinc.com -RemoveLicenses "litwareinc:ENTERPRISEPACK"
upvoted 2 times
```

 **mali1969** 5 months, 2 weeks ago

The role that should be assigned to User1 is User administrator. This role can create and manage users and groups, and can reset passwords for users, Helpdesk administrators and User administrators

upvoted 1 times

 **dule27** 6 months ago

**Selected Answer: A**

A. the Set-MsolUserLicense cmdlet

upvoted 1 times

 **HOTDOGG** 6 months, 4 weeks ago

**Selected Answer: B**

I am not convinced A is the correct answer. Using the Set-MsolUserLicense command would work if the licence was directly linked. The license is linked via a group. The group will always win. I feel in this case, removing the group via Powershell is the answer.

upvoted 1 times

 **wheeldj** 6 months, 2 weeks ago

so reading the question again it says the group is used to assign E5 licenses, the question asks how to remove the individually assigned E3 licenses... so Answer A

upvoted 3 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: A**

Set-MsolUserLicense

upvoted 3 times

 **Aquintero** 10 months, 1 week ago

**Selected Answer: A**

A. el cmdlet Set-MsolUserLicense

upvoted 1 times

 **mayleni** 10 months, 2 weeks ago

**Selected Answer: A**

A!!

[https://www.bing.com/ck/a?!&&p=ee69ca3a6024a8f9JmItdHM9MTY3NDYwNDgwMCZpZ3VpZD0wYjdiNTU2OC1lYzc5LTZmM2ItMGQ3OC00NTIxZWQxYTZIMjImaW5zaWQ9NTE4MA&ptn=3&hsh=3&fclid=0b7b5568-ec79-6f3b-0d78-4521ed1a6e22&psq=Set-MsolUserLicense&u=a1aHR0cHM6Ly9sZWFrbi5taWNyb3NvZnQuY29tL2VuLXVzL3Bvd2Vyc2hlbGwvbW9kdWxIL21zb25saW5l3NldC1tc29sdXNlcmxpY2Vuc2U\\_dmlldz1henVyzWFkcHMtMS4w&ntb=1](https://www.bing.com/ck/a?!&&p=ee69ca3a6024a8f9JmItdHM9MTY3NDYwNDgwMCZpZ3VpZD0wYjdiNTU2OC1lYzc5LTZmM2ItMGQ3OC00NTIxZWQxYTZIMjImaW5zaWQ9NTE4MA&ptn=3&hsh=3&fclid=0b7b5568-ec79-6f3b-0d78-4521ed1a6e22&psq=Set-MsolUserLicense&u=a1aHR0cHM6Ly9sZWFrbi5taWNyb3NvZnQuY29tL2VuLXVzL3Bvd2Vyc2hlbGwvbW9kdWxIL21zb25saW5l3NldC1tc29sdXNlcmxpY2Vuc2U_dmlldz1henVyzWFkcHMtMS4w&ntb=1)

upvoted 1 times

 **Oknip** 10 months, 2 weeks ago

**Selected Answer: A**

cmdlet Set-MsolUserLicense

upvoted 2 times

 **jojoseph** 10 months, 2 weeks ago

**Selected Answer: A**

Set-MsolUserLicense cmdlet

upvoted 2 times

 **dobriv** 10 months, 3 weeks ago

but -> The Set-MsolUserLicense and New-MsolUser (-LicenseAssignment) cmdlets are scheduled to be retired. Please migrate your scripts to the Microsoft Graph SDK's Set-MgUserLicense cmdlet as described above. For more information, see Migrate your apps to access the license management APIs from Microsoft Graph.

upvoted 2 times

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to a group that includes all the users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the Set-AzureAdGroup cmdlet
- B. the Identity Governance blade in the Azure Active Directory admin center**
- C. the Set-WindowsProductKey cmdlet
- D. the Set-MsolUserLicense cmdlet

**Correct Answer: B**

*Community vote distribution*

D (100%)

 **Nyamnyam** 4 weeks, 1 day ago

**Selected Answer: D**

Oh, come on, contributors - Identity Governance blade is about Entitlement Management and Access Reviews. No licensing management there.  
upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

You can unassign licenses from users on either the Active users page, or on the Licenses page. The method you use depends on whether you want to unassign product licenses from specific users or unassign users licenses from a specific product.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1. the Licenses blade in the Azure Active Directory admin center
2. the Set-MsolUserLicense cmdlet

Other incorrect answer options you may see on the exam include the following:

- the Administrative units blade in the Azure Active Directory admin center
- the Groups blade in the Azure Active Directory admin center
- the Set-AzureAdGroup cmdlet

upvoted 1 times

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: D**

Plz check these questions: Q25, Q40,Q41,Q43.and Q53

upvoted 1 times

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: D**

D. the Set-MsolUserLicense cmdlet

The Set-MsolUserLicense cmdlet allows you to manage license assignments for Microsoft 365 users. In this scenario, you want to remove the Office 365 Enterprise E3 licenses from users who are part of the group that now has the Microsoft 365 Enterprise E5 licenses assigned.

Here's how you can do it using PowerShell:

```
# Connect to Azure AD
Connect-MsolService

# Get the users in the group
$groupMembers = Get-MsolGroupMember -GroupObjectId <GroupObjectID>

# Loop through and remove the E3 licenses
foreach ($user in $groupMembers) {
    Set-MsolUserLicense -UserPrincipalName $user.UserPrincipalName -RemoveLicenses "<E3 License SkuId>"
}
```

upvoted 1 times

 **dule27** 6 months ago

**Selected Answer: D**

D. the Set-MsolUserLicense cmdlet  
upvoted 2 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: D**

D is correct  
upvoted 2 times

 **AmplifiedStitches** 7 months, 3 weeks ago

So it is possible to perform group-based license management from the Identity Governance portal, so I think what the question is getting at is that this is preferred over using PowerShell, since the PowerShell command can also accomplish the same thing.

The question does specify reducing administrative overhead, so it's probably just that it's simpler to use the Portal vs a PowerShell command.

References:

- <https://learn.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview>  
upvoted 1 times

 **f2bf85a** 8 months ago

If Set-MsolUserLicense is deprecated now, "using the Set-MgUserLicense cmdlet in Microsoft Graph API" might be a possible answer.  
<https://learn.microsoft.com/en-us/microsoft-365/enterprise/remove-licenses-from-user-accounts-with-microsoft-365-powershell?view=o365-worldwide#removing-licenses-from-user-accounts>

upvoted 1 times

 **AAsif098** 9 months, 3 weeks ago

Looks like this question may not be on the exam as the following is stated by MS:

The Set-MsolUserLicense cmdlet is deprecated. Learn how to assign licenses with Microsoft Graph PowerShell. For more info, see the Assign License Microsoft Graph API.

upvoted 1 times

 **Taigr** 9 months, 3 weeks ago

Well but when is:

The Set-MsolUserLicense cmdlet is deprecated. Learn how to assign licenses with Microsoft Graph PowerShell. For more info, see the Assign License Microsoft Graph API.

deprecated. Is possible that this powershell command is not right answer :(.

upvoted 2 times

 **Aquintero** 10 months, 1 week ago

**Selected Answer: D**

D. el cmdlet Set-MsolUserLicense  
upvoted 2 times

 **mayleni** 10 months, 2 weeks ago

**Selected Answer: D**

the same question again! Is D  
upvoted 2 times

 **Oknip** 10 months, 2 weeks ago

**Selected Answer: D**

cmdlet Set-MsolUserLicense  
upvoted 2 times

 **Oknip** 10 months, 2 weeks ago

D is correct:

cmdlet Set-MsolUserLicense  
<https://learn.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0>  
upvoted 1 times

 **divyakanth** 10 months, 2 weeks ago

**Selected Answer: D**

Set-MsolUserLicense cmdlet  
upvoted 3 times

 **Halwagy** 10 months, 3 weeks ago

**Selected Answer: D**

Set-MsolUserLicense cmdlet  
upvoted 4 times

**HOTSPOT**

Your on-premises network contains an Active Directory domain that uses Azure AD Connect to sync with an Azure AD tenant.

You need to configure Azure AD Connect to meet the following requirements:

- User sign-ins to Azure AD must be authenticated by an Active Directory domain controller.
- Active Directory domain users must be able to use Azure AD self-service password reset (SSPR).

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

NOTE: Each correct selection is worth one point.

**Answer Area**

**Authentication by the domain controller:**

Federation with Active Directory Federation Services (AD FS)  
Pass-through authentication  
Password hash synchronization

**SSPR:**

Device writeback  
Group writeback  
Password hash synchronization  
Password writeback

**Answer Area**

**Authentication by the domain controller:**

Federation with Active Directory Federation Services (AD FS)  
**Pass-through authentication**  
Password hash synchronization

**Correct Answer:**

**SSPR:**

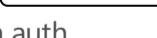
Device writeback  
Group writeback  
Password hash synchronization  
**Password writeback**

 **jojoseph**  10 months, 2 weeks ago

pass- through auth

password write back

upvoted 13 times

 **EmnCours**  3 months, 3 weeks ago

pass- through auth

password write back

upvoted 3 times

 **AMZ** 5 months, 1 week ago

Question valid - 06/23

upvoted 3 times

 **mali1969** 5 months, 2 weeks ago

To configure Azure AD Connect to meet the following requirements:

- User sign-ins to Azure AD must be authenticated by an Active Directory domain controller.
- Active Directory domain users must be able to use Azure AD self-service password reset (SSPR).

You can use Pass-through Authentication (PTA) for the first requirement. PTA validates user credentials against your on-premises Active Directory environment without the need for complex network infrastructure or for managing a separate set of credentials in the cloud. You can find more information on how to configure PTA in the Microsoft documentation 1.

For the second requirement, you can use Password Hash Synchronization (PHS). PHS synchronizes a hash of the user's password from your on-premises Active Directory environment to Azure AD. You can find more information on how to configure PHS in the Microsoft documentation  
upvoted 2 times

✉ **danielolickan\_yahoo** 3 months, 2 weeks ago

For 2nd requirement, it should be password write back. PHS doesn't help with SSPR  
upvoted 1 times

✉ **dule27** 6 months ago

1. Pass-through authentication
  2. Password writeback
- upvoted 1 times

✉ **DoMing** 8 months, 1 week ago

PTA and Password hash synchronization  
upvoted 1 times

✉ **kmk\_01** 7 months, 4 weeks ago

How does PHS help with SSPR for On-premises AD accounts?  
It's password write back for the second question.  
upvoted 4 times

✉ **Aquintero** 10 months, 1 week ago

Al parecer la respuesta es correcta segun el siguiente link: <https://learn.microsoft.com/es-es/azure/active-directory/authentication/tutorial-enable-cloud-sync-sspr-writeback>  
upvoted 3 times

✉ **Halwagy** 10 months, 3 weeks ago

The Answer is Correct  
upvoted 3 times

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all users.

You needed to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the Groups blade in the Azure Active Directory admin center
- B. the Set-AzureADGroup cmdlet
- C. the Identity Governance blade in the Azure Active Directory admin center
- D. the Set-MsolUserLicense cmdlet

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **Martyss** Highly Voted 5 months, 2 weeks ago

At least they got it right on the 4th try lol  
upvoted 18 times

 **haskelatchi** Highly Voted 6 months, 3 weeks ago

How many times are they going to repeat the same question? This is not going to stop me from answering D all the time  
upvoted 8 times

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

same as question before  
upvoted 1 times

 **Firefarter** 4 months, 1 week ago

Set-MsolUserLicense would be correct but it is deprecated  
upvoted 1 times

 **dule27** 6 months ago

**Selected Answer: D**  
D. the Set-MsolUserLicense cmdlet  
upvoted 1 times

 **ShoaibPKDXB** 6 months, 3 weeks ago

**Selected Answer: D**  
D is 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.

You have an Active Directory forest that syncs to an Azure AD tenant.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.

You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.

Solution: You configure conditional access policies.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **shuhaidawahab** 1 month, 3 weeks ago

same as question before  
upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: B**  
B. No is correct answer  
upvoted 1 times

 **mali1969** 5 months, 2 weeks ago

o ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD, you can configure Pass-through Authentication (PTA). PTA validates user credentials against your on-premises Active Directory environment without the need for complex network infrastructure or for managing a separate set of credentials in the cloud. You can find more information on how to configure PTA in the Microsoft documentation 1.

Alternatively, you can configure Azure AD provisioning to deprovision or deactivate disabled users in applications. For applications that don't use Azure AD SaaS App Provisioning, you can use Identity Manager (MIM) or a 3rd party solution to automate the deprovisioning of users. You should also identify and develop a process for applications that require manual deprovisioning

upvoted 1 times

 **dule27** 6 months ago

**Selected Answer: B**  
B. No is correct answer  
upvoted 1 times

 **haskelatchi** 6 months, 3 weeks ago

Another repeat question. The answer is obviously C  
upvoted 1 times

 **kanew** 7 months ago

B) <https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/users-revoke-access>  
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 a user named User1.

You need to ensure that User1 can update the status of Identity Secure Score improvement actions.

Solution: You assign the Exchange Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: A**

*Community vote distribution*

A (80%)

B (20%)

✉ **AMZ** Highly Voted 8 months ago

answer looks correct according to this  
<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#read-and-write-roles>  
upvoted 11 times

✉ **kmk\_01** 7 months, 4 weeks ago

Thanks for the link.  
upvoted 1 times

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

**Selected Answer: A**  
<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#read-and-write-roles>

With read and write access, you can make changes and directly interact with identity secure score.

- \* Global Administrator
- \* Security Administrator
- \* Exchange Administrator
- \* SharePoint Administrator

(Redundant. Just tipping the vote scale a little because ShoaibPKDXB managed to answer both A and B.)  
upvoted 1 times

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

With read and write access, you can make changes and directly interact with identity secure score.

- Global Administrator
  - Security Administrator
  - Exchange Administrator
  - SharePoint Administrator
- upvoted 1 times

✉ **EmnCours** 4 months, 2 weeks ago

**Selected Answer: A**  
<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#read-and-write-roles>  
upvoted 1 times

✉ **mali1969** 5 months, 2 weeks ago

Yes, that meets the goal. According to Microsoft documentation, to access Identity Secure Score, you must be assigned one of the following roles in Azure Active Directory: Global administrator; Security administrator; Exchange administrator; SharePoint administrator.

So assigning the Exchange Administrator role to User1 will allow them to update the status of Identity Secure Score improvement actions upvoted 3 times

 **mali1969** 5 months, 2 weeks ago

To ensure that User1 can update the status of Identity Secure Score improvement actions, you can assign the Security Administrator role to User1. The Security Administrator role has permissions to view and manage security-related configuration settings in the Microsoft 365 admin center and the Azure portal 1.

You can assign roles to users in the Microsoft 365 admin center or by using PowerShell

upvoted 1 times

 **Rynol** 5 months, 2 weeks ago

What you should know

Who can use the identity secure score?

To access identity secure score, you must be assigned one of the following roles in Azure Active Directory.

Read and write roles

With read and write access, you can make changes and directly interact with identity secure score.

Global administrator

Security administrator

Exchange administrator

SharePoint administrator

Read-only roles

With read-only access, you aren't able to edit status for an improvement action.

Helpdesk administrator

User administrator

Service support administrator

Security reader

Security operator

Global reader

upvoted 1 times

 **dule27** 6 months ago

**Selected Answer: A**

A. Yes is the correct answer

upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: A**

correct

upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **LeonLau** 6 months, 3 weeks ago

No, A is the correct answer.

Only the following 4 role can update identity secure score

Global administrator

Security administrator

Exchange administrator

SharePoint administrator

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 a user named User1.

You need to ensure that User1 can update the status of Identity Secure Score improvement actions.

Solution: You assign the User Administrator role to User1.

Does this meet the goal?

A. Yes

**B. No**

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **EmnCours** 4 months, 2 weeks ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#read-and-write-roles>  
upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: B**

B. NO is the correct answer  
upvoted 1 times

 **m4rv1n** 6 months, 4 weeks ago

**Selected Answer: B**

With read and write access, you can make changes and directly interact with identity secure score.

Global administrator  
Security administrator  
Exchange administrator  
SharePoint administrator  
upvoted 2 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: B**

Correct B  
upvoted 1 times

 **boapaulo** 8 months ago

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#read-and-write-roles>  
upvoted 1 times

**HOTSPOT****Case Study****Overview**

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

**Existing Environment. Existing Environment**

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso\_Resources. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

**Existing Environment. Microsoft 365/Azure Environment**

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security E5
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

#### Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

#### Requirements. Planned Changes

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

You need to meet the technical requirements for license management by the help desk administrators.

What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Object to create for each branch office:

- An administrative unit
- A custom role
- A Dynamic User security group
- An OU

Tool to use:

- Azure Active Directory admin center
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft Purview Compliance portal

## Answer Area

Object to create for each branch office:

- An administrative unit
- A custom role
- A Dynamic User security group
- An OU

Correct Answer:

Tool to use:

- Azure Active Directory admin center
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft Purview Compliance portal

✉  **mikekrt** Highly Voted 2 months, 3 weeks ago

correct

upvoted 6 times

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

Trick question. You might think Dynamic group because of "License allocation for new users must be assigned automatically based on the location of the user". But there is also this line: "The helpdesk administrators must be able to manage licenses for only the users in their respective office." This one makes Administrative Unit correct instead of dynamic group. Very tricky

upvoted 2 times

✉  **haazybanj** 1 month ago

box1= Dynamic group  
box = Azure admin center

upvoted 1 times

✉  **haazybanj** 3 weeks, 1 day ago

Box1= Administrative unit  
upvoted 1 times

✉  **kijken** 3 weeks, 2 days ago

first is administrative unit, please read what that is  
upvoted 1 times

✉  **haazybanj** 3 weeks, 1 day ago

You're right  
upvoted 1 times

✉  **hw121693** 4 months, 2 weeks ago

I think the first choice should be dynamic security group  
"License allocation for new users must be assigned automatically based on the location of the user."  
upvoted 2 times

hw121693 4 months, 2 weeks ago

Sorry scratch that:

"The helpdesk administrators must be able to manage licenses for only the users in their respective office."

answer is correct

upvoted 4 times

ivzdf 4 months, 1 week ago

you cannot apply a role to a dynamic security group - tested

upvoted 2 times

## Case Study -

## Overview -

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

## Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | <i>None</i>                       |
| User2 | <i>None</i>                       |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner       | Members                        |
|-------------|----------|-----------------|-------------|--------------------------------|
| IT_Group1   | Security | Assigned        | <i>None</i> | All users in the IT department |
| AdatumUsers | Security | Assigned        | <i>None</i> | User1, User2                   |

## Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

## Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

## Requirements. Planned Changes -

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

## Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You need to resolve the issue of the sales department users.

What should you configure for the Azure AD tenant?

A. the Device settings

B. the User settings

C. the Access reviews settings

D. Security defaults

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **marot** 4 months, 1 week ago

**Selected Answer: A**

Azure Portal > Azure AD > Device > Device Settings > in the "Azure AD join and registration settings" section, change the maximum number of devices a user can have in Azure AD.

upvoted 4 times

 **Hull** 4 months, 2 weeks ago

**Selected Answer: A**

Correct. Issue is:

"Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit."

Within Device settings, you can increase maximum number of devices a user can join/register to Azure AD.

upvoted 4 times

## Case Study -

## Overview -

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

## Existing Environment: ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | None                              |
| User2 | None                              |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner | Members                        |
|-------------|----------|-----------------|-------|--------------------------------|
| IT_Group1   | Security | Assigned        | None  | All users in the IT department |
| AdatumUsers | Security | Assigned        | None  | User1, User2                   |

## Existing Environment: Litware Environment

Litware has an AD DS forest named litware.com

## Existing Environment: Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

## Requirements. Planned Changes -

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

## Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You need to resolve the issue of IT\_Group1.

What should you do first?

A. Change Membership type of IT\_Group1 to Dynamic User.

**B. Recreate the IT\_Group1 group.**

C. Change Membership type of IT Group1 to Dynamic Device.

D. Add an owner to IT\_Group1.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 razmus Highly Voted 4 months, 2 weeks ago

And when recreating, set isAssignableToRole. <https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept>  
upvoted 9 times

 Studytime2023 Most Recent 3 weeks, 2 days ago

The only answer possible is: recreate the group and toggle is-assignable-to-role to true. Adding owners to this group only allows the "Owner" to add members.  
See: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept>  
upvoted 2 times

 Studytime2023 3 weeks, 2 days ago

Read these segments:

\*Only groups that have the isAssignableToRole property set to true at creation time can be assigned a role.

\*By default, only Global Administrators and Privileged Role Administrators can manage the membership of a role-assignable group, but you can delegate the management of role-assignable groups by adding group owners.

\*For example, assume that a group named Contoso\_User\_Administrators is assigned the User Administrator role. An Exchange administrator who can modify group membership could add themselves to the Contoso\_User\_Administrators group and in that way become a User

Administrator. As you can see, an administrator could elevate their privilege in a way you didn't intend. This stops a person with lower admin authority further elevating their admin access.

upvoted 2 times

 **Nyamnyam** 4 weeks, 1 day ago

**Selected Answer: B**

For the ones who missed the logic: you need a role-assignable security group. Unfortunately this cannot be modified on existing ones. Search for: "cannot be changed later" here: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-create-eligible?tabs=ms-powershell>

upvoted 2 times

 **ServerBrain** 3 months ago

**Selected Answer: B**

recreate group, set isAssignableToRole

upvoted 2 times

 **mali1969** 3 months, 4 weeks ago

Correct answer is "Add an owner to IT\_Group1"

upvoted 1 times

 **mali1969** 3 months, 4 weeks ago

and also answer A is corrected

A. Change Membership type of IT\_Group1 to Dynamic User

upvoted 1 times

## Case Study -

## Overview -

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

## Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | <i>None</i>                       |
| User2 | <i>None</i>                       |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner       | Members                        |
|-------------|----------|-----------------|-------------|--------------------------------|
| IT_Group1   | Security | Assigned        | <i>None</i> | All users in the IT department |
| AdatumUsers | Security | Assigned        | <i>None</i> | User1, User2                   |

## Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

## Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

## Requirements. Planned Changes -

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

## Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You need to implement the planned changes for litware.com.

What should you configure?

A. Azure AD Connect cloud sync between the Azure AD tenant and litware.com

**B. Azure AD Connect to include the litware.com domain**

C. staging mode in Azure AD Connect for the litware.com domain

### Correct Answer: B

Community vote distribution

A (100%)

 0byte 2 months, 1 week ago

**Selected Answer: A**

Even though Azure Connect Sync (Azure AD Connect) supports syncing objects from multiple AD forests, it does not support syncing from more than one on-prem server (<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/plan-connect-topologies#multiple-forests-multiple-sync-servers-to-one-microsoft-entra-tenant>). For this to work, AD trust would be required and we cannot do it.

Cloud Sync does support multi-forest natively:

<https://learn.microsoft.com/en-us/azure/active-directory/cloud-sync/plan-cloud-sync-topologies#multi-forest-single-microsoft-entra-tenant>

upvoted 2 times

 Kipper\_2022 2 months, 3 weeks ago

**Selected Answer: A**

No trust = Cloud sync

upvoted 2 times

 penatuna 2 months, 3 weeks ago

**Selected Answer: A**

Existing Environment. Litware Environment:  
"Litware has an AD DS forest named litware.com."

Planned Changes:  
"Sync the AD DS users and groups of litware.com with the Azure AD tenant."

Technical Requirements:  
"Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains."

You need a Azure AD Connect Cloud Sync to connect to multiple disconnected on-premises AD forests.

See the video from 7:42  
<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/cloud-sync/what-is-cloud-sync>

You can also use evaluate your options using the Wizard to evaluate sync options:

<https://setup.microsoft.com/azure/add-or-sync-users-to-azure-ad>

upvoted 2 times

 **ServerBrain** 3 months ago

**Selected Answer: A**

"Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains."

upvoted 2 times

 **KrissB** 3 months, 4 weeks ago

There is a requirement to not create a trust between the two merging companies ADDS. Wouldn't cloud sync be the right selection?

upvoted 2 times

 **AZ\_Master** 4 months, 1 week ago

Why not A for cloud sync?

"Support for synchronizing to an Azure AD tenant from a multi-forest disconnected Active Directory forest environment: The common scenarios include merger & acquisition (where the acquired company's AD forests are isolated from the parent company's AD forests), and companies that have historically had multiple AD forests."

Ref: <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/cloud-sync/what-is-cloud-sync>

upvoted 4 times

 **katvik001** 4 months, 2 weeks ago

B is correct, litware.com should be included in AADC.

upvoted 4 times

You have the Azure resources shown in the following table.

| Name   | Description                                               |
|--------|-----------------------------------------------------------|
| User1  | User account                                              |
| Group1 | Security group that uses the Dynamic user membership type |
| VM1    | Virtual machine with a system-assigned managed identity   |
| App1   | Enterprise application                                    |
| RG1    | Resource group                                            |

To which identities can you assign the Contributor role for RG1?

- A. User1 only
- B. User1 and Group1 only
- C. User1 and VM1 only
- D. User1, VM1, and App1 only
- E. User1, Group1, VM1, and App1

**Correct Answer: E**

*Community vote distribution*

E (76%)      B (24%)

 **RoelvD** 2 weeks, 6 days ago

**Selected Answer: E**

<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps>

- \* User
- \* Group
- \* Service Principal
- \* Managed Identity

Screenshot: VM1 = Virtual machine WITH A SYSTEM-ASSIGNED MANAGED IDENTITY

Enterprise app is one of three types of Service Principals:

- \* Application
- \* Managed Identity
- \* Legacy

<https://learn.microsoft.com/en-us/entra/identity-platform/app-objects-and-service-principals?tabs=browser>  
upvoted 1 times

 **Nyamnyam** 4 weeks, 1 day ago

**Selected Answer: E**

E. should be correct: User and Group with no doubt. VM has MI => works as well. Service principal = Enterprise app => this works as well.  
upvoted 1 times

 **ACSC** 2 months, 1 week ago

**Selected Answer: E**

You can assign RBAC roles to any of the options, user, group, MI and apps.  
upvoted 4 times

 **j11v0sud** 2 months, 1 week ago

**Selected Answer: E**

Tested in-lab, fyi user-assigned managed identity works also  
upvoted 4 times

 **mtberdaan** 3 months ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps>  
I think the scope is RG1 here, so you can only assign the role to a User, Group, Service principal or Managed Identity.  
So I feel like this should be B  
upvoted 4 times

RoelvD 2 weeks, 6 days ago

You are mistaken. The screenshot literally says:  
VM1 = Virtual machine WITH A SYSTEM-ASSIGNED MANAGED IDENTITY

And an enterprise app is one of three types of Service Principals:

- \* Application
- \* Managed Identity
- \* Legacy

<https://learn.microsoft.com/en-us/entra/identity-platform/app-objects-and-service-principals?tabs=browser>  
upvoted 1 times

ServerBrain 3 months, 1 week ago

**Selected Answer: E**

I'm failing to establish how you cannot assign to groups. Would love test this and see..  
E looks best for the answer.

upvoted 3 times

c2thelint 3 months, 1 week ago

E looks correct. <https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps>  
upvoted 2 times

Kyumogi 3 months, 2 weeks ago

Un contributeur Azure AD est généralement une identité qui a la capacité de gérer certaines ressources liées à Azure AD, telles que les utilisateurs, les groupes, les applications et les paramètres de sécurité.

upvoted 1 times

KrissB 3 months, 4 weeks ago

I would say answer is A.  
A group cannot be added as a member of role assignable group. You cannot add a Dynamic user membership type.  
<https://learn.microsoft.com/en-us/azure-active-directory/roles/groups-concept>  
upvoted 4 times

einkaufacs 2 months, 2 weeks ago

It is not about assigning to azure ad roles. It is about assigning contributor permissions to azure resources. In this case to a Resource Group.  
You can assign dynamic user groups to azure resources. As well as Users, managed identities and apps. So it is E.  
upvoted 1 times

**HOTSPOT**

You have an Azure AD tenant that contains a user named User1. User1 is assigned the User Administrator role.

You need to configure External collaboration settings for the tenant to meet the following requirements:

- Guest users must be prevented from querying staff email addresses.
- Guest users must be able to access the tenant only if they are invited by User1.

Which three settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Guest user access restrictions:

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 restrictions:

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  
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:

|     |
|-----|
| No  |
| Yes |

## Answer Area

Guest user access restrictions:

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)**

Correct Answer:

Guest invite restrictions:

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  
**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:

No  
Yes

RoelvD 2 weeks, 6 days ago

'only if they are invited by User1' > This is impossible. But I guess this is the best answer given the options...

<https://learn.microsoft.com/en-us/microsoft-365/solutions/limit-who-can-invite-guests?view=o365-worldwide>

"Note that global administrators can always invite guests regardless of this setting."

You have at least one global admin and All global admins, User admins & Guest Inviter Role can send guest invites or nobody at all.

upvoted 1 times

Nyamnyam 4 weeks, 1 day ago

Correct

upvoted 1 times

sehlohomoletsane 2 months, 4 weeks ago

tested in lab  
the answer is correct

upvoted 1 times

ServerBrain 3 months, 1 week ago

100% correct  
upvoted 1 times

EmnCours 3 months, 3 weeks ago

Correct  
upvoted 1 times

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all users.

You needed to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the Groups blade in the Azure Active Directory admin center
- B. the Set-AzureAdUser cmdlet
- C. the Identity Governance blade in the Azure Active Directory admin center
- D. the Licenses blade in the Azure Active Directory admin center

**Correct Answer: D**

*Community vote distribution*

D (100%)

✉️  **ServerBrain** 3 months ago

**Selected Answer: D**

D is correct.  
B is used to configure properties for user accounts, which is not what the question is about  
upvoted 1 times

✉️  **mtberdaan** 3 months ago

B is not correct here, it should be Set-AzureADUserLicense or Set-MsolUserLicense.

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/remove-licenses-from-user-accounts-with-microsoft-365-powershell?view=o365-worldwide>

upvoted 1 times

✉️  **Vince\_MCT** 3 months, 2 weeks ago

Agree. it should be powershell script  
upvoted 1 times

✉️  **stai** 3 months, 3 weeks ago

I think B is correct.<https://learn.microsoft.com/en-us/microsoft-365/enterprise/configure-user-account-properties-with-microsoft-365-powershell?view=o365-worldwide>  
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 a user named User1.

You need to ensure that User1 can update the status of Identity Secure Score improvement actions.

Solution: You assign the Security Operator role to User1.

Does this meet the goal?

A. Yes

**B. No**

**Correct Answer: B**

*Community vote distribution*

B (100%)

nils241 Highly Voted 4 months ago

**Selected Answer: B**

B

With read and write access, you can make changes and directly interact with identity secure score.

Global administrator

Security administrator

Exchange administrator

SharePoint administrator

Security Operator has only read access, so he can not update anything

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#who-can-use-the-identity-secure-score>  
upvoted 5 times

sehlohomoletsane Most Recent 2 months, 4 weeks ago

**Selected Answer: B**

The answer is no

upvoted 1 times

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

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

You have a Microsoft 365 E5 subscription.

You create a user named User1.

You need to ensure that User1 can update the status of Identity Secure Score improvement actions.

Solution: You assign the SharePoint Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: A**

A. Yes

upvoted 1 times

 **nils241** 4 months ago

**Selected Answer: A**

From Microsoft:

With read and write access, you can make changes and directly interact with identity secure score.

Global administrator

Security administrator

Exchange administrator

SharePoint administrator

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#who-can-use-the-identity-secure-score>  
upvoted 2 times

 **1c67a2c** 4 months ago

You need read and write permissions:

(<https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide#read-and-write-roles>)

Global administrator

Security administrator

Exchange administrator

SharePoint administrator

upvoted 1 times

You have an Azure AD tenant that contains a user named Admin1.

You need to ensure that Admin1 can perform only the following tasks:

- From the Microsoft 365 admin center, create and manage service requests.
- From the Microsoft 365 admin center, read and configure service health.
- From the Azure portal, create and manage support tickets.

The solution must minimize administrative effort.

What should you do?

- A. Create an administrative unit and add Admin1.
- B. Enable Azure AD Privileged Identity Management (PIM) for Admin1.
- C. Assign Admin1 the Helpdesk Administrator role.
- D. Create a custom role and assign the role to Admin1.

**Correct Answer: D**

*Community vote distribution*

C (56%)

D (41%)

 **hellawaits111** Highly Voted 4 months ago

**Selected Answer: C**

Role explained here:

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

upvoted 7 times

 **Logitech** 2 months, 2 weeks ago

You need to ensure that Admin1 can perform only the following tasks... Sounds pretty clear that the user should not be able to do more than this 3 things.

With Helpdesk Admin you can do more. Really stupid MS Question again....

D should be the answer.

upvoted 2 times

 **kanag1** Highly Voted 4 months ago

**Selected Answer: C**

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

upvoted 5 times

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

**Selected Answer: D**

It doesn't ask for password resets so why would you give such privileges. Has to be D.

upvoted 1 times

 **kijken** 2 weeks, 1 day ago

**Selected Answer: D**

Least privileged option is D. C can be, but has too much permissions

upvoted 1 times

 **Nyamnyam** 4 weeks, 1 day ago

**Selected Answer: D**

ONLY the following tasks. Indeed Helpdesk Admin can fulfill the three requirements, but has other permissions, which are labeled PRIVILEGED in <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#helpdesk-administrator>

upvoted 2 times

 **MacDanorld** 1 month ago

**Selected Answer: D**

You need to make sure Admin1 can perform ONLY the following tasks sound like LEAST PRIVILEGE should be factored into your answer.

upvoted 1 times

 **Nivos23** 1 month ago

**Selected Answer: D**

The main requirement is to ensure that Admin1 can perform only the specified tasks and minimize administrative effort. The Helpdesk Administrator role (option C) is not the best choice because it grants additional privileges beyond the specified tasks.

To ensure that Admin1 can perform only the three specified tasks with the minimum administrative effort, you should choose option D:

D. Create a custom role and assign the role to Admin1.

Creating a custom role allows you to define and assign only the necessary permissions for the specified tasks without granting broader privileges. This approach aligns with the requirement to minimize administrative effort while ensuring that Admin1 can perform only the specified tasks.

upvoted 1 times

 **BenLam** 1 month ago

C - Helpdesk Admin can manage tickets so no need to customise. Check in Azure AD and look for helpdesk admin role and go to the description it clearly says can manage tickets

upvoted 1 times

 **Larax** 1 month, 2 weeks ago

**Selected Answer: C**

For me it's C because they ask us the solution with the minimal administrative effort and not the least privileged.

least administrative --> C

Least privileged --> D

upvoted 3 times

 **curtmcgirt** 3 weeks ago

but they also use the word "\_only\_ these tasks."

upvoted 2 times

 **ACSC** 1 month, 4 weeks ago

**Selected Answer: D**

There is a restriction for the tasks Admin1 can do. The role must be customized.

upvoted 1 times

 **0byte** 2 months, 1 week ago

**Selected Answer: D**

Initially I was going for C, because Helpdesk Administrator can do all the required tasks and assigning a built-in role would minimize needed effort. However, the question does state:

"You need to ensure that Admin1 can perform only the following tasks"

Helpdesk Administrator is a privileged role and can do much more than the three tasks. I think it should be D.

upvoted 2 times

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: C**

C. Assign Admin1 the Helpdesk Administrator role.

This is the best solution because the Helpdesk Administrator role allows the user to perform the tasks specified in the question.

upvoted 2 times

 **betaC4t** 2 months, 1 week ago

**Selected Answer: D**

D. Create a custom role and assign the role to Admin1.

upvoted 2 times

 **ACSC** 2 months, 1 week ago

**Selected Answer: D**

HelpDesk Administrator role does much more than the required tasks. So, you should create a custom role.

upvoted 1 times

 **MacWilson** 2 months, 1 week ago

Yes it appears that is too many should be custom.

upvoted 1 times

 **MacWilson** 2 months, 2 weeks ago

**Selected Answer: C**

Its C. Verbatim here <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#helpdesk-administrator>

upvoted 2 times

 **MacWilson** 2 months, 2 weeks ago

Its C. Verbatim here <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#helpdesk-administrator>

upvoted 1 times

 **Logitech** 2 months, 2 weeks ago

**Selected Answer: D**

You need to ensure that Admin1 can perform only the following tasks, C does not fulfill this.

upvoted 2 times

店铺：专业认证88

店铺：专业认证88

**HOTSPOT**

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

You need to ensure that user authentication always occurs by validating passwords against the AD DS domain.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Configure:

- Azure AD Password protection
- Cross-tenant synchronization
- Pass-through authentication
- Password hash synchronization

Use:

- Azure AD Connect
- Microsoft Identity Manager (MIM)
- The Microsoft Entra admin center
- The Microsoft Purview compliance portal

**Answer Area**

Configure:

- Azure AD Password protection
- Cross-tenant synchronization
- Pass-through authentication**
- Password hash synchronization

Correct Answer:

Use:

- Azure AD Connect**
- Microsoft Identity Manager (MIM)
- The Microsoft Entra admin center
- The Microsoft Purview compliance portal

 **penatuna** 2 months, 2 weeks ago

PTA and Azure AD Connect.

PTA:

When PTA is deployed, the user provides a password on the Azure AD login page, and Azure AD validates the password with on-premises Active Directory with the help of the PTA agent deployed on-premises.

Password hash sync is wrong, cause it only syncs the on-premise passwords to Azure in every too minutes. The authentication happens in Azure AD.

Azure AD Connect:

You can enable Pass-through Authentication through Azure AD Connect.

If you're installing Azure AD Connect for the first time, choose the custom installation path. At the User sign-in page, choose Pass-through Authentication as the Sign On method. On successful completion, a Pass-through Authentication Agent is installed on the same server as Azure AD Connect. In addition, the Pass-through Authentication feature is enabled on your tenant.

If you have already installed Azure AD Connect by using the express installation or the custom installation path, select the Change user sign-in task on Azure AD Connect, and then select Next. Then select Pass-through Authentication as the sign-in method. On successful completion, a Pass-through Authentication Agent is installed on the same server as Azure AD Connect and the feature is enabled on your tenant.

upvoted 1 times

 **Wicke** 2 months, 3 weeks ago

MS: <https://learn.microsoft.com/en-us/azure/active-directory-domain-services/synchronization#password-hash-synchronization-and-security-considerations>

First one should be definitely Password Hash

upvoted 1 times

 **CoSaWe** 3 months ago

password hash synchronization: <https://learn.microsoft.com/en-us/azure/active-directory-domain-services/synchronization#password-hash-synchronization-and-security-considerations>

upvoted 1 times

 **ServerBrain** 3 months, 1 week ago

Correct. PTA using AD Connect

upvoted 4 times

 **EmnCours** 3 months, 3 weeks ago

Correct Answer

upvoted 1 times

 **sehlohomoletsane** 4 months ago

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises>

upvoted 1 times

You have a Microsoft 365 tenant that uses the domain named fabrikam.com. The Guest invite settings for Azure Active Directory (Azure AD) are configured as shown in the exhibit. (Click the Exhibit tab.)

### Guest user access

Guest user access restrictions [\(i\)](#)

[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 [\(i\)](#)

[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 [\(i\)](#)

[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)

A user named bsmith@fabrikam.com shares a Microsoft SharePoint Online document library to the users shown in the following table.

| Name  | Email              | Description                                             |
|-------|--------------------|---------------------------------------------------------|
| User1 | User1@contoso.com  | A guest user in fabrikam.com                            |
| User2 | User2@outlook.com  | A user who has never accessed resources in fabrikam.com |
| User3 | User3@fabrikam.com | A user in fabrikam.com                                  |

Which users will be emailed a passcode?

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

**Correct Answer: A**

*Community vote distribution*

A (57%)

B (43%)

 **fatilaura** 2 weeks ago

What happens to my existing guest users if I enable email one-time passcode?

Your existing guest users won't be affected if you enable email one-time passcode, as your existing users are already past the point of redemption. Enabling email one-time passcode will only affect future redemption process activities where new guest users are redeeming into the tenant.

upvoted 1 times

**Matajare** 2 weeks, 5 days ago

**Selected Answer: A**

I think "A".

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode> (At the end of page)

--Frequently asked questions--

What happens to my existing guest users if I enable email one-time passcode?

Your existing guest users won't be affected if you enable email one-time passcode, as your existing users are already past the point of redemption. Enabling email one-time passcode will only affect future redemption process activities where new guest users are redeeming into the tenant.

Say: Your existing guest users won't be affected...

User1 is already inside. So it doesn't affect him.

upvoted 2 times

**kijken** 3 weeks, 1 day ago

B

A is wrong because is @ outlook.com and that is a microsoft account and authenticated by microsoft

upvoted 1 times

**Nivos23** 1 month ago

**Selected Answer: A**

I think the answer is A. User2 only

upvoted 2 times

**BenLam** 1 month ago

**Selected Answer: B**

It will be the guest as outlook.com is a microsoft account already.

<https://support.microsoft.com/en-us/office/why-you-need-a-microsoft-account-or-work-or-school-account-with-microsoft-365-or-office-914e6610-2763-47ac-ab36-602a81068235#:~:text=Accounts%20such%20as%20an%20outlook,therefore%20already%20considered%20Microsoft%20accounts.>

Also guest sessions expire after 24 hours so the user will need to be provided with a new one. <https://learn.microsoft.com/en-us/entra/external-id/one-time-passcode>

upvoted 2 times

**Nivos23** 1 month ago

**Selected Answer: A**

I think the answer is A. User2 only

Because it will never connect before that and also because user1 has limited accesses

upvoted 2 times

**lahl** 1 month, 2 weeks ago

B

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode#when-does-a-guest-user-get-a-one-time-passcode>

upvoted 1 times

**lahl** 1 month, 1 week ago

None of the answers is correct! Got this question in the exam and the user 3 was gmail account.

upvoted 5 times

**Florian74** 1 month, 3 weeks ago

**Selected Answer: B**

For me, the Outlook user has already a MS account and log in with his password.

upvoted 1 times

**ACSC** 1 month, 4 weeks ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode#user-experience-for-one-time-passcode-guest-users>

upvoted 3 times

**Obyte** 2 months, 1 week ago

**Selected Answer: B**

Since there is no mention about enabling passcode option, we need to assume it has already been enabled, at some point in the past. Out of the three users, the only one that could've have passcode set as its authentication method is User1 (this is assuming contoso.com doesn't run on M365 :-)).

User3 has already account in Fabrikam, so can login, and User2 already has Microsoft account (Outlook.com) and can use this to login. Passcode is

basically an option to login to Microsoft without creating an account in Microsoft. If a user already has an account in MS (work, school or personal, on outlook) you won't get passcode as an option to login.

upvoted 2 times

✉ **Nyamnyam** 4 weeks, 1 day ago

I follow Obyte logic: User2 has personal MSA. User3 is part of the org. They will both authenticate against Microsoft with their respective credentials. User1 is not stated as MS Entra tenant client. AND: "When a user redeems a one-time passcode and later obtains an MSA, Microsoft Entra account, or other federated account, they'll continue to be authenticated using a one-time passcode.", so don't get fooled on the fact that it is already a Guest. <https://learn.microsoft.com/en-us/entra/external-id/one-time-passcode#when-does-a-guest-user-get-a-one-time-passcode>

upvoted 2 times

✉ **kalyankrishna1** 2 months, 2 weeks ago

**Selected Answer: A**

Users and guest already available in the tenant dont need a passcode

upvoted 2 times

✉ **kalyankrishna1** 2 months, 2 weeks ago

nope I take it back , its B

upvoted 2 times

✉ **Wicke** 2 months, 3 weeks ago

**Selected Answer: B**

Realistically answer should be B because user 1 =outlook.com is a microsoft account and because of that, he/she will not get an "one-time passcode"

upvoted 3 times

✉ **mdijoux25** 3 months, 2 weeks ago

**Selected Answer: B**

Also agree with mali1969

upvoted 1 times

✉ **e56f13e** 3 months, 2 weeks ago

**Selected Answer: B**

Agree with mali1969

upvoted 1 times

✉ **EmnCours** 3 months, 3 weeks ago

**Selected Answer: A**

Correct Answer: A

upvoted 2 times

✉ **mali1969** 3 months, 3 weeks ago

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode>

upvoted 1 times

✉ **mali1969** 3 months, 3 weeks ago

When a guest user redeems an invitation or uses a link to a resource that has been shared with them, they'll receive a one-time passcode if:

They don't have an Azure AD account.

They don't have a Microsoft account.

The inviting tenant didn't set up federation with social (like Google) or other identity providers.

They don't have any other authentication method or any password-backed accounts.

Email one-time passcode is enabled.

At the time of invitation, there's no indication that the user you're inviting will use one-time passcode authentication. But when the guest user signs in, one-time passcode authentication will be the fallback method if no other authentication methods can be used.

upvoted 2 times



You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the Administrative units blade in the Azure Active Directory admin center
- B. the Set-MsolUserLicense cmdlet
- C. the Groups blade in the Azure Active Directory admin center
- D. the Set-WindowsProductKey cmdlet

**Correct Answer: A**

*Community vote distribution*

B (100%)

BenLam 1 month ago

**Selected Answer: B**

AU does not manage licenses regardless what it says on Microsoft site. <https://www.cloudpartner.fi/?p=6193>

I have tested and i do not see an option to manage licenses.

upvoted 1 times

JimboJones99 1 month, 1 week ago

**Selected Answer: B**

B as per the other questions

upvoted 1 times

MS\_RF 1 month, 1 week ago

**Selected Answer: B**

B of course

upvoted 1 times

JckD4Ni3L 1 month, 2 weeks ago

**Selected Answer: B**

B is the correct answer...

upvoted 1 times

shuhaidawahab 1 month, 3 weeks ago

REPEATED QUESTIONS

You can unassign licenses from users on either the Active users page, or on the Licenses page. The method you use depends on whether you want to unassign product licenses from specific users or unassign users licenses from a specific product.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1. the Licenses blade in the Azure Active Directory admin center
2. the Set-MsolUserLicense cmdlet

Other incorrect answer options you may see on the exam include the following:

- Ⓐ the Administrative units blade in the Azure Active Directory admin center
- Ⓐ the Groups blade in the Azure Active Directory admin center
- Ⓐ the Set-AzureAdGroup cmdlet

upvoted 1 times

Ed2learn 1 month, 1 week ago

I really don't mind repeated questions but it seems like everyone of these reviews has at least one that gets repeated more than others. For this test, I am getting to the point that I am just going to assume Set-MsolUserLicense is the right answer whenever I see it on the test no matter the question. :)

upvoted 1 times

Anonymous1312 1 month, 3 weeks ago

**Selected Answer: B**

As with the previous 100 times this question has been asked it is  
B. the Set-MsolUserLicense cmdlet  
upvoted 1 times

MicrosoftMaster2023 1 month, 3 weeks ago

**Selected Answer: B**

This PowerShell cmdlet is used to adjust licenses for users in the Microsoft 365 admin center and can be used to add, replace, or remove licenses. It allows for bulk operations when used in a script, making it quite efficient for managing licenses for a large number of users.  
upvoted 1 times

## HOTSPOT

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD and contains the users shown in the following table.

| Name  | Organizational unit (OU) |
|-------|--------------------------|
| User1 | OU1                      |
| User2 | OU2                      |

In Azure AD Connect, Domain/OU Filtering is configured as shown in the following exhibit.

The screenshot shows the 'Domain and OU filtering' configuration page in the Azure AD Connect wizard. The left sidebar lists navigation options, and the main area displays the filtering settings for the 'contoso.com' directory. The 'Sync selected domains and OUs' option is selected. A tree view shows the domain structure with specific OUs checked for synchronization: 'OU1' and 'Users' under 'contoso.com'. Navigation buttons 'Previous' and 'Next' are at the bottom.

Azure AD Connect is configured as shown in the following exhibit.

Welcome  
Express Settings  
Required Components  
User Sign-In  
Connect to Azure AD  
Sync  
  Connect Directories  
  Azure AD sign-in  
  Domain/OU Filtering  
Identifying users  
  Filtering  
Optional Features  
**Configure**

## Ready to configure

Once you click Install, we will do the following:

- Configure synchronization services on this computer
- Install Microsoft Azure AD Connect Authentication Agent for Pass-Through Authentication
- Enable Pass-through authentication
- Configure Source Anchor Attribute
- Configure sk220630outlook.onmicrosoft.com - AAD Connector
- Configure contoso.com Connector
- Disable Password hash synchronization
- Enable Password writeback
- Enable Azure AD Export Deletion Threshold (500)

Start the synchronization process when configuration completes.

Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.

Previous

Install

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

NOTE: Each correct selection is worth one point.

### Answer Area

| Statements                                                                                                 | Yes                   | No                    |
|------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| User1 can use self-service password reset (SSPR) to reset his password.                                    | <input type="radio"/> | <input type="radio"/> |
| If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller. | <input type="radio"/> | <input type="radio"/> |
| User2 can be added to a Microsoft SharePoint Online site as a member.                                      | <input type="radio"/> | <input type="radio"/> |

### Answer Area

#### Statements

**Correct Answer:**

User1 can use self-service password reset (SSPR) to reset his password.

If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller.

User2 can be added to a Microsoft SharePoint Online site as a member.

Yes

No



Yes

No



**niesz1** Highly Voted 1 month, 3 weeks ago

YES

YES

NO- User 2 is not synced to 365

upvoted 13 times

**Another\_one** Highly Voted 1 month, 3 weeks ago

NO

YES

NO

By default SSPR is enabled, but not configured. You have to configure SSPR for users to be able to use it.

upvoted 7 times

 **OrangeSG** 3 weeks, 5 days ago

Password write-backup are enabled in the last screenshot.  
upvoted 2 times

 **85ae6ea** Most Recent 2 weeks ago

YES - Pass writeback is enabled (and SSPR works with PTA, PHS and ADFS federated environments)  
YES - Because auth is PTA  
NO - User2 not synced  
upvoted 1 times

 **Kali13** 3 weeks ago

NO : password hash synchronization is disabled  
YES : PTA is enabled  
NO : No Sync to AAD  
upvoted 1 times

Question #61

Topic 1

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the Update-MgGroup cmdlet
- B. the Licenses blade in the Azure Active Directory admin center**
- C. the Set-WindowsProductKey cmdlet
- D. the Administrative units blade in the Azure Active Directory admin center

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **ralphw** 1 week, 2 days ago

I ate the purple berries. And this question is starting to make as much sense.  
upvoted 1 times

 **OrangeSG** 3 weeks, 5 days ago

**Selected Answer: B**

There are several versions of this question in the exam. The question has two possible correct answers:

1. the Licenses blade in the Azure Active Directory admin center
2. the Set-MsolUserLicense cmdlet

Other incorrect answer options you may see on the exam include the following:

- the Administrative units blade in the Azure Active Directory admin center
- the Groups blade in the Azure Active Directory admin center
- the Set-AzureAdGroup cmdlet

upvoted 1 times

 **Ed2learn** 1 month, 1 week ago

the other right answer.  
upvoted 2 times

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

| Name   | Role                      |
|--------|---------------------------|
| Admin1 | User Administrator        |
| Admin2 | Password Administrator    |
| Admin3 | Application Administrator |

You need to compare the role permissions of each user. The solution must minimize administrative effort.

What should you use?

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

**Correct Answer: C**

*Community vote distribution*

B (84%)      C (16%)

 **Julesy** Highly Voted 2 months ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/admin-roles-page#compare-roles>

upvoted 7 times

 **Alscoran** 1 week, 1 day ago

When you look at that site and the available roles, you WILL NOT see the Application Administrator listed. You do see all three when you look at Entra roles. So it must be C.

upvoted 1 times

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

**Selected Answer: C**

Application Administrator not visible on M365 site

upvoted 1 times

 **Blagojche** 1 week ago

Application Administrator is present in M365 Admin Center, check!

upvoted 1 times

 **Alscoran** 6 days, 6 hours ago

Weird that it doesn't show in the documentation but does show up in the admin center. I cannot find a compare function on the Entra ID portal either. So I guess its B after all !

upvoted 1 times

 **MacDanorld** 2 weeks, 4 days ago

**Selected Answer: B**

The Answer is B. the Microsoft 365 admin center. I have tested it and all roles are there and you can compare them in the 365 admin center

upvoted 1 times

 **JaySapkota** 3 weeks, 6 days ago

**Selected Answer: C**

Entra Admin Center has all the roles

upvoted 1 times

 **penatuna** 1 month ago

**Selected Answer: B**

Just tested with Microsoft 365 admin center, and you can compare all three roles mentioned.

upvoted 2 times

 **Ed2learn** 1 month, 1 week ago

I don't see Application Administrator in the Microsoft 365 admin center. Unless I am missing it, the answer is C.  
I suspect they are trying to make the question about the tool so perhaps in the exam they use a different role than Application Admin?  
upvoted 1 times

 **JanioHSilva** 1 day, 5 hours ago  
Eu acredito que você passou despercebido  
upvoted 1 times

 **AlfaExamPro** 1 month, 1 week ago  
Read basic properties on all resources in the Microsoft 365 admin center for All that 3 Roles  
upvoted 1 times

 **Akira1979** 1 month, 1 week ago  
**Selected Answer: C**  
Correct answer is "C".

Yes, you can compare admin roles in M365 admin portal, but there is no Application Admin role in M365.  
upvoted 1 times

 **haazybanj** 1 month, 1 week ago  
**Selected Answer: B**  
B is right  
upvoted 2 times

 **Florian74** 1 month, 3 weeks ago  
**Selected Answer: B**  
To compare roles: M365 admin portal  
upvoted 2 times

 **AK\_1234** 1 month, 3 weeks ago  
C- Entra Admin Center  
upvoted 1 times

 **Softeng** 2 months ago  
**Selected Answer: B**  
It's M365 admin portal. Look at Julesy link.  
upvoted 2 times

You have a Microsoft Exchange organization that uses an SMTP address space of contoso.com.

Several users use their contoso.com email address for self-service sign-up to Azure AD.

You gain global administrator privileges to the Azure AD tenant that contains the self-signed users.

You need to prevent the users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services.

Which PowerShell cmdlet should you run?

- A. Update-MgOrganization
- B. Update-MgPolicyPermissionGrantPolicyExclude
- C. Update-MgDomain
- D. Update-MgDomainFederationConfiguration

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **haazybanj** 4 weeks ago

**Selected Answer: B**

The correct answer is B. Update-MgPolicyPermissionGrantPolicyExclude.

The Update-MgPolicyPermissionGrantPolicyExclude cmdlet is used to exclude a policy from being applied to a specific set of users. In this case, you can use the cmdlet to exclude the self-service sign-up policy from being applied to users with the contoso.com SMTP address space.

upvoted 2 times

 **Ed2learn** 1 month, 1 week ago

I think the answer is B.

The given answer seems to be related to the organizational data not setting what can and cannot be done within the organization.

B does provide mechanisms to prevent user actions.

C - doesn't seem to apply at all.

upvoted 1 times

**HOTSPOT**

You have an Azure AD tenant.

You need to configure the following External Identities features:

- B2B collaboration
- Monthly active users (MAU)-based pricing

Which two settings should you configure? To answer, select the settings in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area****External Identities**

Contoso Ltd - Azure Active Directory

- Search
- Overview
- Cross-tenant access settings
- All identity providers
- External collaboration settings
- Diagnose and solve problems

**Self-service sign up**

- Custom user attributes
- All API connectors
- User flows

**Subscriptions**

- Linked subscriptions

**Lifecycle management**

- Terms of use
- Access reviews

## Answer Area

The screenshot shows the 'External Identities' blade for the 'Contoso Ltd - Azure Active Directory'. The left sidebar lists several options: 'Search', 'Overview', 'Cross-tenant access settings', 'All identity providers', 'External collaboration settings' (which is highlighted with a black box), and 'Diagnose and solve problems'. A red watermark '店铺：专业认证88' is visible across the page.

Correct Answer:

### Self-service sign up

- Custom user attributes
- All API connectors
- User flows

### Subscriptions

- Linked subscriptions

### Lifecycle management

- Terms of use
- Access reviews

penatuna 1 week, 1 day ago

The second one is Linked Subscriptions.

For the first one, we don't have enough info to be sure. What B2B setting are we configuring? I assume that the answer is external collaboration settings, since there's no mention about collaborating with another Microsoft Entra organization.

Microsoft says:

B2B collaboration is enabled by default, but comprehensive admin settings let you control your inbound and outbound B2B collaboration with external partners and organizations:

For B2B collaboration with other Microsoft Entra organizations, use cross-tenant access settings. Manage inbound and outbound B2B collaboration, and scope access to specific users, groups, and applications. Set a default configuration that applies to all external organizations, and then create individual, organization-specific settings as needed. Using cross-tenant access settings, you can also trust multi-factor (MFA) and device claims (compliant claims and Microsoft Entra hybrid joined claims) from other Microsoft Entra organizations.

upvoted 1 times

penatuna 1 week, 1 day ago

Use external collaboration settings to define who can invite external users, allow or block B2B specific domains, and set restrictions on guest user access to your directory.

Use Microsoft cloud settings to establish mutual B2B collaboration between the Microsoft Azure global cloud and Microsoft Azure Government or Microsoft Azure operated by 21Vianet.

<https://learn.microsoft.com/en-us/entra/external-id/what-is-b2b#manage-collaboration-with-other-organizations-and-clouds>

upvoted 1 times

penatuna 1 week, 1 day ago

In Entra ID's Cross-tenant access settings it actually says this:

"Use cross-tenant access settings to manage collaboration with external Microsoft Entra tenants. For non-Microsoft Entra tenants, use collaboration settings."

upvoted 1 times

Nivos23 1 month ago

I think the answer is correct

External Collaboration settings

And

Linked Subscriptions

upvoted 4 times



You have an Azure AD tenant that contains the external user shown in the following exhibit.

You update the email address of the user.

You need to ensure that the user can authenticate by using the updated email address.

What should you do for the user?

- A. Modify the Authentication methods settings.
- B. Reset the password.
- C. Revoke the active sessions.
- D. Reset the redemption status.

**Correct Answer: D**

*Community vote distribution*

D (100%)

**kijken** 3 weeks, 1 day ago

Cool,  
I didnt know this one, I would have recreated the guest user  
upvoted 1 times

**kijken** 3 weeks, 1 day ago

answer is D btw  
upvoted 1 times

**OrangeSG** 3 weeks, 5 days ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/entra/external-id/reset-redemption-status>

update the guest user's sign-in information after they've redeemed your invitation for B2B collaboration. There might be times when you'll need to update their sign-in information, for example when:

- The user wants to sign in using a different email and identity provider
- etc

To manage these scenarios previously, you had to manually delete the guest user's account from your directory and reinvite the user. Now you can

use the Microsoft Entra admin center, PowerShell or the Microsoft Graph invitation API to reset the user's redemption status and reinvite the user while keeping the user's object ID, group memberships, and app assignments.

upvoted 2 times

## Question #66

Topic 1

You have an Azure AD tenant.

You need to ensure that only users from specific external domains can be invited as guests to the tenant.

Which settings should you configure?

- A. External collaboration settings
- B. All identity providers
- C. Cross-tenant access settings
- D. Linked subscriptions

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **haazybanj** 4 weeks ago

**Selected Answer: A**

The correct answer is A. External collaboration settings.

External collaboration settings allow you to control who can collaborate with your Azure AD tenant. You can use external collaboration settings to specify which external domains are allowed to be invited as guests to your tenant.

upvoted 3 times

You have an Azure AD tenant that contains a user named User1 and a Microsoft 365 group named Group1. User1 is the owner of Group1.

You need to ensure that User1 is notified every three months to validate the guest membership of Group1.

What should you do?

- A. Configure the External collaboration settings.
- B. Create an access review.**
- C. Configure an access package.
- D. Create a group expiration policy.

**Correct Answer: D**

*Community vote distribution*

B (100%)

 **Nazir97** 4 weeks, 1 day ago

**Selected Answer: B**

Access review

upvoted 1 times

 **penatuna** 4 weeks, 1 day ago

**Selected Answer: B**

A. External collaboration settings let you specify what roles in your organization can invite external users for B2B collaboration. These settings also include options for allowing or blocking specific domains, and options for restricting what external guest users can see in your Microsoft Entra directory.

B. Access reviews in Microsoft Entra ID, part of Microsoft Entra, enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed regularly to make sure only the right people have continued access.  
upvoted 1 times

 **penatuna** 4 weeks, 1 day ago

C. An access package is a bundle of resources that a team or project needs and is governed with policies. Access packages are defined in containers called catalogs. To reduce the risk of stale access, you should enable periodic reviews of users who have active assignments to an access package in entitlement management. You can enable reviews when you create a new access package or edit an existing access package assignment policy.

D. Group expiration policy can help remove inactive groups from the system and make things cleaner. It only removes inactive groups, it will NOT validate guest membership of group.

<https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview>

<https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure>

<https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-access-reviews-create>

<https://learn.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-groups-expiration-policy?view=o365-worldwide>

upvoted 1 times

 **haazybanj** 1 month ago

**Selected Answer: B**

The answer is B. Create an access review.

An access review is a process that allows you to review and manage the access of users and groups to resources. You can use access reviews to validate the guest membership of Group1 every three months.

upvoted 4 times

 **einkaufacs** 1 month ago

**Selected Answer: B**

Validating a membership is access review, in my opinion.

upvoted 3 times

You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.

You need to ensure that you can control access to Microsoft 365 resources by using conditional access policies.

What should you do first?

- A. Disable the User consent settings.
- B. Disable Security defaults.**
- C. Configure a multi-factor authentication (MFA) registration policy.
- D. Configure password protection for Windows Server Active Directory.

**Correct Answer: B**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

Community vote distribution

B (100%)

 **Eltooth** Highly Voted 2 years, 6 months ago

Taken from article in answer: "If your tenant was created on or after October 22, 2019, it is possible security defaults are already enabled in your tenant. To protect all of our users, security defaults are being rolled out to all new tenants created."

To enable CAP you have to disable Security defaults - Answer is correct.

upvoted 20 times

 **kalyankrishna1** Most Recent 2 months, 2 weeks ago

**Selected Answer: B**

Correct answer

upvoted 1 times

 **EmnCours** 4 months, 2 weeks ago

**Selected Answer: B**

B. Disable Security defaults

upvoted 1 times

 **mali1969** 5 months, 2 weeks ago

To control access to Microsoft 365 resources by using conditional access policies, you should first disable Security defaults. This is because Security defaults are a set of basic identity and access management features that are automatically enabled for new tenants. They are not compatible with conditional access policies.

After disabling Security defaults, you can then configure conditional access policies to control access to Microsoft 365 resources

upvoted 1 times

 **dule27** 6 months ago

**Selected Answer: B**

B. Disable Security defaults

upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: B**

Correct B

upvoted 1 times

 **francescoc** 8 months, 1 week ago

**Selected Answer: B**

B is correct.

If you're using Conditional Access in your environment today, security defaults won't be available to you.

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

upvoted 1 times

 **Aquintero** 10 months, 1 week ago

**Selected Answer: B**

Deshabilite los valores predeterminados de seguridad.

upvoted 1 times

 **Oknip** 10 months, 2 weeks ago

**Selected Answer: B**

Disable the security defaults to enable Conditional Access policies  
upvoted 2 times

 **[Removed]** 11 months, 4 weeks ago

**Selected Answer: B**

As per the Microsoft documentation, Microsoft recommend to disable security defaults if conditional access policies are used.  
upvoted 2 times

 **Boknows** 1 year, 1 month ago

On exam- 10/28/22  
upvoted 2 times

 **Seed001** 1 year, 4 months ago

**Selected Answer: B**

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults#conditional-access>  
upvoted 2 times

 **jedboy88** 1 year, 5 months ago

**Selected Answer: B**

You need to disable Security defaults to enable Conditional access policies, si the answer is correctt  
upvoted 3 times

 **shine98** 1 year, 5 months ago

On the exam - June 12, 2022  
upvoted 1 times

 **stromnessian** 1 year, 9 months ago

**Selected Answer: B**

Yes, it's B.  
upvoted 1 times

 **gwerin** 1 year, 9 months ago

**Selected Answer: B**

Disable security defaults  
upvoted 1 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.  
upvoted 1 times

Your company has a Microsoft 365 tenant.

The company has a call center that contains 300 users. In the call center, the users share desktop computers and might use a different computer every day. The call center computers are NOT configured for biometric identification.

The users are prohibited from having a mobile phone in the call center.

You need to require multi-factor authentication (MFA) for the call center users when they access Microsoft 365 services.

What should you include in the solution?

- A. a named network location
- B. the Microsoft Authenticator app
- C. Windows Hello for Business authentication
- D. FIDO2 tokens

**Correct Answer: D**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>

*Community vote distribution*

D (100%)

 **Ed2learn** Highly Voted 2 years, 5 months ago

ignoring the terrible working conditions, terribly configured network (or you would just set MFA and CA to ignore that network segment), and obviously micromanaging bosses - the given answer is correct.

upvoted 24 times

 **Beitran** Highly Voted 2 years, 7 months ago

The only logical option.

upvoted 24 times

 **Nivos23** Most Recent 1 month ago

**Selected Answer: D**

Correct Answer is D

upvoted 1 times

 **EmnCours** 4 months, 2 weeks ago

**Selected Answer: D**

Correct Answer: D

upvoted 1 times

 **dule27** 6 months ago

**Selected Answer: D**

D. FIDO2 tokens

upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: D**

Correct D

upvoted 1 times

 **Aquintero** 10 months, 1 week ago

**Selected Answer: D**

D. Fichas FIDO2

upvoted 2 times

 **Halwagy** 10 months, 3 weeks ago

**Selected Answer: D**

The FiDO2 token

upvoted 1 times

 **[Removed]** 11 months, 4 weeks ago

**Selected Answer: D**

Ali\_Pin explained correctly. FIDO2 is the correct answer.

upvoted 2 times

 **ali\_pin** 1 year, 5 months ago

A. a named network location - not an MFA option  
B. the Microsoft Authenticator app - no mobile phones allowed  
C. Windows Hello for Business authentication - no biometrical options in the office and the data is stored in the local device - they switch PCs every day  
  
so D. FIDO2 key  
upvoted 14 times

 **sapien45** 1 year, 5 months ago

Users can use passwordless credentials to access resources in tenants where they are a guest, but they may still be required to perform MFA in that resource tenant  
Fido2 is a MFAer  
upvoted 1 times

 **jasonga** 1 year, 6 months ago

windows hello for business can also use a PIN instead of biometrics so both it and fido are viable 店铺：专业认证88 but I think fido is better don't like the question as either could be user  
upvoted 1 times

 **ZauberSRS** 1 year ago

No, Windows Hello Pin is store locally, they may change computer every day it says  
upvoted 2 times

 **bleedinging** 1 year, 6 months ago

D. This one is clever. Windows hello for Business would require each user to scan their faces for each computer. It wouldn't be a viable solution.  
it'd have to be Fido2 instead.  
upvoted 3 times

 **janshal** 1 year, 7 months ago

The call center computers are NOT configured for biometric identification  
  
Answer- C  
upvoted 1 times

 **PanBrown** 1 year, 7 months ago

FIDO2 key is the only option in this situation.  
upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022  
upvoted 2 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.  
upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

All users who run applications registered in Azure AD are subject to conditional access policies.

You need to prevent the users from using legacy authentication.

What should you include in the conditional access policies to filter out legacy authentication attempts?

- A. a cloud apps or actions condition
- B. a user risk condition
- C. a client apps condition**
- D. a sign-in risk condition

**Correct Answer: C**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

Community vote distribution

C (100%)

 **JerryGolais** Highly Voted 2 years, 7 months ago

Client apps condition is the correct answer

upvoted 17 times

 **melatocaroca** Highly Voted 2 years, 4 months ago

Directly blocking legacy authentication

The easiest way to block legacy authentication across your entire organization is by configuring a Conditional Access policy that applies specifically to legacy authentication clients and blocks access.

Conditional Access policies apply to all client apps by default

Client apps

By default, all newly created Conditional Access policies will apply to all client app types even if the client apps condition is not configured.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

upvoted 13 times

 **Aquintero** 10 months, 1 week ago

Estoy deacuerdo contigo, en este caso para mi la respuesta no esta o no es clara o esta confusa. La informacion que brinda una solucion esta en el link <https://learn.microsoft.com/es-es/azure/active-directory/conditional-access/block-legacy-authentication#directly-blocking-legacy-authentication>

upvoted 1 times

 **haazybanj** Most Recent 4 weeks ago

**Selected Answer: C**

The correct answer is C. a client apps condition.

A client apps condition allows you to filter out legacy authentication attempts by specifying the client apps that users are allowed to use to sign in. To block legacy authentication, you can use a client apps condition to exclude all legacy authentication clients.

upvoted 1 times

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: C**

C. a client apps condition

Legacy authentication clients typically use older protocols such as IMAP, SMTP, POP3, and older versions of protocols like OAuth 2.0 and ActiveSync. By creating a conditional access policy that includes a "client apps" condition, you can target these legacy clients and restrict their access

upvoted 1 times

 **sherifhamed** 2 months, 2 weeks ago

**Selected Answer: C**

C. a client apps condition

In your conditional access policy, you can use a client apps condition to filter out legacy authentication attempts.

upvoted 1 times

 **Heshan** 4 months, 4 weeks ago

On the exam, 09/07/2023

upvoted 2 times

**AMZ** 5 months, 1 week ago

Question valid - 06/23

upvoted 2 times

**mali1969** 5 months, 2 weeks ago

To filter out legacy authentication attempts in the conditional access policies, you should include a client apps condition

To do this, you can create a Conditional Access policy that blocks legacy authentication requests. This policy is put in to Report-only mode to start so administrators can determine the impact they'll have on existing users

upvoted 1 times

**dule27** 6 months ago

**Selected Answer: C**

C. a client apps condition

upvoted 1 times

**ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: C**

C is correct

upvoted 1 times

**Halwagy** 10 months, 3 weeks ago

**Selected Answer: C**

Client App

upvoted 1 times

**[Removed]** 11 months, 4 weeks ago

**Selected Answer: C**

Correct answer given.

upvoted 1 times

**kerimnl** 1 year, 1 month ago

**Selected Answer: C**

C. a client apps condition

upvoted 1 times

**Tokiki** 1 year, 5 months ago

C is correct

upvoted 1 times

**shine98** 1 year, 5 months ago

On the exam - June 12, 2022

upvoted 2 times

**Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022

upvoted 2 times

**Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant.

You open the risk detections report.

Which risk detection type is classified as a user risk?

- A. impossible travel
- B. anonymous IP address
- C. atypical travel
- D. leaked credentials

**Correct Answer: D**

Leaked credentials indicates that the user's valid credentials have been leaked.

Note:

There are several versions of this question in the exam. The question can have other incorrect answer options, including the following:

- ⇒ password spray
- ⇒ malicious IP address
- ⇒ unfamiliar sign-in properties

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

*Community vote distribution*

D (93%) 7%

 **JakubK64** Highly Voted  2 years, 6 months ago

Correct - leaked credentials. Rest belongs to sign-in risk

upvoted 23 times

 **Nivos23** Most Recent  1 month ago

**Selected Answer: D**

D. leaked credentials  
upvoted 1 times

 **sherifhamed** 2 months, 2 weeks ago

**Selected Answer: D**

D. leaked credentials

Leaked credentials refer to instances where a user's username and password have been compromised and exposed externally. This is considered a user risk because it involves potential unauthorized access to a user's account due to the compromise of their login credentials.

upvoted 1 times

 **EmnCours** 4 months, 2 weeks ago

**Selected Answer: D**

Correct Answer: D  
upvoted 1 times

 **mali1969** 5 months, 2 weeks ago

The risk detection type that is classified as a user risk in Azure Active Directory (Azure AD) tenant is leaked credentials  
upvoted 1 times

 **dule27** 6 months ago

**Selected Answer: D**

D. leaked credentials  
upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: D**

correct D  
upvoted 1 times

 **francescoc** 8 months, 1 week ago

**Selected Answer: D**

Correct Answer D  
Leaked credentials: This risk detection type indicates that the user's valid credentials have been leaked. When cybercriminals compromise valid

passwords of legitimate users, they often share those credentials. This sharing is typically done by posting publicly on the dark web, paste sites, or by trading and selling the credentials on the black market.

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

upvoted 1 times

 **Aquintero** 10 months, 1 week ago

**Selected Answer: D**

D. credenciales filtradas

upvoted 1 times

 **[Removed]** 11 months, 4 weeks ago

**Selected Answer: D**

Leaked credentials is the correct answer. The other options are sign-in risk.

upvoted 1 times

 **BTL\_Happy** 1 year ago

this came out with different multiple choice.

upvoted 1 times

 **Tokiki** 1 year, 5 months ago

D is correct

upvoted 1 times

 **dangerdizzy** 1 year, 5 months ago

**Selected Answer: D**

Leaked Credentials is the answer

upvoted 1 times

 **dangerdizzy** 1 year, 6 months ago

**Selected Answer: D**

Leaked Credentials

upvoted 1 times

 **Davidf** 1 year, 7 months ago

**Selected Answer: D**

Absolutely D

upvoted 1 times

 **PanBrown** 1 year, 7 months ago

Leaked Credentials is correct, consider credentials are always classified.

upvoted 1 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 1 times

You have a Microsoft 365 tenant.

All users have computers that run Windows 10. Most computers are company-owned and joined to Azure Active Directory (Azure AD). Some computers are user-owned and are only registered in Azure AD.

You need to prevent users who connect to Microsoft SharePoint Online on their user-owned computer from downloading or syncing files. Other users must NOT be restricted.

Which policy type should you create?

- A. a Microsoft Cloud App Security activity policy that has Microsoft Office 365 governance actions configured
- B. an Azure AD conditional access policy that has session controls configured**
- C. an Azure AD conditional access policy that has client apps conditions configured
- D. a Microsoft Cloud App Security app discovery policy that has governance actions configured

**Correct Answer: B**

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad>

*Community vote distribution*

B (73%) C (27%)

✉️  Val\_0 Highly Voted 2 years, 7 months ago

B is the correct answer imo - <https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices> - You need to use "Use app enforced restrictions" from the "Session" control of the CA

upvoted 34 times

✉️  melatocaroca 2 years, 5 months ago

Most computers are company-owned and joined to Azure Active Directory (Azure AD).

You need to prevent users who connect to Microsoft SharePoint Online on their user-owned computer

<https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use>  
<https://docs.microsoft.com/en-us/mem/intune/protect/app-based-conditional-access-intune-create>

upvoted 1 times

✉️  melatocaroca 2 years, 4 months ago

IMHO

After review this on a real tenant first you need to select SPO in Cloud apps or actions  
 that action will enable in session settings App enforced restrictions might require additional admin configurations within the cloud apps.  
 The restrictions will only take effect for new sessions.

So because first action is configure the application that will be affected by sessions settings, choosing C, instead B can be the option to select as demoxy told 2 months, 1 week ago C is the answer

upvoted 4 times

✉️  Beitrain Highly Voted 2 years, 6 months ago

So, first step is to create a Conditional Access Policy with Session configured in Azure AD, then create a Session Policy in Cloud App Security:  
<https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-blocking-data-downloads-via-microsoft-cloud-app/ba-p/326357>

So I'd say that since the first step is the Azure one the correct answer is B, since none of the other options for Cloud App Security make sense.  
 upvoted 12 times

✉️  Azurefox79 2 years, 5 months ago

Nope, for this question you need to first configured settings in SP and EXO admin centers which creates CA policies that enforce these. I just had a client project with this. Also, to do session controls for an app, first register it in AzAd, 2nd connect the app in CAS, 3rd create a session policy in CAS and lastly create a CA policy referencing session control policy in step 3.

upvoted 4 times

✉️  JerryGolais 2 years, 6 months ago

This is right. Link explains everything.

upvoted 2 times

✉️  haazybanj Most Recent 4 weeks ago

**Selected Answer: B**

The correct answer is B. an Azure AD conditional access policy that has session controls configured.

Azure AD conditional access policies allow you to control who can access your Azure AD resources and under what conditions. You can use conditional access policies to block users from downloading or syncing files from SharePoint Online on their user-owned computers.

upvoted 2 times

 **haazybanj** 1 month ago

**Selected Answer: B**

The answer is: B. an Azure AD conditional access policy that has session controls configured

Azure AD Conditional Access policies allow you to control user access to cloud apps based on conditions such as user identity, device state, and location. In this case, you can create a Conditional Access policy that prevents users from downloading or syncing files from SharePoint Online when they are using a user-owned device.

upvoted 1 times

 **ACSC** 2 months, 1 week ago

**Selected Answer: B**

You need to use "Use app enforced restrictions" from the "Session" control of the CA and then "Use conditional access App Control". After that configure Conditional Access App Control app.

upvoted 2 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: B**

Correct Answer is: B

upvoted 2 times

 **sehlohomoletsane** 4 months ago

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions>

upvoted 1 times

 **hellawaits111** 4 months ago

**Selected Answer: B**

B is the answer

<https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: C**

Correction

C. an Azure AD conditional access policy that has client apps conditions configured

upvoted 1 times

 **mali1969** 5 months, 2 weeks ago

Based on this information, the policy type that should be created is C. an Azure AD conditional access policy that has client apps conditions configured. This policy type allows you to control access to cloud apps based on specific conditions such as device platform and client app

upvoted 2 times

**Correct answer is an Azure AD conditional access policy that has session controls configured to prevent users who connect to SharePoint Online on their user-owned computer from downloading or syncing files. Session controls allow you to restrict access to content based on device state, such as whether it is company-owned or user-owned.**

upvoted 2 times

 **venumurki** 5 months, 3 weeks ago

C is the answer: <https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad>

upvoted 1 times

 **dule27** 6 months ago

**Selected Answer: B**

B. an Azure AD conditional access policy that has session controls configured

upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: B**

B correct

upvoted 1 times

 **jojoseph** 10 months, 2 weeks ago

**Selected Answer: B**

B or C could be right. But I am inclined to B

upvoted 1 times

 **Holii** 5 months, 4 weeks ago

You need to use session control because you need access to 'use app-enforced restrictions'.

Only via the SharePoint admin center can you edit that ability to sync files to OneDrive and SharePoint.

Settings -> Sync -> Allow syncing only on computer joined to specific domains

Questions asks to "Restrict download and sync"

upvoted 1 times

 **Halwagy** 10 months, 3 weeks ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>  
upvoted 1 times

 **shoutiv** 11 months, 2 weeks ago

**Selected Answer: B**

B

Source: <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-policy-app-enforced-restriction>

Block or limit access to SharePoint, OneDrive, and Exchange content from unmanaged devices:

...  
7. Under Access controls > Session, select "Use app enforced restrictions", then select "Select".

...

upvoted 2 times

 **syougun200x** 2 months, 3 weeks ago

Thanks. This and it seems the below also has to be configured on Sharedpoint.

<https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

Users on unmanaged devices will have browser-only access with no ability to download, print, or sync files. They also won't be able to access content through apps, including the Microsoft Office desktop apps.

upvoted 1 times

 **mcas** 11 months, 3 weeks ago

**Selected Answer: C**

This one should be C (CA policy configured with Client Apps) you can verify this by changing the SPO Policy -> Access Control -> Unmanaged devices -> Block, it automatically creates a CA policy in AAD with name in this format "[SharePoint admin center]Use app-enforced Restrictions for browser access - 2022/11/29" which has 1 condition on Client Apps and 1 condition on Device Platform. It does not create a CA policy with Session configured

upvoted 1 times

 **Holii** 5 months, 4 weeks ago

Yes, and you would have successfully locked everyone with an unmanaged device from accessing SPO.

The question is asking for people to not be able to download files, not block access entirely. Access policies are only for...access, it's in the name..

You can also specify in the policy "Grant > Require Hybrid Azure AD joined device", this would follow the same action that SPO is doing with its in-app controls.

This is a session policy; because only session policy has the ability to monitor/block downloading. "Session Policy -> Use Conditional Access Policy Control -> Block Downloads"

upvoted 1 times

 **Holii** 5 months, 4 weeks ago

I should add:- all "Client Apps Conditions" does is restrict what authentication types you can use to access the application:  
"Browser/Desktop/Mobile" or legacy authentication "Exchange/Other"

So it doesn't answer the blocking restriction either.

upvoted 1 times

You have an Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant.

The on-premises network contains a VPN server that authenticates to the on-premises Active Directory domain. The VPN server does NOT support Azure Multi-Factor Authentication (MFA).

You need to recommend a solution to provide Azure MFA for VPN connections.

What should you include in the recommendation?

- A. Azure AD Application Proxy
- B. an Azure AD Password Protection proxy
- C. Network Policy Server (NPS)**
- D. a pass-through authentication proxy

**Correct Answer: C**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension-vpn>

*Community vote distribution*

C (100%)

✉ **Official\_Fridaws** Highly Voted 2 years ago

Yes! C is indeed the correct answer.

NPS (Network Policy and Access Service) is like a middle man between the VPN client and Azure MFA. The NPS role is installed on a domain-joined server or the domain controller and is configured to authenticate and authorize RADIUS requests from the VPN client.

The VPN should be configured to use RADIUS authentication and point to the NPS server.

The MFA NPS extension is installed anywhere but the VPN server. When a user/VPN client attempts to authenticate, it sends a RADIUS request to the NPS server through the VPN which performs the primary authentication and then triggers the NPS Extension for secondary authentication.

upvoted 130 times

✉ **NickHSO** 1 year, 10 months ago

Upvote for additional knowledge! thank you

upvoted 10 times

✉ **Official\_Fridaws** Highly Voted 2 years ago

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension>

upvoted 5 times

✉ **haazybanj** Most Recent 4 weeks ago

**Selected Answer: C**

The correct answer is C. Network Policy Server (NPS).

Network Policy Server (NPS) is a server role that allows you to implement RADIUS authentication, authorization, and accounting. You can use NPS to integrate Azure MFA with your VPN server.

upvoted 1 times

✉ **EmnCours** 4 months, 2 weeks ago

**Selected Answer: C**

Correct Answer: C

upvoted 1 times

✉ **mali1969** 5 months, 2 weeks ago

To provide Azure MFA for VPN connections, you can integrate Azure MFA with existing on-premises network policy server (NPS) servers. You can also use Azure Multi-Factor Authentication Server (Azure MFA Server) to connect with various third-party VPN solutions

Based on this information, the solution that should be recommended is C. Network Policy Server (NPS). This is because it allows you to secure RADIUS client authentication by deploying either an on-premises based MFA solution or a cloud-based MFA solution

upvoted 2 times

✉ **dule27** 6 months ago

**Selected Answer: C**

C. Network Policy Server (NPS)

upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: C**

Correct C

upvoted 1 times

 **[Removed]** 11 months, 4 weeks ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **Zubairr13** 1 year, 4 months ago

On the exam, 7/23/2022.

upvoted 2 times

 **Tokiki** 1 year, 5 months ago

Yes, NPS is ~~needed~~

upvoted 1 times

 **shine98** 1 year, 5 months ago

On the exam - June 12, 2022

upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 1 times

 **Pravda** 1 year, 10 months ago

**Selected Answer: C**

On the exam 1/20/2022

upvoted 2 times

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant is configured to sync with an on-premises Active Directory domain. The domain contains the servers shown in the following table.

| Name    | Operating system    | Configuration     |
|---------|---------------------|-------------------|
| Server1 | Windows Server 2019 | Domain controller |
| Server2 | Windows Server 2016 | Domain controller |
| Server3 | Windows Server 2019 | Azure AD Connect  |

The domain controllers are prevented from communicating to the internet.

You implement Azure AD Password Protection on Server1 and Server2.

You deploy a new server named Server4 that runs Windows Server 2019.

You need to ensure that Azure AD Password Protection will continue to work if a single server fails.

What should you implement on Server4?

- A. Azure AD Connect
- B. Azure AD Application Proxy
- C. Password Change Notification Service (PCNS)
- D. the Azure AD Password Protection proxy service

**Correct Answer: D**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

Community vote distribution

D (90%) 10%

 **jhap** Highly Voted 2 years, 1 month ago

The AzureAD Password Protection proxy service initiates an outbound connection (Port 443) to Azure to pull the banned password list. The downloaded banned password list is pulled by the agent installed on DCs.

Given answer is correct.

upvoted 31 times

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

**Selected Answer: D**

Correct Answer: D

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

upvoted 1 times

 **mali1969** 5 months, 2 weeks ago

To ensure that Azure AD Password Protection will continue to work if a single server fails, you should implement D. the Azure AD Password Protection proxy service on Server4

upvoted 1 times

 **dule27** 6 months ago

**Selected Answer: D**

D. the Azure AD Password Protection proxy service

upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: D**

D correct

upvoted 1 times

 **Marian2023** 9 months, 1 week ago

**Selected Answer: A**

two Azure AD Password Protection proxy servers is enough to ensure availability - <https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

"What happens if my Azure AD Connect server goes offline?"

<https://www.ipswitch.com/blog/provide-high-availability-for-azure-ad-connect>

You already have two instance of Azure AD Password Protection on two different servers. There is no need to have third instance. But you can provide HA for Azure AD connect.

upvoted 1 times

**Aquintero** 10 months, 1 week ago

**Selected Answer: D**

D. el servicio de proxy de protección con contraseña de Azure AD

upvoted 2 times

**[Removed]** 11 months, 4 weeks ago

**Selected Answer: D**

The answer given is a correct answer. Azure AD Password Protection proxy service.

upvoted 2 times

**den5\_pepito83** 1 year ago

ON EXAM 14/11/2022

upvoted 3 times

**SangSang** 1 year ago

which one do you choose in your exam?

upvoted 1 times

**lmeet** 1 year, 2 months ago

on the exam 09222022, i answered the same. Passed the exam, btw.

upvoted 1 times

**Zubairr13** 1 year, 4 months ago

On the exam, 7/23/2022.

upvoted 1 times

**rachee** 1 year, 5 months ago

would the answer not be A. Azure AD Connect? there are 2 domain controllers both configured with Azure AD Password Protection. The question is to ensure Azure AD Password protection will continue if a "single" server fails. If one of the DCs fail, the other will still be available. There is only 1 Azure AD Connect server; I would think you would configure a HA Azure AD connect server. Bad question, because the password list is cached on the DCs and only a single server failure.

upvoted 1 times

**rachee** 1 year, 5 months ago

Reading the link where it says Azure AD Password Protection proxy for HA, I change the answer to D.

upvoted 3 times

**sapien45** 1 year, 5 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

Choose one or more servers to host the Azure AD Password Protection proxy service. The following considerations apply for the server(s):

The host machine must be joined to any domain in that forest

upvoted 2 times

**shine98** 1 year, 5 months ago

On the exam - June 12, 2022

upvoted 1 times

**Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022

upvoted 1 times

**Nilz76** 1 year, 8 months ago

Answer is D

The Azure AD Password Protection proxy service is typically installed on a member server in your on-premises AD DS environment. Once installed, the Azure AD Password Protection proxy service communicates with Azure AD to maintain a copy of the global and customer banned password lists for your Azure AD tenant.

You then install the Azure AD Password Protection DC agents on domain controllers in your on-premises AD DS environment. These DC agents communicate with the proxy service to get the latest banned password lists for use when processing password change events within the domain.

upvoted 3 times

**Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

## DRAG DROP -

You have a Microsoft 365 E5 tenant.

You purchase a cloud app named App1.

You need to enable real-time session-level monitoring of App1 by using Microsoft Cloud App Security.

In which order should you perform the actions? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

**Actions****Answer Area**

From Microsoft Cloud App Security, create a session policy.



Publish App1 in Azure Active Directory (Azure AD).

Create a conditional access policy that has session controls configured.

From Microsoft Cloud App Security, modify the Connected apps settings for App1.



Correct Answer:

**Actions****Answer Area**

Publish App1 in Azure Active Directory (Azure AD).



From Microsoft Cloud App Security, modify the Connected apps settings for App1.



From Microsoft Cloud App Security, create a session policy.



Create a conditional access policy that has session controls configured.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/proxy-deployment-any-app> <https://docs.microsoft.com/en-us/cloud-app-security/session-policy-aad>

JasonYin Highly Voted 2 years, 5 months ago

1. Publish App1.
2. Create a conditional access policy that has session controls configured.
3. From MCAS modify the Connected apps settings
4. From MCAS create a session policy

Reference - <https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-blocking-data-downloads-via-microsoft-cloud-app/ba-p/326357>

upvoted 79 times

jack987 11 months, 2 weeks ago

I agree with JasonYin. The correct answer is:

1. Publish App1.
2. Create a conditional access policy that has session controls configured.
3. From MCAS modify the Connected apps settings
4. From MCAS create a session policy

Reference - <https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-blocking-data-downloads-via-microsoft-cloud-app/ba-p/326357>

upvoted 1 times

Xyz\_40 1 year, 6 months ago

Correct... perfect

upvoted 2 times

Ed2learn 2 years, 5 months ago

From my reading - I think you have 3 and 4 reversed. The MCAS session policy is first created then the setting is modified. let me know if you think I am wrong.

upvoted 1 times

w00t 1 year, 2 months ago

Within MCAS, you need to click "Edit Settings" within the Connected App (App1), and check the checkbox for allowing "Session controlled policies" before you can actually create a Session controlled policy.

JasonYin posted the corrected steps.

upvoted 3 times

NawafAli 1 year, 10 months ago

based on testing, From modify the Connected apps settings will be before you can create a session policy in mcas.

upvoted 3 times

Ed2learn Highly Voted 2 years, 5 months ago

The given answer is wrong and I differ slightly from Jason below.

- 1) publish app
- 2) create a conditional access policy that has session controls - this begins the process for
- 3) From MCAS create a session policy
- 4) from MCAS modify the connected apps settings.

upvoted 31 times

melatocaroca 2 years, 5 months ago

Sorry after review you are right

upvoted 4 times

melatocaroca 2 years, 4 months ago

JasonYin order is the right one, if you go top down the menu of conditional policy,

Publish App1

Create a conditional access policy that has session controls configured

From Microsoft Cloud Application Security modify the connected apps settings for App1

From Microsoft Cloud Application Security create a session policy

upvoted 6 times

Xyz\_40 1 year, 6 months ago

CORRECT...

upvoted 2 times

w00t 1 year, 2 months ago

Ed2Learn - incorrect.

Steps 3 and 4 should be swapped. You CANNOT CREATE A SESSION POLICY IN MCAS for a specific app (App1) unless the app (App1) has its Connected Apps settings changed (Enable Session Controlled policy checkbox needs to be checked - this is not done by default)

upvoted 2 times

melatocaroca 2 years, 5 months ago

check jason link <https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-blocking-data-downloads-via-microsoft-cloud-app/ba-p/326357>

upvoted 1 times

Xyz\_40 1 year, 6 months ago

Nop, the last two should be interchanged.

upvoted 3 times

EmnCours Most Recent 3 months, 3 weeks ago

1. Publish App1
2. Create a conditional access policy that has session controls configured.
3. From MCAS modify the Connected apps settings
4. From MCAS create a session policy

upvoted 2 times

Heshan 4 months, 4 weeks ago

On the exam, 09/07/2023

upvoted 2 times

dule27 5 months ago

1. Publish App1.
2. Create a conditional access policy that has session controls configured.
3. From MCAS modify the Connected apps settings
4. From MCAS create a session policy

upvoted 1 times

AMZ 5 months, 1 week ago

Question valid - 06/23

upvoted 2 times

eleazar 7 months, 3 weeks ago

Publicar App1 en Azure Active Directory (Azure AD).

Desde Microsoft Cloud App Security, crear una política de sesión.

Crear una política de acceso condicional que tenga configurado el control de sesión.

Desde Microsoft Cloud App Security, modifique la configuración de aplicaciones conectadas para App1.

La publicación de App1 en Azure AD es el primer paso para habilitar la supervisión en tiempo real de la aplicación con Microsoft Cloud App Security. Luego, se debe crear una política de sesión en Microsoft Cloud App Security para la aplicación App1. Después, se debe crear una política de acceso condicional que tenga configurado el control de sesión. Finalmente, se debe modificar la configuración de aplicaciones conectadas para App1 en Microsoft Cloud App Security para habilitar la supervisión en tiempo real de la aplicación.

upvoted 2 times

fuzzilogic 9 months ago

I ask to chat GPT, and this is the correct answer:

1. Publish App1 in Azure Active Directory (Azure AD)
2. Create a conditional access policy that has session control configured
3. From Microsoft Cloud App Security, Create A session policy
4. From Microsoft Cloud App Security, modify the Connected apps settings for app1

upvoted 3 times

Arjanussie 9 months, 1 week ago

I agree with Jason

<https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-deployment-aad>

upvoted 1 times

[Removed] 11 months, 4 weeks ago

Explanation is correct: <https://www.examtopics.com/exams/microsoft/sc-300/view/11/#:~:text=The%20correct%20order%20is,allowing%20session%20controlled%20policies.>

upvoted 1 times

Faheem2020 1 year, 2 months ago

After creating conditional access policy with session control, you then go to Defender for Cloud Apps, select the app and use onboard with session control. After that you create session policy as per this article

<https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-deployment-any-app>

upvoted 1 times

samir45 1 year, 2 months ago

Correct answer:

- 1) Publish App
- 2) In Azure AD, create a conditional access policy that has session controls.
- 3) From MCAS, create a session policy
- 4) From MCAS, modify the connected apps settings.

upvoted 2 times

w00t 1 year, 2 months ago

The correct order is what JasonYin posted:

1. Publish App1.
2. Create a conditional access policy that has session controls configured.
3. From MCAS modify the Connected apps settings
4. From MCAS create a session policy

Everyone who is saying that Step 3 should be "Create a Session Policy" is wrong. When creating a Session policy for the specific application in question (App1), you won't be able to select App1 from the list of applications in this policy unless you FIRST "Modify the Connected Apps settings for App1", and select "Edit Settings" and check the checkbox for allowing session controlled policies.

upvoted 2 times

Zubairr13 1 year, 4 months ago

On the exam, 7/23/2022.

upvoted 2 times

shine98 1 year, 5 months ago

On the exam - June 12, 2022

upvoted 1 times

RandomNickname 1 year, 6 months ago

After looking into the video by VinoTee and Jason's link, 3, 4 should be create session pol for it to be generated, once it's generated modify from its base settings.

Unless I'm misunderstanding, but how can you modify something that you haven't already initially created?

Feel free to add your input but;

- 1:Publish App
- 2: Created conditional access pol with session control
- 3: Create session pol
- 4: Modify connected app settings

upvoted 2 times

Nilz76 1 year, 7 months ago

This question was in the exam 28/April/2022  
upvoted 1 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a notification through the Microsoft Authenticator app
- B. an app password
- C. Windows Hello for Business**
- D. SMS

**Correct Answer: C**

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.

Incorrect Answers:

A: A notification through the Microsoft Authenticator app requires connectivity to send the verification code to the device requesting the logon

B: An app password can be used to open an application but it cannot be used to sign in to a computer.

D: SMS requires a mobile phone -

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods> <https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview>

*Community vote distribution*

C (100%)

 **stromnessian** Highly Voted 1 year, 9 months ago

**Selected Answer: C**

If you think it's anything other than C, maybe you need to consider a career change.

upvoted 21 times

 **ServerBrain** 3 months, 1 week ago

yeah, it's never too late..

upvoted 2 times

 **DiscGolfer** 9 months, 2 weeks ago

I think answer is C - <https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-faq#is-windows-hello-for-business-considered-multi-factor-authentication>

upvoted 1 times

 **Melwin86** Highly Voted 2 years ago

Answer C is correct. Why everyone thinking that answer A is correct ?

upvoted 7 times

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

**Selected Answer: C**

C: Windows Hello for Business Overview:

Windows Hello for Business is a secure authentication method that uses biometrics or PINs to provide strong and convenient authentication to Windows devices.

The overview provides an introduction to Windows Hello for Business, its features, and its benefits.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: C**

C. Windows Hello for Business  
upvoted 1 times

**DasChi\_cken** 4 months ago

You dont have cellular Connection so SMS wont Work

An App passcode is Not a MFA at all, its just an on-top Security layer

As mentioned from Cepheid a Hotspot could be used but IT was never mentioned in the question. You cant tell If the Hotspot Feature is disabled by Policy...

Windows hello is the only correct answer, even if the Laptop does not have any biometrics sensor you can use a PIN

upvoted 1 times

**dule27** 6 months ago

**Selected Answer: C**

C. Windows Hello for Business  
upvoted 1 times

**ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: C**

C correct  
upvoted 1 times

**SusanGlenn5** 8 months, 2 weeks ago

I think it's A  
upvoted 1 times

**ra1paul** 9 months, 2 weeks ago

Definitely C.  
upvoted 1 times

**Cepheid** 11 months, 1 week ago

Technically speaking, the user can then use their laptop as a mobile hotspot for that wired connection and then connect their phone to wifi. Thus, the Authenticator App is also a possible solution. The question has poor wording, we don't know if this refers to the cloud or just signing in to the PC.

upvoted 1 times

**Passy** 11 months, 2 weeks ago

I think it's A though  
upvoted 1 times

**Rearalfonsina** 1 year, 4 months ago

Microsoft Authenticator  
Approve sign-ins from a mobile app using push notifications, biometrics, or one-time passcodes.

Windows Hello for Business

Replace your passwords with strong two-factor authentication (2FA) on Windows 10 devices. Use a credential tied to your device along with a PIN, a fingerprint, or facial recognition to protect your accounts.

upvoted 3 times

**subhuman** 1 year, 5 months ago

**Selected Answer: C**

The answer C is correct . The question states " The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity ". so there is no way a user would get a notification through Microsoft Authenticator App. Windows Hello for business is also considered an MFA authentication method for Azure AD registered and Joined devices

upvoted 5 times

**Rameshbetha** 1 year, 5 months ago

have in exam on June 21 2022.  
upvoted 1 times

**Benkyoujin** 1 year, 6 months ago

**Selected Answer: C**

C - hello for business. A mentions sending a notification vs. totp code. Hello for business is acceptable as MFA for aad registered devices - <https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-faq#how-does-windows-hello-for-business-work-with-azure-ad-registered-devices>, although I think the question should be more accurately worded.

upvoted 1 times

**Yelad** 1 year, 8 months ago

On the exam - March 28, 2022  
upvoted 1 times

**Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.  
upvoted 2 times

 **Cloud\_apps** 1 year ago

what was your answer ?

upvoted 1 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

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 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Azure portal, you configure the Notifications settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

You need to configure the fraud alert settings.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

Community vote distribution

B (100%)

KB10 Highly Voted 2 years ago

No indeed | Referenced to <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#block-and-unblock-users-with-Fraud-alert>  
upvoted 5 times

syougun200x Most Recent 1 month, 3 weeks ago

To enable the alert function.

Azure Entre -> security -> MFA -> Fraud Alert

upvoted 1 times

EmnCours 3 months, 3 weeks ago

**Selected Answer: B**

You need to configure the fraud alert settings.

upvoted 2 times

mali1969 5 months, 2 weeks ago

You can configure fraud alert notifications in Azure Active Directory > Security > Multi-Factor Authentication > Notifications1. You can enter the email address to send the notification to and remove an existing email address by selecting "... next to the email address and then selecting Delete. You can also configure multi-factor authentication during a sign-in event to the Azure portal by selecting Conditional Access from the left navigation blade, then selecting Named location, and clicking on "Configure MFA trusted IPs" in the bar across the top of the Conditional Access | Named Locations window

upvoted 1 times

dule27 6 months ago

**Selected Answer: B**

B. No is the answer

upvoted 1 times

ShoaibPKDXB 6 months, 4 weeks ago

**Selected Answer: B**

Correct B. NO

upvoted 1 times

Aquintero 10 months, 1 week ago

**Selected Answer: B**

<https://learn.microsoft.com/es-es/azure/active-directory/authentication/howto-mfa-mfasettings#account-lockout>

upvoted 1 times

Zubairr13 1 year, 4 months ago

On the exam, 7/23/2022.

upvoted 1 times

 **DemekeAd** 1 year, 7 months ago

No.

to block user

Browse to Azure Active Directory > Security > MFA > Block/unblock users.

upvoted 2 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 1 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 1 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

 **lamjudeicon** 1 year, 11 months ago

Indeed No

upvoted 1 times

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

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

You have a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Azure portal, you configure the Account lockout settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

You need to configure the fraud alert settings.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

*Community vote distribution*

B (100%)

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: B**

B. No is the correct answer  
upvoted 1 times

 **dule27** 6 months ago

**Selected Answer: B**

B. No is the correct answer  
upvoted 1 times

 **jack987** 11 months, 2 weeks ago

The answer is correct - NO.

The account lockout settings are applied only when a PIN code is entered for the MFA prompt.

Fraud Alert:

The fraud alert feature lets users report fraudulent attempts to access their resources. When an unknown and suspicious MFA prompt is received, users can report the fraud attempt by using the Microsoft Authenticator app or through their phone.

The following fraud alert configuration options are available:

Automatically block users who report fraud. If a user reports fraud, the Azure AD Multi-Factor Authentication attempts for the user account are blocked for 90 days or until an administrator unblocks the account.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

upvoted 2 times

 **[Removed]** 11 months, 4 weeks ago

**Selected Answer: B**

Fraud Settings need to be configured, meaning this solution does not meet the goal.

upvoted 2 times

 **Zubairr13** 1 year, 4 months ago

On the exam, 7/23/2022.

upvoted 1 times

 **tqtuan1512** 1 year, 6 months ago

I think it should be B

upvoted 1 times

 **mzsfc3c** 1 year, 7 months ago

A: Fraud alert only enables the user to report fraud by pressing 0# (default), in account lockout you can configure automatic user lockout after # of MFA denials.

upvoted 3 times

 **Benkyoujin** 1 year, 6 months ago

This is incorrect, should be B. Fraud alert setting literally has an option to configure it to automatically block - <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert>  
o enable and configure fraud alerts, complete the following steps:

1. Go to Azure Active Directory > Security > MFA > Fraud alert.
2. Set Allow users to submit fraud alerts to On.
3. Configure the Automatically block users who report fraud or Code to report fraud during initial greeting setting as needed.
4. Select Save.

upvoted 6 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022

upvoted 1 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 1 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

 **KB10** 2 years ago

No indeed | Refferenced to <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#block-and-unblock-users-with-Fraud-alert>

upvoted 3 times

 **casti** 2 years, 1 month ago

Should Be A

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout>

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 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Azure portal, you configure the Block/unblock users settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

You need to configure the fraud alert settings.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

*Community vote distribution*

B (100%)

✉  **MORK2000** Highly Voted 2 years ago

go to MFA>settings>Fraud Alert>allow>autoblock>on>save  
upvoted 9 times

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

**Selected Answer: B**

You need to enable "Report suspicious activity".

To enable Report suspicious activity from the Authentication Methods Settings:

- 1- In the Azure portal, click Azure Active Directory > Security > Authentication Methods > Settings.
- 2- Set Report suspicious activity to Enabled.
- 3- Select All users or a specific group.

upvoted 1 times

✉  **hellawaits111** 4 months ago

This is incorrect. Documentation states "Reporting suspicious activity will set the user's risk to high. If the user is subject to risk-based Conditional Access policies, they MAY be blocked."

It is the Fraud Alert configuration that is required.

upvoted 1 times

✉  **dule27** 6 months ago

**Selected Answer: B**

B. No is the correct answer

upvoted 1 times

✉  **[Removed]** 11 months, 4 weeks ago

**Selected Answer: B**

Fraud Settings need to be configured, meaning this solution does not meet the goal.

upvoted 1 times

✉  **shoutiv** 12 months ago

**Selected Answer: B**

B - No

It should be Azure Active Directory > Security > Multifactor authentication > Fraud alert -> Allow users to submit fraud alerts to On

Pay attention to the words - you need to block the users AUTOMATICALLY

Explanation from MS docs:

FRAUD ALERT

The fraud alert feature lets users report fraudulent attempts to access their resources. When an unknown and suspicious MFA prompt is received, users can report the fraud attempt by using the Microsoft Authenticator app or through their phone.

The following fraud alert configuration options are available:

- Automatically block users who report fraud.
- Code to report fraud during initial greeting.

#### BLOCK AND UNBLOCK USERS

If a user's device is lost or stolen, you can block Azure AD Multi-Factor Authentication attempts for the associated account. Any Azure AD Multi-Factor Authentication attempts for blocked users are automatically denied. Users remain blocked for 90 days from the time that they're blocked.

upvoted 3 times

 **Joshuaau** 1 year ago

Is the given answer correct or incorrect? I would think the answer is A

upvoted 1 times

 **Zubairr13** 1 year, 4 months ago

On the exam 7/23/2022.

upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022

upvoted 1 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 2 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

 **KB10** 2 years ago

Should be Yes referenced to <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#block-and-unblock-users> with Fraud alert

upvoted 1 times

 **KB10** 2 years ago

Sorry my fault, answer is right

upvoted 2 times

**HOTSPOT -**

You have a Microsoft 365 tenant.

You need to identify users who have leaked credentials. The solution must meet the following requirements:

- Identify sign-ins by users who are suspected of having leaked credentials.
- Flag the sign-ins as a high-risk event.
- Immediately enforce a control to mitigate the risk, while still allowing the user to access applications.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

To classify leaked credentials as high-risk, use:

|                                                                        |
|------------------------------------------------------------------------|
| Azure Active Directory (Azure AD) Identity Protection                  |
| Azure Active Directory (Azure AD) Privileged Identity Management (PIM) |
| Identity Governance                                                    |
| Self-service password reset (SSPR)                                     |

To trigger remediation, use:

|                                             |
|---------------------------------------------|
| Client apps not using Modern authentication |
| Device state                                |
| Sign-in risk                                |
| User location                               |
| User risk                                   |

To mitigate the risk, select:

|                                                |
|------------------------------------------------|
| Apply app enforced restrictions                |
| Block access                                   |
| Grant access but require app protection policy |
| Grant access but require password change       |

**Correct Answer:****Answer Area**

To classify leaked credentials as high-risk, use:

|                                                                        |
|------------------------------------------------------------------------|
| Azure Active Directory (Azure AD) Identity Protection                  |
| Azure Active Directory (Azure AD) Privileged Identity Management (PIM) |
| Identity Governance                                                    |
| Self-service password reset (SSPR)                                     |

To trigger remediation, use:

|                                             |
|---------------------------------------------|
| Client apps not using Modern authentication |
| Device state                                |
| Sign-in risk                                |
| User location                               |
| User risk                                   |

To mitigate the risk, select:

|                                                |
|------------------------------------------------|
| Apply app enforced restrictions                |
| Block access                                   |
| Grant access but require app protection policy |
| Grant access but require password change       |

**Reference:**

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

✉  **abelchior**  2 years, 3 months ago

It's correct

upvoted 11 times

✉  **BaderJ**  2 years, 2 months ago

Passed the exam today 23/09/2021

This question came in the exam.

upvoted 7 times

□  **EmnCours** Most Recent ⓘ 4 months, 2 weeks ago

It's correct

upvoted 1 times

□  **Heshan** 4 months, 4 weeks ago

On the exam, 09/07/2023

upvoted 4 times

□  **dule27** 5 months ago

Azure AD Identity protection

User risk

Grant access but require password change

upvoted 1 times

□  **chriss1992** 11 months, 3 weeks ago

Answer is correct.

upvoted 1 times

□  **Zubairr13** 1 year, 4 months ago

On the exam, 7/23/2022.

upvoted 4 times

□  **rachee** 1 year, 5 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

upvoted 2 times

□  **Xyz\_40** 1 year, 6 months ago

correct.

upvoted 2 times

□  **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 2 times

□  **Bluediamond** 1 year, 9 months ago

this should be user risk not sign in risk. Leaked creds is user. <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

upvoted 5 times

□  **Bluediamond** 1 year, 9 months ago

NVM. It is right...read it wrong

upvoted 3 times

□  **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 2 times

## HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name  | Role                             |
|-------|----------------------------------|
| User1 | Conditional Access administrator |
| User2 | Authentication administrator     |
| User3 | Security administrator           |
| User4 | Security operator                |

You plan to implement Azure AD Identity Protection.

Which users can configure the user risk policy, and which users can view the risky users report? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Configure the user risk policy:

User3 only  
User3 and User4 only  
User1, User2, and User3 only  
User1, User3, and User4 only  
User1, User2, User3, and User4

View the risky users report:

User3 only  
User3 and User4 only  
User1, User2, and User3 only  
User1, User3, and User4 only  
User1, User2, User3, and User4

**Answer Area**

Configure the user risk policy:

User3 only  
User3 and User4 only  
User1, User2, and User3 only  
User1, User3, and User4 only  
User1, User2, User3, and User4

Correct Answer:

View the risky users report:

User3 only  
User3 and User4 only  
User1, User2, and User3 only  
User1, User3, and User4 only  
User1, User2, User3, and User4

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

oberte007 Highly Voted 2 years, 3 months ago

Given answers are not right. Users who can set up policies have the security or global admin role. According to given Link <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>, security operator can view all Identity Protection reports and Overview blade, Dismiss user risk, confirm safe sign-in and confirm compromise but can't Configure or change policies, and Configure alerts

So the first box should be User3 only because he is security admin and the second one User3 and User4.

upvoted 53 times

JckD4Ni3L 1 month, 1 week ago

Answers are right, it's already User3 for box 1 and User3 and User4 for Box 2... you must have seen an older version of this questions... (2 years ago I guess)

upvoted 4 times

 **jack987** 11 months, 2 weeks ago

I agree with oberte007.  
upvoted 1 times

 **rsamant** 1 year, 7 months ago

Correct. Tested and verified  
upvoted 2 times

 **Anju18** 2 years, 3 months ago

agree your point  
upvoted 2 times

 **007Ali** Highly Voted  1 year, 10 months ago

Configure user risk policy: User3 (Security Administrator)  
View the Risky Users Report: User3 and User4 (Security Administrator and Security Operator)

Conditional Access Administrator

- Does not have access to Identity Protection | User risk policy
- Does not have "Grants access to Risky Users Report"

Authentication Administrator

- Does not have access to Identity Protection | User risk policy
- Does not have "Grants access to Risky Users Report"

Security Administrator

- Has update access to Identity Protection | User risk policy

[microsoft.directory/identityProtection/allProperties/update](https://microsoft.directory/identityProtection/allProperties/update) = Update all resources in Azure AD Identity Protection

- Grants access to Risky Users Report

Security Operator

- Has only read access to Identity Protection | User risk policy

[microsoft.directory/identityProtection/allProperties/allTasks](https://microsoft.directory/identityProtection/allProperties/allTasks) = Create and delete all resources, and read and update standard properties in Azure AD Identity Protection

- Grants access to Risky Users Report

upvoted 32 times

 **dule27** Most Recent  6 months ago

Configure the user risk policy: User 3 only  
View the risky users report: User 3 and User 4 only  
upvoted 2 times

 **LeTrinh** 9 months, 2 weeks ago

It is correct, See the link: <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>  
upvoted 2 times

 **Aquintero** 10 months, 1 week ago

configurar la politica solo el Usuario 3 y luego 3 y 4.  
upvoted 2 times

 **[Removed]** 11 months, 4 weeks ago

Oberte is correct User 3 and then 3 and 4.  
upvoted 2 times

 **Zubairr13** 1 year, 4 months ago

On the exam, 7/23/2022.  
upvoted 3 times

 **Silent\_Muzinde** 1 year, 8 months ago

Sec admin can configure and view all reports but cannot reset passwords

Sec operate - can view reports but cannot change policies or reset passwords  
upvoted 3 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.  
upvoted 1 times

 **stromnessian** 1 year, 9 months ago

Tested to confirm:  
Configure: User 3 only  
Read report: Users 3 and 4  
upvoted 6 times

 **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022  
upvoted 2 times

 **GPerez73** 1 year, 9 months ago

First box: User3 // Second box: User3 and User4

Tested!

upvoted 4 times

 **KennethYY** 1 year, 10 months ago

Configure policy:User3 (Security Administrator)

View : tried granted Eligible Security Operator cannot see the security blade, but if change to active, it can see Security Blade and see the report  
upvoted 1 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

 **NawafAli** 1 year, 11 months ago

Tested in Lab, correct answer is -

Configure the user risk policy - user3

View the risky users report - user3 & user4

upvoted 9 times

 **goonerraka6** 1 year, 11 months ago

Security Operator - All permissions of the Security Reader role

Additionally, the ability to perform all Identity Protection Center operations except for resetting passwords and configuring alert e-mails.

Security Reader - Users with this role have global read-only access on security-related feature, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in Office 365 Security & Compliance Center

1. User3

2. User3 and User4

upvoted 2 times

 **Javed8008** 2 years ago

Configure: User 3 only

View Reports: User 3 and User 4 only

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

upvoted 7 times

**HOTSPOT -**

You have an Azure Active Directory (Azure AD) tenant that contains a group named Group3 and an administrative unit named Department1. Department1 has the users shown in the Users exhibit. (Click the Users tab.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

### Department1 Administrative Unit | Users (Preview)

ContosoAzureAD - Azure Active Directory

+ Add member Remove member Bulk operations Refresh Columns Preview features Got feedback?

This page includes previews available for your evaluation. View previews →

Search users Add filters

2 users found

| Name                              | User principal name               | User type | Directory synced |
|-----------------------------------|-----------------------------------|-----------|------------------|
| <input type="checkbox"/> US User1 | User1@m365x629615.onmicrosoft.com | Member    | No               |
| <input type="checkbox"/> US User2 | User2@m365x629615.onmicrosoft.com | Member    | No               |

Department1 has the groups shown in the Groups exhibit. (Click the Groups tab.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

### Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

+ Add Remove Refresh Columns Preview features Got feedback?

Search groups Add filters

| Name                               | Group Type | Membership Type |
|------------------------------------|------------|-----------------|
| <input type="checkbox"/> GR Group1 | Security   | Assigned        |
| <input type="checkbox"/> GR Group2 | Security   | Assigned        |

Department1 has the user administrator assignments shown in the Assignments exhibit. (Click the Assignments tab.)

Dashboard > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

### User Administrator | Assignments

Privileged Identity Management | Azure AD roles

+ Add assignments Settings Refresh Export Got feedback?

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

| Name                | Principal name                     | Type | Scope                                                 |
|---------------------|------------------------------------|------|-------------------------------------------------------|
| User Administration |                                    |      |                                                       |
| Admin1              | Admin1@m365x629615.onmicrosoft.com | User | Department1 Administrative Unit (Administrative unit) |
| Admin2              | Admin2@m365x629615.onmicrosoft.com | User | Directory                                             |

The members of Group2 are shown in the Group2 exhibit. (Click the Group2 tab.)

Dashboard > ContosoAzureAD > Groups > Group2

### Group2 | Members

Group

+ Add members Remove Refresh Bulk operations Columns Preview features Got feedback?

This page includes previews available for your evaluation. View previews →

Direct members

| Name                              | User type |
|-----------------------------------|-----------|
| <input type="checkbox"/> US User3 | Member    |
| <input type="checkbox"/> US User4 | Member    |

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

| Statements                                         | Yes                   | No                    |
|----------------------------------------------------|-----------------------|-----------------------|
| Admin1 can reset the passwords of User3 and User4. | <input type="radio"/> | <input type="radio"/> |
| Admin1 can add User1 to Group 2                    | <input type="radio"/> | <input type="radio"/> |
| Admin 2 can reset the password of User1.           | <input type="radio"/> | <input type="radio"/> |

Correct Answer:

## Answer Area

| Statements                                         | Yes                              | No                               |
|----------------------------------------------------|----------------------------------|----------------------------------|
| Admin1 can reset the passwords of User3 and User4. | <input type="radio"/>            | <input checked="" type="radio"/> |
| Admin1 can add User1 to Group 2                    | <input type="radio"/>            | <input checked="" type="radio"/> |
| Admin 2 can reset the password of User1.           | <input checked="" type="radio"/> | <input type="radio"/>            |

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units>

Beitran Highly Voted 2 years, 7 months ago

So the correct answer is No, Yes, Yes  
upvoted 94 times

jack987 11 months, 2 weeks ago

I agree with Beitran.  
The correct answer is No, Yes, Yes.

Here are some of the constraints for administrative units:  
Administrative units can't be nested.

<https://learn.microsoft.com/en-gb/azure/active-directory/roles/administrative-units>  
upvoted 6 times

NawafAli 1 year, 11 months ago

Correct answer, tested in lab.  
upvoted 2 times

xDinoKoalax 1 year, 9 months ago

Tested in lab on Mar.06, 2022, the answer is NO, YES, YES  
upvoted 8 times

GlenRMag16 1 year, 10 months ago

Tested in my lab as well. Just make sure that Admin1 has no role assigned in M365 Admin Center, so that scope only shows Department 1 Admin Unit.  
upvoted 2 times

 **googie\_egg**  2 years, 3 months ago

Tested in my own lab. No, Yes, Yes is correct.  
upvoted 12 times

 **Nivos23**  1 month ago

the correct answer is No, Yes, Yes  
upvoted 2 times

 **Nyamnyam** 4 weeks ago

NO, YES, YES!  
Why don't the Examtopics contributors ever update the info?  
upvoted 1 times

 **joe9527** 2 months ago

notice that group 2 is not in the administrative units: department1. so, no no yes is correct.  
upvoted 1 times

 **joe9527** 1 month, 3 weeks ago

there are two groups named group 2, first group 2 is in the department1 administrative units, second group which where user 3 is located in is not part of the administrative unit.  
upvoted 1 times

 **joe9527** 1 month, 3 weeks ago

nvm. I'm making a fool of myself lol.  
upvoted 1 times

 **EmnCours** 4 months, 2 weeks ago

The correct answer is No, Yes, Yes.  
<https://learn.microsoft.com/en-gb/azure/active-directory/roles/administrative-units>  
upvoted 2 times

 **Heshan** 4 months, 4 weeks ago

On the exam, 09/07/2023  
upvoted 2 times

 **Sango** 5 months ago

N, Y, Y. 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 (unless those users and devices are separately added as members of the administrative unit). Only Users 1 and 2 are directly added in the AU.  
upvoted 2 times

 **AMZ** 5 months, 1 week ago

Question valid - 06/23  
upvoted 2 times

 **dule27** 6 months ago

NO  
YES  
YES  
upvoted 1 times

 **HelloItsSam** 9 months, 3 weeks ago

I would say Yes, Yes, Yes  
<https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad/password-reset-an-example-of-how-you-can-use-administrative/m-p/2562069>  
Ultimately admin 1 can goto URL on: mystaff.microsoft.com and reset the password  
upvoted 1 times

 **Aquintero** 10 months, 1 week ago

Para mi la respuesta es No, No, Si; Admin1 es administrador de la unidad administrativa Department1, entonces el Grupo2 y el usuario1 pertenecen a la unidad administrativa de donde pertenece el administrador de AU Department1. que alguien me corrija si me equivoco pero el administrador de usuario de la unidad administrativa deberia gestionar los grupos y los usuarios de la AU  
upvoted 1 times

 **Halwagy** 10 months, 3 weeks ago

the correct answer is No, Yes, Yes  
<https://learn.microsoft.com/en-us/azure/active-directory/roles/administrative-units>  
upvoted 1 times

 **Jhill777** 1 year ago

No, Yes, Yes. Confirmed in lab.  
upvoted 2 times

 **Jhill777** 1 year ago

Correction: No, Yes, Yes. Confirmed in lab because that's the only time you'd see something this idiotic and difficult.  
upvoted 8 times

 **DeepMoon** 1 year, 2 months ago

Only contention every has is about  
#2.

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  
(unless those users and devices are separately added as members of the administrative unit)  
User 1 is separately added.  
<https://learn.microsoft.com/en-us/azure/active-directory/roles/administrative-units#groups>

That means #2 is Yes.

upvoted 3 times

 **Hot\_156** 1 year, 2 months ago

If you think this is No, Yes, Yes, and you tested this on your lab. Test again!!!! If you have User Admin role for a specific AU, it doesn't give you rights to the membership of that group. I tested this and the provided answer is correct. Watch this video if you still have issues  
<https://www.youtube.com/watch?v=1-x86jJuK7c&list=PLIVtbbG169nGj4rfaMUQiKiBZNDlxoo0y&index=6&t=1s>

upvoted 1 times

 **Hot\_156** 1 year, 2 months ago

I wish I could delete messages... lol This is N, Y, Y...

upvoted 6 times

 **keanwegas** 7 months, 3 weeks ago

Respect coming back 2 weeks later to fix your response

upvoted 6 times

 **Ceuse** 1 year, 4 months ago

Q2 : In the Exam there was a group 3 outside of the Administrative Unit, which Admin1 wanted to add User 1 into

upvoted 1 times

 **Jhill777** 1 year ago

Reproduced this in case it comes up. Add members is greyed out.

upvoted 1 times

 **RandomNickname** 1 year, 6 months ago

#1: N

Because user 3,4 are nested and from G2

See below from:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units>

"A scoped role assignment doesn't apply to members of groups added to an administrative unit, unless the group members are directly added to the administrative unit. For more information, see Add members to an administrative unit."

#2: Y

User Admin have the following attributes

"microsoft.directory/groups/members/update"

Which can be confirmed;

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#user-administrator>

#3: Y, User1, is a direct member for the admin unit

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 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Azure portal, you configure the Fraud alert settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

B. No

**Correct Answer: A**

The fraud alert feature lets users report fraudulent attempts to access their resources. When an unknown and suspicious MFA prompt is received, users can report the fraud attempt using the Microsoft Authenticator app or through their phone.

The following fraud alert configuration options are available:

- ☞ Automatically block users who report fraud.
- ☞ Code to report fraud during initial greeting.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

*Community vote distribution*

A (100%)

✉  **lamjudeicon** Highly Voted 1 year, 11 months ago

Correct Answer A  
upvoted 5 times

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

**Selected Answer: A**  
Report suspicious activity, the updated MFA Fraud Alert feature  
upvoted 1 times

✉  **dule27** 6 months ago

**Selected Answer: A**  
A. Yes is the correct answer  
upvoted 1 times

✉  **Jhill777** 1 year ago

**Selected Answer: A**  
Correct answer is A.  
upvoted 1 times

✉  **samir45** 1 year, 2 months ago

**Selected Answer: A**  
Correct answer.  
upvoted 1 times

✉  **Zubairr13** 1 year, 4 months ago

On the exam, 7/23/2022.  
upvoted 1 times

✉  **mzsfc3c** 1 year, 7 months ago

B: The question is "You need to block the users automatically when they report an MFA request that they did not initiate" and Fraud alert will NOT automatically block users, it will allow user to report only!  
upvoted 1 times

✉  **Davidf** 1 year, 7 months ago

These are the settings in the console  
Allow users to submit fraud alerts  
On  
Off  
Automatically block users who report fraud  
On  
Off  
    upvoted 3 times

曰  **Benkyoujin** 1 year, 6 months ago  
You're wrong, just check in the portal.  
    upvoted 3 times

曰  **Yelad** 1 year, 8 months ago  
On the exam - March 28, 2022  
    upvoted 2 times

曰  **Dineshshri** 1 year, 9 months ago  
We've renamed Microsoft Cloud App Security. It's now called Microsoft Defender for Cloud Apps. This is in MS docs link.  
    upvoted 2 times

曰  **TonytheTiger** 1 year, 9 months ago  
On the exam today - March 4, 2022  
    upvoted 1 times

曰  **zmlapq99** 1 year, 10 months ago  
On exam few days ago.  
    upvoted 1 times

曰  **Pravda** 1 year, 10 months ago  
On the exam 1/20/2022  
    upvoted 1 times

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a notification through the Microsoft Authenticator app
- B. email
- C. security questions
- D. a verification code from the Microsoft Authenticator app**

**Correct Answer: D**

The Authenticator app can be used as a software token to generate an OATH verification code. After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface.

Incorrect Answers:

A: A notification through the Microsoft Authenticator app requires connectivity to send the verification code to the device requesting the logon.

B: An email requires network connectivity.

C: Security questions are not used as an authentication method but can be used during the self-service password reset (SSPR) process.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#verification-code-from-mobile-app>

*Community vote distribution*

D (100%)

✉ **Nilz76** Highly Voted 1 year, 7 months ago

**Selected Answer: D**

This question was in the exam 28/April/2022 (and yes, I passed).

I chose Option D - A verification code from the Microsoft Authenticator app

upvoted 6 times

✉ **DiscGolfer** 9 months, 2 weeks ago

I tested this by turning off Cellular and WiFi to my phone then used the one-time password code from the Microsoft Authenticator app on my phone and it worked, verification code from Microsoft Authenticator App is the correct answer

upvoted 1 times

✉ **RandomNickname** Highly Voted 1 year, 6 months ago

**Selected Answer: D**

B,C Aren't valid, neither is push notification due to no external access, so only valid choice is D.

However this is assuming they've already had previously downloaded, added, scanned the QR code and set MFA from a location the has WiFi/external access.

This question has cropped up repeatedly with different answers, and many discussions....

upvoted 5 times

✉ **DasChi\_cken** Most Recent 3 months, 2 weeks ago

**Selected Answer: D**

6 digit verification code is useable offline

upvoted 1 times

✉ **stev\_au** 4 months, 1 week ago

**Selected Answer: D**

- A. Requires Internet connectivity which the user does not have
- B. Requires internet connectivity which the user does not have
- C. Requires internet connectivity which the user does not have
- D. Does not require internet connectivity.**

upvoted 1 times

✉ **EmnCours** 4 months, 2 weeks ago

**Selected Answer: D**

D. a verification code from the Microsoft Authenticator app  
upvoted 1 times

 **dule27** 6 months ago

**Selected Answer: D**

D. a verification code from the Microsoft Authenticator app  
upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: D**

correct  
upvoted 1 times

 **VeIN** 11 months, 2 weeks ago

**Selected Answer: D**

Hope this will illustrate better if someone is confused:

<https://www.strath.ac.uk/professionalservices/is/cybersecurity/mfa/whatifidonthaveasignalorwi-ficonnectiononmyphone/>  
upvoted 2 times

 **Fcnet** 1 year, 1 month ago

the D solution is not valid, if there is no phone connectivity (you have to validate a code at laptop screen, well but where this code comes from ?) the laptop is connected but not the phone and the authenticator app can be installed only on mobile, you can't find it on the Windows (10-11) store.

Windows Hello should be the only solution, not D, the code from Authenticator is not a solution here.

<https://support.microsoft.com/en-us/account-billing/download-and-install-the-microsoft-authenticator-app-351498fc-850a-45da-b7b6-27e523b8702a>

Install the latest version of the Authenticator app, based on your operating system:

1 - Google Android. On your Android device, go to Google Play to download and install the Authenticator app.

2 - Apple iOS. On your Apple iOS device, go to the App Store to download and install the Authenticator app.

upvoted 1 times

 **Fcnet** 1 year, 1 month ago

oops my bad D solution is right as you can install the authenticator App from the windows store so you can validate the code, everything is fine :)

<https://www.microsoft.com/en-us/p/microsoft-authenticator/9nblggzmcj6?activetab=pivot:overviewtab>

upvoted 1 times

 **hieverybody** 11 months, 1 week ago

OS: Windows 10 Mobile version 14393.0 or higher, Windows 8 Mobile

No desktop versions.

upvoted 1 times

 **Fcnet** 1 year, 1 month ago

i've made a test, the authenticator app installed on windows 10 device redirect calls to mobile, so if you don't have connectivity to your phone the call to authenticator will fail (ans no code will be sent to your Windows 10 device)  
so Solution A or D is the same the authenticator call could not end,  
as far as i see only Windows Hello for business is a solution

upvoted 1 times

 **Fcnet** 1 year, 1 month ago

after test effectively you do not need any connections from your phone (no wifi or data) to get a code and validate it it works  
<https://support.microsoft.com/en-us/account-billing/common-questions-about-the-microsoft-authenticator-app-12d283d1-bcef-4875-9ae5-ac360e2945dd>

So answer D is correct

upvoted 2 times

 **w00t** 1 year, 2 months ago

Wouldn't Email be a valid option? If they are hardwired on their laptop and have internet connectivity at the time of MFA, email would be valid...

Technically would be B or D, kind of a dumb question.

upvoted 1 times

 **w00t** 1 year, 2 months ago

Disregard, i'm a dumb dumb. Of course, there is no "Email" Azure MFA option.

Answer is D

upvoted 1 times

**HOTSPOT -**

You have a Microsoft 365 tenant.

You create a named location named HighRiskCountries that contains a list of high-risk countries.

You need to limit the amount of time a user can stay authenticated when connecting from a high-risk country.

What should you configure in a conditional access policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Configure HighRiskCountries by using:

- A cloud app or action
- A condition
- A grant control
- A session control

Configure Sign-in frequency by using:

- A cloud app or action
- A condition
- A grant control
- A session control

**Answer Area**

Configure HighRiskCountries by using:

- A cloud app or action
- A condition
- A grant control
- A session control

Configure Sign-in frequency by using:

- A cloud app or action
- A condition
- A grant control
- A session control

Correct Answer:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition> <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>

 **Xyz\_40** Highly Voted 1 year, 6 months ago

This is correct. CONDITION-->named LOCATION.

SESSION-->SIGN-IN FREQUENCY

upvoted 11 times

 **JcKD4Ni3L** Most Recent 1 month, 1 week ago

Correct answers!

upvoted 2 times

 **EmnCours** 4 months, 2 weeks ago

This is correct.

CONDITION-->named LOCATION.

SESSION-->SIGN-IN FREQUENCY  
upvoted 1 times

□ **AMZ** 5 months, 1 week ago

Question valid - 06/23

upvoted 3 times

□ **dule27** 6 months ago

High Risk Countries : A condition  
Sign in frequency : A session control  
upvoted 2 times

□ **Aquintero** 10 months, 1 week ago

Correcto, primero la condición y después el control de sesión  
upvoted 2 times

□ **[Removed]** 11 months, 4 weeks ago

Given answers are correct.  
upvoted 2 times

□ **RandomNickname** 1 year, 6 months ago

Given answer correct  
upvoted 4 times

**HOTSPOT -**

A user named User1 attempts to sign in to the tenant by entering the following incorrect passwords:

- Pa55w0rd12
- Pa55w0rd12
- Pa55w0rd12
- Pa55w.rd12
- Pa55w.rd123
- Pa55w.rd123
- Pa55w.rd123
- Pa55word12
- Pa55word12
- Pa55word12
- Pa55w.rd12

You need to identify how many sign-in attempts were tracked for User1, and how User1 can unlock her account before the 300-second lockout duration expires.

What should identify? To answer, select the appropriate

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Tracked sign-in attempts:

|    |
|----|
| 4  |
| 5  |
| 10 |
| 11 |

Unlock by:

|                                                 |
|-------------------------------------------------|
| Clearing the browser cache                      |
| Signing in by using inPrivate browsing mode     |
| Performing a self-service password reset (SSPR) |

## Answer Area

Tracked sign-in attempts:

|    |
|----|
| 4  |
| 5  |
| 10 |
| 11 |

Correct Answer:

Unlock by:

|                                                 |
|-------------------------------------------------|
| Clearing the browser cache                      |
| Signing in by using inPrivate browsing mode     |
| Performing a self-service password reset (SSPR) |

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>

  Hot\_156  1 year, 1 month ago

I tested this, if you stick to the question about Track Sig-In Attempts and the information provided in the question, Azure AD logs will log 11 attempts!!!

You are assuming Smart lockout tracks, but there is nothing in the question related to this. If I have the same question in the exam, I will go with 11 as I tested it  
upvoted 11 times

✉ **dejo** Highly Voted 1 year, 1 month ago

I'm almost certain that 5 sign-in attempts were tracked, and the user got locked out because of that! For the same 3 passwords in a row, MS counts only 1!

"Smart lockout tracks the last three bad password hashes to avoid incrementing the lockout counter for the same password." -  
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout>

upvoted 10 times

✉ **Nyamnyam** Most Recent 4 weeks ago

OK, presuming the smart lockout reference is the source of truth here.  
As of today, the default lockout threshold is 10 attempts and the default lockout duration is 60 seconds.  
THIS is just to mention that 300 secs is not the current default anymore (might have been 2 years ago).  
ALSO be aware that the 'last three identical hashes'-principle is still valid, and the \*lockout counter\* is \*really\* 5, meaning that since the user was locked out, someone has changed the default threshold from 10 to 5 without MSFT being so polite to explicitly inform us examinees about this fact!  
BUT nevertheless, 11 attempts were \*tracked\*. Indeed. Read the reference again: "Smart lockout tracks the last three bad password hashes to avoid..." The stress here is on "tracks", and the question was "how many attempts were tracked".  
FINALLY: SSPR is quite a claim! It will only reset the lockout count to 0 seconds if the user selects the "I forgot my password" option.  
All in all - absolutely speculative scenario and solution statements. Just learn it by heart and don't mull over it.

upvoted 1 times

✉ **Nivos23** 1 month ago

Chet Gpt : After reviewing all the comments and considering the provided information and the specific focus of the question on "tracked sign-in attempts," it appears that the most accurate answer should be 11.

The logic behind this is that the Sign-In logs will track all 11 sign-in attempts, regardless of the Smart Lockout behavior, as long as they are attempted within the specified time frame.

So, the final answer is 11.

upvoted 1 times

✉ **Nivos23** 1 month ago

11  
SSPR  
upvoted 1 times

✉ **JckD4Ni3L** 1 month, 1 week ago

The key here is the 300s lockout value. This is the default value when Smart Lockout is turned on. It's a trick question to fool you into assuming it isn't turned on and give 11 as tracked count.

The correct answer is 5 count, and SSPR. □

upvoted 1 times

✉ **JckD4Ni3L** 1 month, 1 week ago

Oups meant 4, as smart lockout only tracks the last 3 password variation.

See : <https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-smart-lockout#how-smart-lockout-works>  
upvoted 1 times

✉ **EmnCours** 3 months, 3 weeks ago

11  
SSPR  
upvoted 3 times

✉ **dule27** 5 months ago

11  
SSPR  
upvoted 2 times

✉ **Holii** 5 months, 4 weeks ago

This is a stupid question.  
Tracked where? Conditional Sign-in audit logs get reported to Sign-In logs which will track 11 records, regardless of whether Smart Lockout is configured or not.

I get why everyone is saying 4, but the wording is just terrible.

upvoted 1 times

✉ **diego17** 8 months, 2 weeks ago

Ele quis dizer rastreio de tentativas de login, não quantas são consideradas para bloqueio, então a resposta correta é 11  
upvoted 1 times

✉ **ThotSlayer69** 10 months, 2 weeks ago

For Tracked sign-in attempts, it could be 4, 5, or 11

5: if it tracks the last 3 bad password hashes and doesn't count them if they are repeated

4: if it tracks the last 3 UNIQUE bad password hashes and doesn't count them

11: if by tracked, it is referring to tracked on Azure AD and not tracked on Smart lockout

Which is it? This question sucks

upvoted 3 times

✉ **wsrudmen** 10 months, 2 weeks ago

Good answer should be:

Tracked sign-in: 4

Unlock by: SSPR

Why 4?

"Smart lockout tracks the last three bad password hashes to avoid incrementing the lockout counter for the same password."

==> The last pwd was already provided. And then it's not five. Check the 3 last pwd

upvoted 1 times

✉ **BRoald** 10 months, 2 weeks ago

Your answer is wrong with the tracked sign ins:

I tested this in my tenant with User1 & User2;

I tried to login with all the passwords in the order that's described in the question.

Then I went to Portal.azure > AAD > Users > User 1 & User 2 > Sign-In Logs:

I got on both users exactly 11 sign-in loggings. Every wrong or correct authentication is logged into Azure.

Final answers:

Tracked sign-in: 11

Unlock by: SSPR

upvoted 10 times

✉ **TimophxMS700** 11 months, 2 weeks ago

Set the Lockout threshold, based on how many failed sign-ins are allowed on an account before its first lockout.

The default is 10 for Azure Public tenants and 3 for Azure US Government tenants.

Set the Lockout duration in seconds, to the length in seconds of each lockout.

The default is 60 seconds (one minute).

upvoted 1 times

✉ **[Removed]** 11 months, 4 weeks ago

The given answer is correct.

upvoted 2 times

✉ **Jhill777** 1 year ago

Welp, I hope this isn't on the test with this wording. Lockout threshold set to 10. Tested with user1@domain.com.

Put in all the passwords provided > Account NOT locked out

Put in completely DIFFERENT passwords and the 3rd one locked the account out.

So it would seem the correct answer would be 7 with the initial list of passwords provided. SMH MSFT.

upvoted 1 times

✉ **Jhill777** 1 year ago

P.S. All 14 sign-ins were tracked in Azure AD Sign-In Logs so I guess it depends what they mean by "Tracking".

upvoted 2 times

✉ **BB6919** 1 year ago

I am not sure why it's not 4. This is my understanding:

The tracking counter is 0 at the beginning.

For the first 3 entries: Pa55w0rd12, the counter will be 1.

For the fourth entry: Pa55w.rd12, the counter will be 2.

Now following three entries: Pa55w.rd123, the counter will be 3.

Since the Smart lockout tracks the last three bad password hashes it should only store hashes of these passwords at this point:

Pa55w0rd12, Pa55w.rd12, Pa55w.rd123

For the eighth entry: Pa55word12, the counter will be 4.

Now the stored password hashes should be Pa55w.rd12, Pa55w.rd123, Pa55word12.

For the following three entries the password hashes are already stored then why should it increment the counter one more time?

Please note counter is the number of attempts being tracked.

upvoted 5 times

✉  **Holii** 5 months, 4 weeks ago

because the question states nothing about Smart Lockout. This question doesn't even care about Smart Lockout. It's not asking "Will the account be locked out after xx logins?"

It's asking "How many are tracked"

Azure AD Sign-in logs will log all login activity; failure, success, smart lockout or not. 11 will be tracked. You all are getting way too caught up in Smart Lockout when it's not even specified in the question.

upvoted 1 times

✉  **faeem** 1 year ago

Perhaps view this article: <https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout>

How smart lockout works

By default, smart lockout locks the account from sign-in attempts for one minute after 10 failed attempts for Azure Public and Azure China 21Vianet tenants and 3 for Azure US Government tenants. The account locks again after each subsequent failed sign-in attempt, for one minute at first and longer in subsequent attempts. To minimize the ways an attacker could work around this behavior, we don't disclose the rate at which the lockout period grows over additional unsuccessful sign-in attempts.

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 won't cause the account to lock out.

based on the above and the hashes, 5 would be correct answer for "tracked sign-in attempts".

upvoted 2 times

店铺：专业认证88

店铺：专业认证88

**HOTSPOT -**

You have an Azure Active Directory (Azure AD) tenant that has Security defaults disabled.

You are creating a conditional access policy as shown in the following exhibit.

**New**

## Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

**Name \***

Policy1

## Assignments

Users and groups (i)

Specific users included

Cloud apps or actions (i)

All cloud apps

Conditions (i)

0 conditions selected

## Access controls

Grant (i)

0 controls selected

Session (i)

0 controls selected

## Enable policy

Report-only

On

Off

**Create**

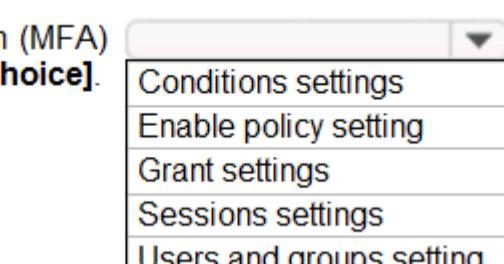
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

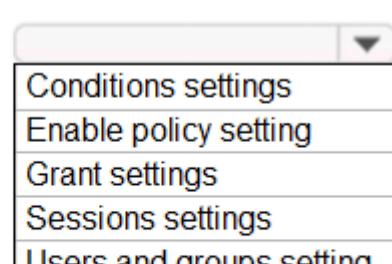
Hot Area:

**Answer Area**

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the **[answer choice]**.



To ensure that User1 is prompted for authentication every eight hours, you must configure the **[answer choice]**.



## Answer Area

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the [answer choice].

|                          |
|--------------------------|
| Conditions settings      |
| Enable policy setting    |
| Grant settings           |
| Sessions settings        |
| Users and groups setting |

Correct Answer:

To ensure that User1 is prompted for authentication every eight hours, you must configure the [answer choice].

|                          |
|--------------------------|
| Conditions settings      |
| Enable policy setting    |
| Grant settings           |
| Sessions settings        |
| Users and groups setting |

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa>

✉ **melatocaroca** Highly Voted 2 years, 5 months ago

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions>

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#sign-in-frequency>

Create a Conditional Access policy

1. Under Access controls > Grant, select Grant access, Require multi-factor authentication, and select Select.

2. Confirm your settings and set Enable policy to On.

3. Select Create to enable your policy.

Sign-in frequency

Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.

upvoted 33 times

✉ **sergioandreslq** 1 year, 5 months ago

Perfect answer and very well explained.

upvoted 2 times

✉ **Sugarrose** 2 years, 3 months ago

Hi friend, do you have exam dump for sc-300 ?

upvoted 1 times

✉ **jimmyjose** 2 months, 2 weeks ago

Hahahahaha

upvoted 1 times

✉ **MajorUrs** Highly Voted 2 years, 6 months ago

Correct

upvoted 7 times

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

Correct

upvoted 2 times

✉ **dule27** 5 months, 2 weeks ago

Prompted for MFA: Grant settings

Prompted for authentication every 8 hours: Session settings

upvoted 3 times

✉ **[Removed]** 11 months, 4 weeks ago

Answer given is correct.

upvoted 1 times

✉ **Imee** 1 year, 2 months ago

on the exam 09222022, i answered the same. Passed the exam, btw.

upvoted 3 times

✉ **Xyz\_40** 1 year, 6 months ago

Correct. This can easily be done in your Azure tenant

upvoted 1 times

✉ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 1 times

 **Nhurexjayyy** 1 year, 11 months ago

Correct.... <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime>

upvoted 2 times

You have an Azure Active Directory (Azure AD) tenant that contains a user named SecAdmin1. SecAdmin1 is assigned the Security administrator role.

SecAdmin1 reports that she cannot reset passwords from the Azure AD Identity Protection portal.

You need to ensure that SecAdmin1 can manage passwords and invalidate sessions on behalf of non-administrative users. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

- A. Authentication administrator
- B. Helpdesk administrator**
- C. Privileged authentication administrator
- D. Security operator

**Correct Answer: C**

Reference:

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

Community vote distribution

|         |         |    |
|---------|---------|----|
| B (75%) | A (21%) | 4% |
|---------|---------|----|

✉️  **sezza\_blunt** Highly Voted 2 years, 5 months ago

Answer must be B - Helpdesk Administrators.

From the docs:

Authentication administrator: can reset passwords for non-admins but can't invalidate sessions. <https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#authentication-administrator>

Helpdesk administrator: Users with this role can change passwords, invalidate refresh tokens, manage service requests, and monitor service health. Invalidating a refresh token forces the user to sign in again. <https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#helpdesk-administrator>

Privileged Authentication Administrator: can reset all passwords (admins & non-admins) but can't invalidate any sessions. <https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-authentication-administrator>

Security Operator: can't reset any passwords. <https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-operator>

upvoted 69 times

✉️  **Jhill777** 1 year ago

Authentication Administrator Role Permissions includes:

`microsoft.directory/users/invalidateAllRefreshTokens`

Force sign-out by invalidating user refresh tokens.

upvoted 4 times

✉️  **Domza** 2 years, 5 months ago

There you go - Help Desk Admin - "Users with this role can change passwords, invalidate refresh tokens"

upvoted 5 times

✉️  **[Removed]** 1 year, 9 months ago

I think it's B too. Helpdesk Administrator seems to be the correct answer.

upvoted 4 times

✉️  **rozgonyi** Highly Voted 2 years, 7 months ago

Tl;dr: A

In details:

Privileged Auth Admin can reset passwords of non admins and admin accounts

Helpdesk Admins can reset non admins and Helpdesk Admins password

Authentication Administrator can only reset non admin accounts password

To follow the least privilege requirement, Authentication Administrator should be the answer

upvoted 64 times

✉️  **med4** 2 years, 1 month ago

not sure why this answer is top voted - auth admin can manage MFA settings which high prev - help desk admin can just manage passwords and invalidated them ( invalidated refresh token)

upvoted 26 times

 **Holii** 5 months, 4 weeks ago

Agreed. Helpdesk Administrator can do explicitly what the question asks.  
Authentication Administrator has additional sensitive controls, such as revoking MFA or forcing users to re-register against non-password authentication methods (FIDO/MFA)  
upvoted 3 times

 **Acbrownit** 1 year, 7 months ago

Definitely A - For non-admin users, permissions needed are Reset Passwords for Non-Admins and Invalidate Refresh Tokens. Both exist in Authentication Administrator role. Privileged would allow access to Admin users.  
upvoted 2 times

 **Nyamnyam** Most Recent 4 weeks ago

**Selected Answer: B**

"manage passwords"-term has only one match by Password Administrator, and the referenced action is microsoft.directory/users/password/update, which is to "Reset the password". This action is assigned to Helpdesk Administrator as well. On the other side, Password Administrator cannot "invalidate sessions". Hmm, this term has no matches, but "invalidate" points to microsoft.directory/users/invalidateAllRefreshTokens, which is the correct action we look for. And guess what - this action is assigned to Helpdesk Administrator again.

upvoted 1 times

 **haazybanj** 4 weeks ago

**Selected Answer: B**

The best answer is B. Helpdesk administrator.

The Helpdesk administrator role allows users to reset passwords, invalidate refresh tokens, manage service requests, and monitor service health. This role is a good choice for SecAdmin1 because it allows her to manage passwords and invalidate sessions on behalf of non-administrative users, without giving her the full permissions of a Security administrator.

upvoted 1 times

 **haazybanj** 1 month ago

**Selected Answer: C**

The answer is: B. Helpdesk administrator

The Helpdesk administrator role allows users to reset passwords and invalidate sessions on behalf of non-administrative users. It also allows users to manage authentication methods and multi-factor authentication settings for non-administrative users.

upvoted 1 times

 **haazybanj** 4 weeks ago

The best answer is B. Helpdesk administrator.

The Helpdesk administrator role allows users to reset passwords, invalidate refresh tokens, manage service requests, and monitor service health. This role is a good choice for SecAdmin1 because it allows her to manage passwords and invalidate sessions on behalf of non-administrative users, without giving her the full permissions of a Security administrator.

upvoted 1 times

 **Nivos23** 1 month ago

**Selected Answer: B**

I think it's B

upvoted 1 times

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: B**

In Azure AD, the principle of least privilege is essential for security. To ensure that SecAdmin1 can manage passwords and invalidate sessions for non-administrative users without granting excessive permissions, you should assign the B: "Helpdesk administrator" role.

Assigning the "Authentication administrator" or "Privileged authentication administrator" roles might provide more privileges than necessary for SecAdmin1's requirements.

upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: A**

A. Authentication administrator

upvoted 1 times

 **Sango** 5 months ago

A. The key here is non-admin accounts. Only the Auth Admin meets the criteria.

Auth Admin: Can access to view, set and reset authentication method information for any non-admin user.

Helpdesk Admin: Can reset passwords for non-administrators and Helpdesk Administrators.

Priv Admin: Can access to view, set and reset authentication method information for any user (admin or non-admin).

Security Operator: Creates and manages security events.

upvoted 2 times

 **Garito** 5 months, 1 week ago

**Selected Answer: B**

Answered correctly in similar question.

upvoted 1 times

 **mali1969** 5 months, 2 weeks ago

You should assign the Privileged authentication administrator role to SecAdmin1. This role allows the user to manage passwords and invalidate sessions on behalf of non-administrative users while using the principle of least privilege

upvoted 1 times

 **dule27** 5 months, 3 weeks ago

**Selected Answer: B**

B. Helpdesk administrator

Authentication Administrator has additional sensitive controls

upvoted 1 times

 **dule27** 5 months ago

Correction:

A. Authentication administrator

Auth admin can only reset non admin accounts password

Helpdesk admin can reset non admins and Helpdesk Admins password

upvoted 1 times

 **OK2020** 6 months, 1 week ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords>

least priv is "helpdesk"

upvoted 3 times

 **haskelatchi** 6 months, 3 weeks ago

**Selected Answer: B**

The answer is B

upvoted 1 times

 **sysmaster01** 6 months, 3 weeks ago

ChatGPT's answer is:

"The appropriate role to assign to SecAdmin1 to manage passwords and invalidate sessions on behalf of non-administrative users is the Privileged authentication administrator role. This role allows SecAdmin1 to perform administrative tasks related to authentication, such as managing passwords, resetting user passwords, and invalidating user sessions, but without granting her full administrative privileges. The Privileged authentication administrator role is a limited administrator role in Azure AD that provides just enough access for performing administrative tasks without giving excessive access. The Authentication administrator role only allows SecAdmin1 to manage authentication methods for non-administrative users, while the Helpdesk administrator role allows her to reset passwords but not invalidate user sessions. The Security operator role is not related to managing passwords or invalidating sessions."

upvoted 1 times

 **AK\_1234** 1 month, 3 weeks ago

To ensure that SecAdmin1 can manage passwords and invalidate sessions on behalf of non-administrative users while following the principle of least privilege, you should assign the "Helpdesk administrator" role to SecAdmin1.

The "Helpdesk administrator" role is designed for scenarios where users need to perform tasks related to resetting passwords and managing user sessions without having full administrative access to Azure AD. It allows for password resets and session validations but doesn't grant excessive privileges that the user might not need for these specific tasks.

Option B: Helpdesk administrator is the most appropriate role for this scenario, as it aligns with the principle of least privilege, which means granting the minimum level of permissions necessary to perform the required tasks.

upvoted 1 times

 **fireweed** 5 months, 3 weeks ago

Lol imagine relying on ChatGPT. Have fun being wrong.

upvoted 2 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **Remus999** 7 months, 3 weeks ago

**Selected Answer: B**

B Helpdesk administrator makes sense as only non-administrative pw resets are required  
<https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#users>

C would only make sense if pw resets are required for admins as well

upvoted 2 times

店铺：专业认证88

店铺：专业认证88

You configure Azure Active Directory (Azure AD) Password Protection as shown in the exhibit. (Click the Exhibit tab.)

#### Custom smart lockout

**Lockout threshold** ⓘ

5



**Lockout duration in seconds** ⓘ

3600



#### Custom banned passwords

**Enforce custom list** ⓘ

Yes

No

**Custom banned password list** ⓘ

Contoso  
Litware  
Tailwind  
project  
Zettabyte  
MainStreet

#### Password protection for Windows Server Active Directory

**Enable password protection on Windows Server Active Directory** ⓘ

Yes

No

**Mode** ⓘ

Enforced

Audit

You are evaluating the following passwords:

- Ⓐ Pr0jectlitw@re
- Ⓑ T@ilw1nd
- Ⓒ C0nt0s0

Which passwords will be blocked?

- A. Pr0jectlitw@re and T@ilw1nd only
- B. C0nt0s0 only
- C. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd**
- D. C0nt0s0 and T@ilw1nd only
- E. C0nt0s0 and Pr0jectlitw@re only

#### Correct Answer: C

Reference:

<https://blog.enablingtechcorp.com/azure-ad-password-protection-password-evaluation>

Community vote distribution

C (85%)

D (15%)

✉ **arghhh** Highly Voted 2 years, 6 months ago

Test on tenant, all three are blocked.

Answer is C

upvoted 32 times

✉ **Goseu** Highly Voted 2 years, 6 months ago

After normalization we have :

- Ⓐ Pr0jectlitw@re -> projectlitware = 2 points
- Ⓑ T@ilw1nd -> tailwind = 1 point
- Ⓒ C0nt0s0 -> contoso = 1 point

You need 5 points therefore everything is blocked.

upvoted 13 times

✉ **Holii** 5 months, 4 weeks ago

(!) Not at all related, this is from my own internal playing around to understand the scoring system::

Funny how Tailw111nd is accepted with a banned word of "Tailwind".

I assume this is because: Tailw + l + l + l + nd = 5 points?

But then I tried a combination of appended strings: Tailw1nd + (strings)  
Tailw1ndadcb accepted (4+ characters had to be appended).  
I assume "Tailwind + a + d + c + b" = 5 points.

So is it 1 = L or 1 = i?  
And if it is 1 = L, how come Tailw1ndadcb didn't match similar to the previous?  
Tailw + l + nd + a + d + c + b

Microsoft has it specified as:  
Original letter Substituted letter  
0 o  
1 l (This is an L, not an i)  
\$ s  
@ a

There's no Microsoft examples for cases of 'special characters' being inserted mid-string in the banned character list. That's what sprung my suspicions. I'd love it if someone could link an article to support this.

upvoted 1 times

✉ Holii 5 months, 4 weeks ago

To add; this is definitely C. Not to misguide anyone with my curiosity lol.  
upvoted 1 times

✉ Holii 5 months, 4 weeks ago

After theoretical testing, I tried the following:  
Tailw%nd! - Password Accepted  
Tailwlnd! - Password Rejected  
Tailwgnd! - Password Accepted

This means that L must be nominalized to L = i = 1...

God this would've saved me a lot of time had Microsoft just included this in their docs.

so "Tailw111nd" = "Tailwi + i + i + n + d = 5 points.  
"Tailw1ndadcb" = "Tailwind + a + d + c + b" = 5 points  
"Tailw%nd!" = "Tailw + % + n + d + !" = 5 points  
"Tailwlnd!" = "Tailwind + !" = 2 points (This was rejected)  
"Tailwgnd!" = "Tailw + g + n + d + !" = 5 points

I can only assume it works off of substrings like this, as it's the only way that makes sense.

Last thing to test was to knock off the start of the substring character to see if it holds true:

"Tgilwind!" Password Accepted.  
"Failwind!" Password Accepted.

Use this as reference as you will...

upvoted 3 times

✉ poesklap [Most Recent] 6 days, 20 hours ago

**Selected Answer: C**

Answer is C

upvoted 1 times

✉ dule27 5 months ago

**Selected Answer: C**

C. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd

upvoted 1 times

✉ Aquintero 10 months, 1 week ago

**Selected Answer: C**

C. C0nt0s0, Pr0jectlitw@re y T@ilw1nd

upvoted 1 times

✉ [Removed] 11 months, 4 weeks ago

**Selected Answer: C**

All passwords will be blocked.

upvoted 1 times

✉ Jhill777 1 year ago

Tested on Tenant. First two are blocked because of the policy but C0nt0s0 states "We've seen that password too many times before. Choose something harder to guess." Also, if you were to try to reset it as an admin in the portal, it's too short.

upvoted 1 times

✉ reastman66 1 year ago

Correct answer C. I tested all 3 in my lab and they were all blocked. The first 2 are blocked based on policy but the last one is only 7 characters so it didn't meet the password minimum characters of 8.

upvoted 1 times

✉ kerimnl 1 year, 1 month ago

**Selected Answer: C**

Correct Answer is C

upvoted 1 times

 **gunjant25** 1 year, 2 months ago

normalization process occurs and multiple variants of a single character are normalized like:

@ - a

\$ - s

1 - i

so all three are going to be blocked because those words are already included in custom banned password list

upvoted 2 times

 **Ferrix** 1 year, 3 months ago

**Selected Answer: D**

Tested

upvoted 2 times

 **Tokiki** 1 year, 5 months ago

yes. it need 5 pts.

upvoted 2 times

 **Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022

upvoted 1 times

 **Nilz76** 1 year, 8 months ago

**Selected Answer: C**

Tested in my tenant, Answer is C

upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 1 times

 **stromnessian** 1 year, 9 months ago

**Selected Answer: C**

The answer is C. Can't understand why people can't just use "password" as it's much easier to remember.

upvoted 5 times

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a verification code from the Microsoft Authenticator app
- B. security questions
- C. voice
- D. SMS

**Correct Answer: A**

The Authenticator app can be used as a software token to generate an OATH verification code. After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface.

Incorrect Answers:

B: Security questions are not used as an authentication method but can be used during the self-service password reset (SSPR) process.

C, D: An automated voice call and an SMS requires mobile connectivity.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

*Community vote distribution*

|         |    |
|---------|----|
| A (95%) | 5% |
|---------|----|

✉  **bobicos** Highly Voted 2 years, 7 months ago

Security questions is not an option for MFA. Using the Authenticator app does not need network connectivity, thus the correct value upvoted 42 times

✉  **melatocaroca** 2 years, 5 months ago

WRONG do not have Wi-Fi access or mobile phone connectivity.  
upvoted 1 times

✉  **Cheif** 2 years, 7 months ago

But they don't have mobile phones? how will they access the mobile authenticator app?  
upvoted 1 times

✉  **tinhnd** 2 months, 2 weeks ago

Reading the requirements carefully is an essential skill to take the test. "All users have mobile phones & laptop". Which they don't have is Wi-fi and mobile connectivity.  
upvoted 1 times

✉  **Cheif** 2 years, 7 months ago

Scratch that A is the correct answer, doesn't need internet IMO  
upvoted 7 times

✉  **Ed2learn** 2 years, 5 months ago

doesn't need internet but the question states "no connectivity" which to me means no signal to receive. Not sure the right answer is here.  
upvoted 2 times

✉  **Ed2learn** 1 month ago

years later I understand the question. They do have connectivity to the internet. Its wired not wifi. P.S. don't forget to renew your certifications or you too will comment on your comment.  
upvoted 1 times

✉  **BO** 2 years, 6 months ago

but they do :) All users have mobile phones and laptops.  
upvoted 4 times

✉  **J4U** 2 years, 1 month ago

Yes, it Authenticator app don't need phone connectivty.

<https://support.microsoft.com/en-us/account-billing/common-problems-with-the-microsoft-authenticator-app-12d283d1-bcef-4875-9ae5-ac360e2945dd>  
upvoted 9 times

✉ **lime568** 1 year, 8 months ago

but need internet. no Wifi no mobile phone  
upvoted 1 times

✉ **tinhnd** 2 months, 2 weeks ago

All OTP apps or FIDO2 don't need internet connection to work.  
upvoted 1 times

✉ **Benkyoujin** 1 year, 6 months ago

Incorrect and you can test this.  
upvoted 1 times

✉ **BluMoon** 1 year, 5 months ago

Thanks for the link. This is correct, it specifically says that no data connection is needed under the heading "Verification codes when connected".  
upvoted 1 times

✉ **sezza\_blunt** 2 years, 5 months ago

The default behaviour of the Authenticator app is to send a notification to your phone, which does require mobile connectivity. However, the user can choose "Sign in another way" and then "Use a verification code from my mobile app" - this method does not require mobile connectivity. So yes, the correct answer is A "a verification code from the Microsoft Authenticator app"  
upvoted 18 times

✉ **melatocaroca** 2 years, 5 months ago

WRONG do not have Wi-Fi access or mobile phone connectivity.  
upvoted 2 times

✉ **ReffG** 1 year, 10 months ago

no it is correct. TOTP also works offline.  
upvoted 2 times

✉ **Acbrownit** 1 year, 7 months ago

The Authenticator app's verification codes are synced using an algorithm and seed that are shared between offline and the app, so the app will continue to generate valid numbers regardless of connectivity. The notification method requires connectivity, though. Voice is invalid, because it should be assigned to a land-line and even if assigned to a cell number, it wouldn't work without connectivity.  
upvoted 8 times

✉ **leeuw86** Highly Voted 2 years, 5 months ago

Had this question in exam today. Option C) voice was replaced by Windows Hello for Business.  
Also Option a) was notification from Authenticator App  
upvoted 18 times

✉ **sezza\_blunt** 2 years, 5 months ago

That changes it a bit. The notification requires mobile connectivity. Did you choose WHFB as the correct answer?  
upvoted 2 times

✉ **Ed2learn** 2 years, 5 months ago

Windows Hello solves the mobile phone connectivity issue. The biometric info is stored on the local machine so this will work. It doesn't require internet or mobile connectivity. Looks like Microsoft corrected the answer choices.  
upvoted 4 times

✉ **easypeacy** Most Recent 2 months, 1 week ago

maybe they are considering that you set the laptop as hotspot for your mobile and then use auth app ....  
upvoted 1 times

✉ **EmnCours** 4 months, 2 weeks ago

Selected Answer: A  
Correct Answer: A  
upvoted 1 times

✉ **dule27** 5 months ago

Selected Answer: A  
A. a verification code from the Microsoft Authenticator app  
upvoted 1 times

✉ **LeTrinh** 9 months, 2 weeks ago

<https://drake.teamdynamix.com/TDClient/2025/Portal/KB/ArticleDet?ID=50929>  
upvoted 2 times

✉ **[Removed]** 11 months, 4 weeks ago

Selected Answer: A

Correct answer.  
upvoted 2 times

 **PadyLoki** 1 year, 4 months ago

Answer would be A, since all users have a mobile and laptop, whilst they may not have mobile connectivity, they can still use the Authenticator App for a OTP  
upvoted 1 times

 **HenryVo** 1 year, 5 months ago

A is the correct answer. Authentication app no need Internet. We can change by input One-time Password Code in App auto random in 30s.  
upvoted 1 times

 **Tokiki** 1 year, 5 months ago

A is correct  
upvoted 1 times

 **sapien45** 1 year, 5 months ago

Verification codes when connected

Q: Do I need to be connected to the Internet or my network to get and use the verification codes?

A: The codes don't require you to be on the Internet or connected to data, so you don't need phone service to sign in. Additionally, because the app stops running as soon as you close it, it won't drain your battery.  
upvoted 1 times

 **shine98** 1 year, 5 months ago

On the exam - June 12, 2022  
upvoted 1 times

 **YetiSpaghetti** 1 year, 5 months ago

**Selected Answer: A**

A is obviously the answer. Voice needs mobile connectivity. MFA authenticators do not.

upvoted 1 times

 **RandomNickname** 1 year, 5 months ago

Voice doesn't necessarily need to be a mobile phone, and could be a landline, since the criteria required to enter on O365 is a phone number, irrespective of what type.  
This is something I've implemented before.  
upvoted 1 times

 **RandomNickname** 1 year, 6 months ago

Question needs more information since it can be both A or C.

See below for accepted MFA methods;

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

Reading the question, it could be C, since there is no "WIFI or mobile phone connectivity" to download the authenticator app to then be able to scan the QR code and register, so answer logically should be C, see comment from user "SnottyPudding".  
However if answer C has changed in the exam to "Windows Hello" this is likely correct, or if question area is reworded, referencing apps exist or some such similar rewording, answer could be A.

Essentially, be careful on test day and read carefully.

upvoted 1 times

 **jasonga** 1 year, 6 months ago

you can put your phone into airplane mode and test this A is correct you can still use the code,

upvoted 1 times

 **sunilkms** 1 year, 6 months ago

**Selected Answer: A**

the question says it clearly that no wifi access to mobile phone connectivity, hence, voice, and SMS is not an option, hence authenticator app is the correct option.

upvoted 1 times

 **Nilz76** 1 year, 7 months ago

This question was in the exam 28/April/2022

upvoted 1 times

**HOTSPOT -**

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name  | Role                                    |
|-------|-----------------------------------------|
| User1 | Security administrator                  |
| User2 | Privileged authentication administrator |
| User3 | Service support administrator           |

User2 reports that he can only configure multi-factor authentication (MFA) to use the Microsoft Authenticator app.

You need to ensure that User2 can configure alternate MFA methods.

Which configuration is required, and which user should perform the configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Configuration:

- Enable access reviews.
- Enable Azure AD Privileged Identity Management (PIM).
- Modify security defaults.

User:

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only
- User2 and User3 only

**Answer Area**

Configuration:

- Enable access reviews.
- Enable Azure AD Privileged Identity Management (PIM).
- Modify security defaults.

Correct Answer:

User:

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only
- User2 and User3 only

Box 1: Modify security defaults.

Privileged Authentication Administrator

Users with this role can set or reset any authentication method (including passwords) for any user, including Global Administrators.

Privileged Authentication

Administrators can force users to re-register against existing non-password credential (such as MFA or FIDO) and revoke 'remember MFA on the device', prompting for MFA on the next sign-in of all users.

The Authentication Administrator role has permission to force re-registration and multifactor authentication for standard users and users with some admin roles.

| Role                                    | Manage user's auth methods     | Manage per-user MFA            | Manage MFA settings | Manage auth method policy | Manage password protection policy |
|-----------------------------------------|--------------------------------|--------------------------------|---------------------|---------------------------|-----------------------------------|
| Authentication Administrator            | Yes for some users (see above) | Yes for some users (see above) | No                  | No                        | No                                |
| Privileged Authentication Administrator | Yes for all users              | Yes for all users              | No                  | No                        | No                                |
| Authentication Policy Administrator     | No                             | No                             | Yes                 | Yes                       | Yes                               |

Box 2: User1 only.

Security Administrator.

Users with this role have permissions to manage security-related features in the Microsoft 365 Defender portal, Azure Active Directory Identity Protection, Azure

Active Directory Authentication, Azure Information Protection, and Office 365 Security & Compliance Center.

Incorrect:

Not User3. Service Support Administrator.

Users with this role can create and manage support requests with Microsoft for Azure and Microsoft 365 services, and view the service dashboard and message center in the Azure portal and Microsoft 365 admin center.

Reference:

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

□  **Cepheid** Highly Voted 11 months, 1 week ago

The correct answer really is security defaults. PIM has nothing to do with it. When you disable security defaults, you can modify MFA settings.  
upvoted 7 times

□  **kanew** 7 months ago

Agree. Security Defaults is the only correct answer I can see. I haven't tested it but it makes sense and here is the statement from MS that I believe supports it . It suggests that the Authenticator App is the only enabled MFA option in Sec Defaults.

"Requiring all users and admins to register for MFA using the Microsoft Authenticator app or any third-party application using OATH TOTP."  
<https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-turn-on-mfa?view=o365-worldwide&tabs=secdefaults>

upvoted 1 times

□  **BB6919** 11 months ago

I agree with Cepheid. We don't need to modify anything within the Security default. Just need to disable it so that we can use Conditional access.

upvoted 1 times

□  **geobarou** Highly Voted 1 year, 2 months ago

Checked in SC300 MOC book. The answer is correct

upvoted 6 times

□  **vaaws** Most Recent 2 weeks, 3 days ago

Security Defaults  
User2

upvoted 1 times

□  **dule27** 5 months, 2 weeks ago

Modify security defaults  
User1 only  
upvoted 2 times

□  **ShoaibPKDXB** 6 months, 4 weeks ago

Correct  
upvoted 1 times

 **BB6919** 11 months ago

I agree with Cepheid. We don't need to modify anything within the Security default. Just need to disable it so that we can use Conditional access.  
upvoted 1 times

 **chrisp1992** 11 months, 3 weeks ago

Authentication Methods are handled in the Security Blade of Azure AD, not PIM. Seems strange, and I can't find anywhere in PIM to modify MFA methods.  
upvoted 1 times

 **[Removed]** 11 months, 4 weeks ago

Agree with DeepMoon. Security Defaults cannot be modified, it must be PIM. 2nd answer is correct.  
upvoted 1 times

 **ooltie** 1 year, 1 month ago

Correct. Security Defaults requires "Require all users to register for Azure AD Multi-Factor Authentication"

Users have 14 days to register for Azure AD Multi-Factor Authentication by using the Microsoft Authenticator app or any app supporting OATH TOTP.

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults#require-all-users-to-register-for-azure-ad-multi-factor-authentication>

upvoted 3 times

 **DeepMoon** 1 year, 2 months ago

I agree with the 2nd part of the answer. But I do question the first part.  
My assumption is the first part of this answer should be PIM.  
Security defaults turn on MFA. But I don't see a place where an admin gets to choose multiple methods. Unfortunately, I don't have P2 license to test this.

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant.

You configure self-service password reset (SSPR) by using the following settings:

- Require users to register when signing in: Yes
- Number of methods required to reset: 1

What is a valid authentication method available to users?

- A. a Microsoft Teams chat
- B. a mobile app notification
- C. a mobile app code**
- D. an FIDO2 security token

**Correct Answer: C**

When administrators require one method be used to reset a password, verification code is the only option available.

Note: When administrators require two methods be used to reset a password, users are able to use notification OR verification code in addition to any other enabled methods.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

*Community vote distribution*

C (100%)

**Leon1969** 2 months, 1 week ago

When administrators require one method be used to reset a password, verification code is the only option available  
upvoted 1 times

**sherifhamed** 2 months, 1 week ago

**Selected Answer: C**  
C. a mobile app code

In this configuration, users are required to register for SSPR and have at least one authentication method. A mobile app code is one of the available methods, which typically involves receiving a code on a mobile app that the user must enter to reset their password.

Options A and B (Microsoft Teams chat and mobile app notification) might be used for multi-factor authentication, but they are not typically used as standalone methods for password reset.

Option D (FIDO2 security token) is a strong authentication method but is not typically used for password reset; it's more commonly used for sign-in or multi-factor authentication.

upvoted 1 times

**EmnCours** 4 months, 2 weeks ago

**Selected Answer: C**  
Correct Answer: C  
upvoted 1 times

**dule27** 5 months, 3 weeks ago

**Selected Answer: C**  
C. a mobile app code  
upvoted 1 times

**ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: C**  
C is correct  
upvoted 1 times

**jojoseph** 10 months, 2 weeks ago

**Selected Answer: C**  
definitely C  
upvoted 1 times

**Boogs** 1 year, 2 months ago

**Selected Answer: C**  
confirmed. while there are other methods, if you set to 1 method, mobile app notification is greyed out and you can only choose app code

upvoted 3 times

□ **DeepMoon** 1 year, 2 months ago

The following authentication methods are available for SSPR:

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone (available only for tenants with paid subscriptions)
- Security questions

From <<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>>

upvoted 3 times

□ **CloudRat** 10 months, 3 weeks ago

Whilst what you are saying is correct if the Number of Methods required is set to 2. The methods available, when set to 1, is only the follow:

Mobile App Code

Email

Mobile Phone (SMS Only)

Security Questions

So, to confirm that the Question is answered Correct by choosing C. You need to deep dive into the settings when choosing 1 method or 2.

upvoted 2 times

You have an Azure Active Directory (Azure AD) tenant that uses Azure AD Identity Protection and contains the resources shown in the following table.

| Name  | Type             | Configuration                                                                     |
|-------|------------------|-----------------------------------------------------------------------------------|
| Risk1 | User risk policy | Users that have a high severity risk must reset their password upon next sign-in. |
| User1 | User             | Not applicable                                                                    |

Azure Multi-factor Authentication (MFA) is enabled for all users.

User1 triggers a medium severity alert that requires additional investigation.

You need to force User1 to reset his password the next time he signs in. The solution must minimize administrative effort.

What should you do?

- A. Reconfigure the user risk policy to trigger on medium or low severity.
- B. Mark User1 as compromised.
- C. Reset the Azure MFA registration for User1.
- D. Configure a sign-in risk policy.

#### Correct Answer: B

Scenario: User compromised (True positive)

'Risky users' report shows an at-risk user [Risk state = At risk] with low risk [Risk level = Low] and that user was indeed compromised.

Feedback: Select the user and click on 'Confirm user compromised'.

What happens under the hood? Azure AD will move the user risk to High [Risk state = Confirmed compromised; Risk level = High] and will add a new detection

'Admin confirmed user compromised'.

Notes: Currently, the 'Confirm user compromised' option is only available in 'Risky users' report.

The detection 'Admin confirmed user compromised' is shown in the tab 'Risk detections not linked to a sign-in' in the 'Risky users' report.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-risk-feedback>

#### Community vote distribution

B (92%) 8%

 **Buzz8** Highly Voted  1 year ago

#### Selected Answer: B

The question assists with the answer: "The solution must minimize administrative effort." So by selecting "user is compromised" in the alert will automatically prompt the user for a password reset on next logon. Less effort than reconfiguring a user risk policy.

upvoted 7 times

 **dule27** Most Recent  5 months, 3 weeks ago

#### Selected Answer: B

B. Mark User1 as compromised  
upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

#### Selected Answer: B

B is correct  
upvoted 1 times

 **kanew** 7 months ago

#### Selected Answer: B

Correct and less effort than A which will impact all users  
upvoted 1 times

 **Aquintero** 10 months, 1 week ago

#### Selected Answer: B

Teniendo en cuenta que hay que minimizar los esfuerzos administrativos la respuesta es: B. Marcar Usuario1 como comprometido.  
upvoted 1 times

 **Cepheid** 11 months, 1 week ago

Once you confirm a sign-in is compromised, Azure AD immediately increases the user's risk and sign-in's aggregate risk (not real-time risk) to High. If this user is included in your user risk policy to force High risk users to securely reset their passwords, the user will automatically remediate itself the next time they sign-in. <https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-risk-feedback>

upvoted 1 times

 [Removed] 11 months, 4 weeks ago

**Selected Answer: B**

Given answer is correct.

upvoted 1 times

 kerimn 1 year, 1 month ago

**Selected Answer: A**

I think the correct answer is A.

upvoted 1 times

**HOTSPOT -**

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name  | Member of      | Multi-factor authentication (MFA) |
|-------|----------------|-----------------------------------|
| User1 | Group1         | Enabled but never used            |
| User2 | Group2         | Disabled                          |
| User3 | Group1, Group2 | Enforced and used                 |

In Azure AD Identity Protection, you configure a user risk policy that has the following settings:

↳ Assignments:

- Users: Group1

- User risk: Low and above

↳ Controls:

- Access: Block access

↳ Enforce policy: On

In Azure AD Identify Protection, you configure a sign-in risk policy that has the following settings:

↳ Assignments:

- Users: Group2

- Sign-in risk: Low and above

↳ Controls:

- Access: Require multi-factor authentication

↳ Enforce 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.

Hot Area:

| Statements                                      | Yes                   | No                    |
|-------------------------------------------------|-----------------------|-----------------------|
| User1 can sign in from an anonymous IP address. | <input type="radio"/> | <input type="radio"/> |
| User2 can sign in from an anonymous IP address. | <input type="radio"/> | <input type="radio"/> |
| User3 can sign in from an anonymous IP address. | <input type="radio"/> | <input type="radio"/> |

| Statements                                      | Yes                              | No                               |
|-------------------------------------------------|----------------------------------|----------------------------------|
| User1 can sign in from an anonymous IP address. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 can sign in from an anonymous IP address. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User3 can sign in from an anonymous IP address. | <input type="radio"/>            | <input checked="" type="radio"/> |

Correct Answer:

User1 can sign in from an anonymous IP address.

User2 can sign in from an anonymous IP address.

User3 can sign in from an anonymous IP address.

Box 1: Yes -

Note: Azure AD Identity Protection can review user sign-in attempts and take additional action if there's suspicious behavior:

Some of the following actions may trigger Azure AD Identity Protection risk detection:

Users with leaked credentials.

\* -> Sign-ins from anonymous IP addresses.

Impossible travel to atypical locations.

Sign-ins from infected devices.

Sign-ins from IP addresses with suspicious activity.

Sign-ins from unfamiliar locations.

Box 2: No -

Box 3: No -

Reference:

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

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

Anonymous IP triggers sign-in risk policy (not user risk policy)

So user1 gets only user risk policy —> not affected, can login YES

User2 affected by the sign-in risk policy, and has no MFA so cannot login NO

User 3 gets both policies, but only policy 2 is used for the anonymous IP, and he has MFA, so can login YES

Ref: <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

upvoted 44 times

 **kanew** 7 months ago

Perfectly explained - I agree it's Y,N,Y

upvoted 3 times

 **mcas** 11 months, 3 weeks ago

I think User 2 should be YES. MFA disabled doesn't mean the user cannot use it, the user will be prompted to set up MFA first and after that he can use it. Tested it in lab

upvoted 1 times

 **purek77** 11 months, 1 week ago

Unfortunately MS thinks that first you use MFA Registration policy to make sure that all users do have MFA enabled+configured. Why ? Because 'If a sign-in risk policy prompts for MFA, the user must already be registered for Azure AD Multi-Factor Authentication.'

So 2nd option is No.

upvoted 2 times

 **Holi** 5 months, 4 weeks ago

You'd have a field day on the AZ-500 examtopics dump. There are a TON of these questions, and every single one tosses out "MFA is enabled but not enforced, but the user can still technically login"

upvoted 1 times

 **LeTrinh** 9 months, 2 weeks ago

You're right, Purek77

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

upvoted 1 times

 **ItchyBrain81** 1 year, 2 months ago

User3 is the tricky one. The question ask "Can user sign-in from anonymous IP Address?". The answer is "No". User can sign-in after MFA is confirmed.

upvoted 3 times

 **existingname** 1 year, 3 months ago

On the exam today, I answered Yes No Yes

upvoted 8 times

 **0byte** Highly Voted  1 year, 1 month ago

Sign-in from an anonymous IP address falls into Sign-in risk. This means only members of Group 2 will be affected by Identity Protection.

User1 can log in from any IP as user's IP is not scrutinized. The user is not in scope of Sign-In policy.

User2 cannot login. This user is in scope of the Sign-In policy and will be challenged to perform MFA. Since MFA is disabled, MFA challenge will be unsuccessful – login fails.

User3 can log in. This user is also in scope of the Sign-In policy, but since user's MFA is working (hence assuming a successful MFA challenge) the user will be granted access.

I'd say: Y-N-Y

upvoted 8 times

 **BenLam** Most Recent  1 month ago

Even the reference provided in the answer says sign in risk prompts for MFA if configured which it is. So its YNY

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

Yes

No

Yes

upvoted 2 times

 **dule27** 5 months, 3 weeks ago

Yes

No

Yes

upvoted 2 times

 **TomasValtor** 6 months ago

# 2 should be no

Makes sure users are registered for Azure AD Multi-Factor Authentication. If a sign-in risk policy prompts for MFA, the user must already be registered for Azure AD Multi-Factor Authentication.

upvoted 1 times

□ **Aquintero** 10 months, 1 week ago

para mi la respuesta correcta es Yes, No, Yes

upvoted 1 times

□ **jojoseph** 10 months, 2 weeks ago

Yes No Yes

upvoted 1 times

□ **jack987** 11 months, 2 weeks ago

The correct answer is Yes - No - No

I agree with zokaniedereenhet:

User 3 is member of both group 1 and 2. Group 1 had blocking action. Block wins over grant so user can't login.

<https://danielchronlund.com/2018/11/23/how-multiple-conditional-access-policies-are-applied/>

upvoted 1 times

□ **jack987** 11 months, 1 week ago

I had a mistake. The correct answer is Y-N-Y.

I agree with existingname and 0byte.

User 3 gets both policies, but only policy 2 is used for the anonymous IP, and he has MFA, so can login YES

upvoted 5 times

□ **zokaniedereenhet** 11 months, 2 weeks ago

I agree given answer (Y,N,N) is correct. User 3 is member of both group 1 and 2. Group 1 had blocking action. Block wins over grant so user can't login.

<https://danielchronlund.com/2018/11/23/how-multiple-conditional-access-policies-are-applied/>

upvoted 2 times

□ **Cepheid** 11 months, 1 week ago

Block wins over grant. However, we're talking here about user and sign in risk policies. The question concerns a sign in risk type. It should be Y,N,Y.

upvoted 3 times

□ **purek77** 11 months, 1 week ago

Come on guys - group 2 is for different policy (sign-in) - you can't even think about who should win here.

upvoted 3 times

□ **[Removed]** 11 months, 4 weeks ago

Given answer is correct!

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant.

You configure self-service password reset (SSPR) by using the following settings:

Require users to register when signing in: Yes

Number of methods required to reset: 1

What is a valid authentication method available to users?

- A. an email to an address outside your organization
- B. a smartcard
- C. an FID02 security token
- D. a Microsoft Teams chat

**Correct Answer: A**

A one-gate policy requires one piece of authentication data, such as an email address or phone number.

A one-gate policy applies in the following circumstances:

It's within the first 30 days of a trial subscription; or

A custom domain hasn't been configured for your Azure AD tenant so is using the default \*.onmicrosoft.com. The default \*.onmicrosoft.com domain isn't recommended for production use; and Azure AD Connect isn't synchronizing identities.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences>

*Community vote distribution*

A (100%)

 **dule27** 5 months ago

**Selected Answer: A**

A. an email to an address outside your organization

upvoted 1 times

 **ShoaibPKDXB** 6 months, 3 weeks ago

**Selected Answer: A**

A is correct

upvoted 1 times

 **shoutiv** 12 months ago

**Selected Answer: A**

A - Email

Explanation:

The following authentication methods are available for SSPR (self-service password reset)

- app notification
- Mobile app code
- Email
- Mobile phone
- Office phone (available only for tenants with paid subscriptions)
- Security questions

upvoted 3 times

 **Jawad1462** 1 year, 1 month ago

**Selected Answer: A**

Is the correct answer

upvoted 1 times

 **TheMCT** 1 year, 1 month ago

The given answer is correct!

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name  | Member of |
|-------|-----------|
| User1 | Group1    |
| User2 | Group2    |
| User3 | Group3    |

The tenant has the authentication methods shown in the following table.

| Method                      | Target | Enabled |
|-----------------------------|--------|---------|
| FIDO2                       | Group2 | Yes     |
| Microsoft Authenticator app | Group1 | Yes     |
| SMS                         | Group3 | Yes     |

Which users will sign in to cloud apps by matching a number shown in the app with a number shown on their phone?

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

#### Correct Answer: A

Microsoft Authenticator -

You can also allow your employee's phone to become a passwordless authentication method. You may already be using the Authenticator app as a convenient multi-factor authentication option in addition to a password. You can also use the Authenticator App as a passwordless option.

The Authenticator App turns any iOS or Android phone into a strong, passwordless credential. Users can sign in to any platform or browser by getting a notification to their phone, matching a number displayed on the screen to the one on their phone, and then using their biometric (touch or face) or PIN to confirm.

Incorrect:

\* Not User2

FIDO2 security keys -

The FIDO (Fast IDentity Online) Alliance helps to promote open authentication standards and reduce the use of passwords as a form of authentication. FIDO2 is the latest standard that incorporates the web authentication (WebAuthn) standard.

FIDO2 security keys are an unphishable standards-based passwordless authentication method that can come in any form factor. Fast Identity Online (FIDO) is an open standard for passwordless authentication. FIDO allows users and organizations to leverage the standard to sign in to their resources without a username or password using an external security key or a platform key built into a device.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>

Community vote distribution

A (100%)

 **EmnCours** 4 months, 2 weeks ago

**Selected Answer: A**

Answer is A

upvoted 1 times

 **dule27** 5 months, 3 weeks ago

**Selected Answer: A**

A. User1 only (MA App)

upvoted 1 times

 **jojoseph** 10 months, 2 weeks ago

**Selected Answer: A**

A is right

upvoted 1 times

□ **zokaniedereenhet** 11 months, 2 weeks ago

SMS is a preview feature, might also work?!

upvoted 1 times

□ **ZauberSRS** 1 year ago

**Selected Answer: A**

Answer: A

I have had this for at least a year on my private MS account with MFA

upvoted 1 times

□ **LHADUK** 1 year ago

Number matching will be enabled by default in February 2023!

How to use number matching in multifactor authentication (MFA) notifications - Authentication methods policy - <https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match>

upvoted 2 times

□ **Faheem2020** 1 year, 1 month ago

The code doesn't come to your phone in the form of SMS

FIDO doesn't display no code

Microsoft Authenticator is the only answer

upvoted 3 times

□ **kanew** 7 months ago

Agree. It is a terribly worded question. I think they are referring to number matching but Authenticator is the only option regardless

upvoted 1 times

□ **DeepMoon** 1 year, 2 months ago

The answer makes sense; it is the only possible answer. But the question doesn't make sense.

upvoted 4 times

□ **keanwvegas** 7 months, 3 weeks ago

I think what pointed it out to me after incorrectly answering was the part saying "...shown in the APP..."

upvoted 1 times

□ **keanwvegas** 7 months, 3 weeks ago

Also, it says "...SIGN IN to cloud apps...", which denotes that they're performing the full user authentication process from their device (app + biometric/pin)

upvoted 1 times

□ **DeepMoon** 1 year, 2 months ago

I find this question a bit confusing.

Well, Authenticator app is on the phone. It may have OATH code that you enter into a webpage.

What is this?

"Which users will sign in to cloud apps by matching a number shown in the app with a number shown on their phone?"

Can someone make sense of this?

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1 and the conditional access policies shown in the following table.

| Name      | Status      | Conditional access requirement           |
|-----------|-------------|------------------------------------------|
| CAPolicy1 | On          | Users connect from a trusted IP address. |
| CAPolicy2 | On          | Users' devices are marked as compliant.  |
| CAPolicy3 | Report-only | The sign-in risk of users is low.        |

You need to evaluate which policies will be applied to User1 when User1 attempts to sign-in from various IP addresses.

Which feature should you use?

- A. Access reviews\*
- B. Identity Secure Score
- C. The What If tool
- D. the Microsoft 365 network connectivity test tool

**Correct Answer: C**

The Azure AD conditional access What if tool allows you to understand the impact of your conditional access policies on your environment. Instead of test driving your policies by performing multiple sign-ins manually, this tool enables you to evaluate a simulated sign-in of a user. The simulation estimates the impact this sign-in has on your policies and generates a simulation report. The report does not only list the applied conditional access policies but also classic policies if they exist.

Reference:

<https://azure.microsoft.com/en-us/updates/azure-ad-conditional-access-what-if-tool-is-now-available>

*Community vote distribution*

C (100%)

 **Kawinho** Highly Voted 1 year, 2 months ago

Correct.

upvoted 5 times

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

**Selected Answer: C**

Correct Answer: C

upvoted 1 times

 **dule27** 5 months, 3 weeks ago

**Selected Answer: C**

C. The What If tool

upvoted 1 times

 **ShoaibPKDXB** 6 months, 3 weeks ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **Aquintero** 10 months, 1 week ago

**Selected Answer: C**

de acuerdo la respuesta es: C. La herramienta What If

upvoted 1 times

 **shoutiv** 11 months, 2 weeks ago

**Selected Answer: C**

C - The what if tool

"The What If tool provides a way to quickly determine the policies that apply to a specific user"

Source:

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/what-if-tool>

upvoted 2 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. an app password
- B. voice
- C. Windows Hello for Business
- D. security questions

**Correct Answer: A**

The Microsoft Authenticator app provides an additional level of security to your Azure AD work or school account or your Microsoft account and is available for

Android and iOS. With the Microsoft Authenticator app, users can authenticate in a passwordless way during sign-in, or as an additional verification option during self-service password reset (SSPR) or multifactor authentication events.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#verification-code-from-mobile-app>

*Community vote distribution*

C (98%)

✉ **birrach** Highly Voted 1 year, 2 months ago

**Selected Answer: C**

App Passwords are a legacy feature for old Office versions. Windows Hello is the way to go.

upvoted 13 times

✉ **ndawg07** Highly Voted 1 year, 3 months ago

**Selected Answer: C**

C should be the answer.

upvoted 9 times

✉ **poesklap** Most Recent 6 days, 20 hours ago

**Selected Answer: C**

Windows Hello for Business is the correct answer.

upvoted 1 times

✉ **BenLam** 1 month ago

**Selected Answer: C**

App Passwords was deprecated last year.

<https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online>

upvoted 1 times

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

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN. After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.

Incorrect Answers:

A: An app password can be used to open an application but it cannot be used to sign in to a computer.

upvoted 1 times

✉ **EmnCours** 4 months, 2 weeks ago

**Selected Answer: C**

C is correct

upvoted 1 times

✉ **dule27** 5 months, 3 weeks ago

**Selected Answer: C**

C. Windows Hello for Business  
upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: C**

C is correct  
upvoted 1 times

 **kanew** 7 months ago

**Selected Answer: C**

C is the correct answer. A is legacy authentication and would bypass MFA  
upvoted 1 times

 **Aquintero** 10 months, 1 week ago

**Selected Answer: C**

Windows Hello  
upvoted 2 times

 **chrisp1992** 11 months, 3 weeks ago

**Selected Answer: C**

App Passwords are legacy  
upvoted 4 times

 **[Removed]** 11 months, 4 weeks ago

**Selected Answer: C**

Windows Hello for Business is the correct answer.  
upvoted 4 times

 **samir45** 1 year, 2 months ago

**Selected Answer: A**

There is nothing in question that says these devices are enabled for 'Windows Hello for Business'. Given answer is correct.  
upvoted 1 times

 **Hot\_156** 1 year, 2 months ago

It says "You plan to implement multi-factor authentication (MFA)." that doesn't mean either they have the option to implement an App... but you are assuming that  
upvoted 3 times

 **Hot\_156** 1 year, 2 months ago

**Selected Answer: C**

C is the answer  
upvoted 5 times

 **ItchyBrain81** 1 year, 2 months ago

**Selected Answer: C**

WHD is considered as MFA (Access to a physical device and a PIN).  
So C is correct.  
upvoted 3 times

 **existingname** 1 year, 3 months ago

Windows Hello for Business  
upvoted 5 times

You create a conditional access policy that blocks access when a user triggers a high-severity sign-in alert.

You need to test the policy under the following conditions:

- A user signs in from another country.
- A user triggers a sign-in risk.

What should you use to complete the test?

- A. the Conditional Access What If tool
- B. sign-ins logs in Azure Active Directory (Azure AD)
- C. the activity logs in Microsoft Defender for Cloud Apps
- D. access reviews in Azure Active Directory (Azure AD)

**Correct Answer: A**

The Azure AD conditional access What if tool allows you to understand the impact of your conditional access policies on your environment. Instead of test driving your policies by performing multiple sign-ins manually, this tool enables you to evaluate a simulated sign-in of a user. The simulation estimates the impact this sign-in has on your policies and generates a simulation report. The report does not only list the applied conditional access policies but also classic policies if they exist.

Reference:

<https://azure.microsoft.com/en-us/updates/azure-ad-conditional-access-what-if-tool-is-now-available>

*Community vote distribution*

A (100%)

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: A**

A. the Conditional Access What If tool

The Conditional Access What If tool allows you to simulate the effects of conditional access policies on users and identify the potential impact of policy changes without affecting real user sessions. This tool will help you test the policy for the given scenarios.

Option B (sign-ins logs in Azure Active Directory) is used to view historical sign-in logs but doesn't allow you to simulate policy changes.

Option C (the activity logs in Microsoft Defender for Cloud Apps) is not directly related to conditional access policy testing.

Option D (access reviews in Azure Active Directory) is used for managing and reviewing access to resources and is not suitable for testing conditional access policies.

upvoted 1 times

 **EmnCours** 4 months, 2 weeks ago

**Selected Answer: A**

Correct Answer: A

upvoted 1 times

 **dule27** 5 months, 3 weeks ago

**Selected Answer: A**

A. the Conditional Access What If tool

upvoted 1 times

 **kmk\_01** 7 months, 4 weeks ago

**Selected Answer: A**

Agreed

upvoted 1 times

 **Aquintero** 10 months, 1 week ago

**Selected Answer: A**

A. la herramienta What If de acceso condicional

upvoted 1 times

 **BRoald** 11 months ago

**Selected Answer: A**

So easy it feels like a trick

upvoted 2 times

 **shoutiv** 11 months, 2 weeks ago

**Selected Answer: A**

A - the Conditional Access what if tool

"In the Conditional Access What If tool, you first need to configure the conditions of the sign-in scenario you want to simulate. These settings may include:

- The user you want to test
- The cloud apps the user would attempt to access
- The conditions under which access to the configured cloud apps is performed (included ip address, country, device platform, client apps, sign-in risk, user risk level, service principal risk, other filters for devices)"

Source:

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/what-if-tool>

upvoted 1 times

 **[Removed]** 11 months, 4 weeks ago

**Selected Answer: A**

Given answer is correct.

upvoted 1 times

## HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name  | Member of | Multi-factor authentication (MFA) |
|-------|-----------|-----------------------------------|
| User1 | Group1    | Disabled                          |
| User2 | Group2    | Enforced                          |

You have the locations shown in the following table.

| Name      | Private address space | Public NAT address space |
|-----------|-----------------------|--------------------------|
| Location1 | 10.10.0.0/16          | 20.93.15.0/24            |
| Location2 | 192.168.0.0/16        | 193.17.17.0/24           |

The tenant contains a named location that has the following configurations:

- Name: Location1
- Mark as trusted location: Enabled

IPv4 range: 10.10.0.0/16 -

-

MFA has a trusted IP address range of 193.17.17.0/24.

- Name: CAPolicy1
- Assignments
  - Users or workload identities: Group1
  - Cloud apps or actions: All cloud apps
- Conditions
- Locations: All trusted locations
- Access controls
  - Grant
  - Grant access: Require multi-factor authentication
  - 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.

Hot Area:

| Statements                                                                                       | Yes                   | No                    |
|--------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.  | <input type="radio"/> | <input type="radio"/> |
| If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.  | <input type="radio"/> | <input type="radio"/> |
| If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA. | <input type="radio"/> | <input type="radio"/> |

Correct Answer:

| Statements                                                                                       | Yes                              | No                               |
|--------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA. | <input checked="" type="radio"/> | <input type="radio"/>            |

Box 1: No -

10.10.0.150 is from a trusted location.

Note: The trusted IPs feature of Azure AD Multi-Factor Authentication bypasses multi-factor 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 Azure AD Multi-Factor

Authentication prompt. The trusted IPs feature requires Azure AD Premium P1 edition.

Box 2: No -

10.10.1.160 is from a trusted location

Box 3: Yes -

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

 **dejo** Highly Voted 1 year, 2 months ago

I think (feel free to discuss):

- 1) No
- 2) Yes (although the request is from a trusted location, that doesn't mean the MFA prompt will be bypassed! If there was CA policy configured to require MFA with the trusted locations EXCLUDED, then the user would not get the MFA prompt)
- 3) No (request is coming from the IP that is added to the MFA trusted IPs list in the legacy MFA portal  
<https://account.activedirectory.windowsazure.com/UserManagement/MfaSettings.aspx>)

upvoted 21 times

 **f2bf85a** 7 months, 4 weeks ago

I agree with the answers, but in 2) it is YES just because the MFA is enforced. The trusted location does not have the public IPs, Azure AD does not see the private IPs of the clients, just the public internet IP.

So User2 does not sign in from a trusted location, thus the CA policy does not apply.

But just because he has MFA Enforced, he will be prompted for MFA, so YES

upvoted 4 times

 **hyc1983** Highly Voted 1 year ago

This is what I think:

- 1 - No. Although 10.10.0.0/16 is a named trusted location, it's a private IP range and won't function correctly, so user 1 won't match the condition of CA policy 1. In addition, user 1 has per-user MFA disabled, it won't be prompted for MFA.
- 2 - Yes. User2's source IP is 10.10.1.160, the public IP of which is in the range of 20.93.15.0/24, which isn't a trusted MFA range. Besides, User2 is a per-user MFA-enforced user. Therefore, User2 will be prompted for MFA.
- 3 - No. The public IP address of 192.168.1.20 is in the space of 193.17.17.0/24, which is an MFA-trusted IP range. Although user2 is a per-user MFA-enforced user, it won't be prompted for MFA.

upvoted 14 times

 **b233f0a** 5 months, 1 week ago

N - User1/Group1 is in CA Policy. IPv4 Range is a trusted location in the CA Policy so no MFA required.

Y - User 2 is not in CA Policy. MFA is Enforced. IP address is not the Public IP for MFA trusted range so not trusted.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips>

Y - Same as above

upvoted 4 times

 **Nivos23** 1 month ago

I agree with you

no

yes

no

upvoted 1 times

 **mibur** 12 months ago

Last one is Y so NYY. a MFA Enforced users is prompted for MFA even when logging in from a whitelisted/trusted location.

upvoted 2 times

 **kanew** 7 months ago

It is yes but not for that reason or not for just that reason. The CA policy applies and is "Grant with MFA" so they will be prompted by the policy in any case.

upvoted 2 times

 **kanew** 7 months ago

My Bad, the last one is a No. See my reasons on the post a couple below this

upvoted 1 times

 **wooyourdaddy** 10 months, 2 weeks ago

From the following link:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates>

If needed, you can instead enable each account for per-user Azure AD Multi-Factor Authentication. When users are enabled individually, they perform multi-factor 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 2 times

 **MrPrasox** 1 year ago

Fully agree with NYN answers and with posted explanation.

upvoted 1 times

✉ **Nyamnyam** Most Recent 3 weeks, 6 days ago

N-Y-N

Think of this:

Location1 is a "named location" marked as trusted, but wrongly configured with a private IP range, which the cloud-based MFA cannot resolve (it sees only the public IP address).

And then we have "MFA has a trusted IP address range of 193.17.17.0/24", which is a service setting under Protection > Multifactor authentication > Service settings. This works outside of CAPs!

Then comes the CAP with the "All trusted locations" condition, which will never be triggered, as clarified above!

Then the answers are clear:

User1 will NEVER be prompted for MFA.

User2 will be prompted for MFA EXCEPT from the "MFA trusted IPs", which is only the public IP from Location2 (which is case 3)

upvoted 1 times

✉ **syougun200x** 2 months, 2 weeks ago

1 No. Regardless if the policy applies or not, User 1 is MFA Disabled. No prompt.

2 Yes. The policy does not apply to User 2 (Assignments only to group 1). User 2 is MFA enforced. to be prompted.

3 No. The policy does not apply to User 2 (Assignments only to group 1). User 2 is MFA enforced, but the IP range is included in the below (MFA setting).

Skip multi-factor authentication for requests from following range of IP address subnets

upvoted 2 times

✉ **Hawklx** 5 months, 3 weeks ago

The question is very confusing and it needs to be broken down a bit further

Location 1: is 20.93.15.0/24 (this is trusted as named location)

Location 2: is 193.17.17.0/24 (this is a trusted IP range for Skip multi-factor authentication in the legacy MFA portal)

The CA policy target only users in Group1 that are in trusted locations, it does not say it All trusted location are excluded (this is an assumption, but this is not what the problem statement says)

so if a user is in the 10.10.0.0/16 range, is actually in Location1  
and if a user is in the 192.168.0.0/16, is in Location2

1. User1 is in Location1 so the CA policy does require to do MFA, the CA apply to trusted location not the other way around, the word "exclude trusted location" was never mentioned.
2. User2 is in Location1 but not in Group1, no CA policy apply
3. User2 is in Location2 that is trusted, so no MFA is going to apply there

so the answers are

Y

N

N

upvoted 2 times

✉ **ServerBrain** 3 months ago

User1 MFA is disabled, so user1 can't be prompted isn't it?

upvoted 1 times

✉ **ivzdf** 4 months, 1 week ago

Completely agree

upvoted 1 times

✉ **ivzdf** 4 months, 1 week ago

if the condition is met which in this case is trusted location, then in order to grant access MFA must be met.

upvoted 1 times

✉ **kanew** 7 months ago

The correct answer is N,Y,Y . It seemed so simple initially and I got it wrong but it's not as easy as it looked at first glance. We are being asked if the user will be prompted for MFA - NOT if they fall within scope of a conditional access policy.

Number 2 is the only part that should cause any confusion. An enforced status means the legacy per user MFA is enabled.(I tested this. MFA Registration because of a CA policy does not change the legacy per MFA status - it remains as "disabled".) In this scenario the user will be asked to MFA every time except from a trusted location. The trusted location exception does not apply here so they will get a MFA prompt because of the per user MFA setting.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates>

upvoted 1 times

✉ **kanew** 7 months ago

Ok so 2 mins after i posted the above i have egg on my face :-(. I missed that the the policy only applied to Group 1 so user 2 isn't in scope. I also missed the terminology of a named location marked as trusted versus a trusted IP. A trusted IP is part of the legacy per user MFA so in part 3 USER 2 is not part of the conditional access policy but does have MFA enforced. However they are coming from a trusted IP so will not receive a MFA prompt. N,Y,N.

upvoted 1 times

✉ **JBail** 7 months, 1 week ago

The answer shown is correct, but the explanation for it is not.

Answer is: N-N-Y

Reason:

- 1 - No - User 1 has MFA Disabled, so will not be prompted for MFA
- 2 - No - User 2 is coming from Location 1 and Location one's IP is only configured in this CA policy using a private address, so it won't be prompted.
- 3 - Yes - User 2 is coming from Location 2, and this is configured in the CA policy to prompt MFA.

The main confusion is due to the configuration being weak.

If you want to prompt for MFA and exclude Trusted locations, you set the locations as "All Locations", exclude "Trusted Locations" and Require MFA - This means that you will be prompted for MFA at all locations except the Trusted Locations.

What this policy will actually achieve is only prompting for MFA in the Trusted Location 193.17.17.0/24, and nowhere else.

upvoted 3 times

✉ **Holii** 5 months, 3 weeks ago

Re-read the question.

Policy is only applying to Group1/User1.

THE POLICY DOES NOT APPLY TO GROUP2/USER2

1 - No - User 1 has MFA disabled, but this doesn't matter. They won't be asked for it because it's not a trusted location. (The policy is looking for only trust location on 193.17.17.0/24, like you said)

2 - Yes - User 2 is coming from a non-trusted location. It has MFA enforced.

3 - No - User 3 is coming from a trusted location. It has MFA enforced.

We only are using the CA policy for User 1. User 2 is treated strictly on only the MFA trusted IP range.

upvoted 3 times

✉ **Holii** 5 months, 3 weeks ago

\*correction: trusted location is the private IP range, which is likely a misconfiguration, because we needed the public NAT here.

upvoted 1 times

✉ **kanew** 7 months ago

2 is Y. The Enforced MFA status of User 2 means they are using the per user MFA setting and will be prompted for MFA every time. Remember we are not being asked if the conditional access policy applies but if the user will be prompted for MFA

upvoted 1 times

✉ **f2bf85a** 7 months, 4 weeks ago

No: User1 Has MFA Disabled, but although he is member of Group1, the public IP range he is logging in from does not belong to the Trusted location (only public IP is visible to Azure AD), so the CA policy will not apply.

Yes: User2 connects from a Public CIDR that is not a trusted location and is in Group2, so CA policy does not apply, but MFA is Enforced, so he will be prompted for MFA.

Yes: User2 policy does not apply (not in trusted locations and member of Group 2), has MFA Enforced, but connects from the MFA Trusted IP range (public range), so he won't be prompted for MFA.

Tested it in lab, if MFA Trusted IP CIDRs are defined and enabled, MFA Enforcement is bypassed.

upvoted 2 times

✉ **f2bf85a** 7 months, 4 weeks ago

Sorry, it is No Yes NO (made a mistake on the 3rd one)

upvoted 1 times

✉ **iwantmyexamsobad** 8 months ago

To me it's YES NO NO

1) YES because the CA policy is only for group1 (user1). His public IP address is not trusted therefore the CA push a MFA prompt no matter his user MFA status.

2) The CA policy only applies to group1 members, user2 isn't a part of that.

3) same as above

upvoted 1 times

✉ **rfuentessc** 8 months, 1 week ago

The level of confusion seems to display the level ridiculousness of some of these questions

upvoted 2 times

✉ **StijnDW** 8 months, 1 week ago

woyourdaddy explained the reasoning though

upvoted 1 times

✉ **Taigr** 9 months, 3 weeks ago

Hi guys, why is 10.10.1.160 trusted IP? IP range for 10.10.0.0/24 is "10.10.0.0 - 10.10.0.255"  
so it should not be in trusted IPs

upvoted 1 times

✉ **Raven84** 7 months, 3 weeks ago

It is /16 not /24

upvoted 1 times

✉ **AWS56** 9 months, 3 weeks ago

No-Yes-No

upvoted 1 times

 **Halwagy** 10 months, 1 week ago

YYN

User 1 is accessing from internal IP which will not be dedicated by the policy so he will be informed for MFA by CA regardless he registered for MFA for not

User 2 already enforced for MFA so will be enforced for MFA regardless part of CA or not as he is not accessing from trusted IPs

User 2 will not be prompt for MFA as accessing from trusted IP range

upvoted 3 times

 **Raven84** 7 months, 3 weeks ago

CA applies to trusted locations only. So User1 will not be affected of any CA imho

upvoted 1 times

 **eternalenvy** 4 months, 1 week ago

User 1 will be affected on CA policy named CAPolicy1, because conditions of Locations is applied to All trusted locations, it does not select exclude all trusted locations. So, when User1 access from any of trusted locations User1 will be prompted for MFA.

upvoted 1 times

 **wsrudmen** 10 months, 2 weeks ago

1-NO

User1 is targeted by the CAPolicy.

The IP is in the trusted location "Location1", so the grant access requiring MFA will be bypassed

2-YES

User2 is out of the CA policy and has MFA enabled for him and have maybe already registered MFA.

He is not in the trusted MFA IP address range (of MFA settings), so MFA will be required

3-NO

User2 is out of the CA policy and has MFA enabled for him and have maybe already registered MFA.

He is in the trusted MFA IP address range (of MFA settings), so MFA will be bypassed

upvoted 2 times

 **LP223** 10 months, 3 weeks ago

1. No-- User1 is in the CA policy and exempt

2. No- User2 is not in the CA but coming from Trusted Location, which is tenant-wide

3. Yes- User 2 is not in the CA and also not logging in from Trusted location. Also has MFA enforced.

upvoted 4 times

 **jack987** 11 months, 2 weeks ago

The answer is correct.

No - No - Yes

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

Note

The trusted IPs can include private IP ranges only when you use MFA Server. For cloud-based Azure AD Multi-Factor Authentication, you can use only public IP address ranges.

upvoted 2 times

 **Ikeinater** 1 year ago

NNN

user 1 is the only one in group 1. User 1 MFA is disabled and the other 2 questions talk about group 2 to which the policy doesn't apply. The rest of the question is just there to trick you.

upvoted 1 times

 **Ikeinater** 12 months ago

NYN\*

See hyc1983 explanation.

upvoted 1 times

**HOTSPOT -**

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Email one-time passcode for guests set to Yes.

You invite the guest users shown in the following table.

| Name   | Email domain | Account type            |
|--------|--------------|-------------------------|
| Guest1 | adatum.com   | Azure AD account        |
| Guest2 | outlook.com  | Microsoft account       |
| Guest3 | gmail.com    | Personal Google account |

Which users will receive a one-time passcode, and how long will the passcode be valid? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Users:

Guest1 only  
 Guest2 only  
 Guest3 only  
 Guest1 and Guest2 only  
 Guest2 and Guest3 only  
 Guest1, Guest2, and Guest3

Valid for:

30 minutes  
 60 minutes  
 24 hours  
 48 hours

Correct Answer:

Users:

Guest1 only  
 Guest2 only  
 Guest3 only  
 Guest1 and Guest2 only  
 Guest2 and Guest3 only  
 Guest1, Guest2, and Guest3

Valid for:

30 minutes  
 60 minutes  
 24 hours  
 48 hours

Box 1: Guest3 only -

When does a guest user get a one-time passcode?

When a guest user redeems an invitation or uses a link to a resource that has been shared with them, they'll receive a one-time passcode if:

They don't have an Azure AD account

They don't have a Microsoft account

The inviting tenant didn't set up federation with social (like Google) or other identity providers.

Box 2: 30 minutes -

One-time passcodes are valid for 30 minutes. After 30 minutes, that specific one-time passcode is no longer valid, and the user must request a new one. User sessions expire after 24 hours. After that time, the guest user receives a new passcode when they access the resource. Session expiration provides added security, especially when a guest user leaves their company or no longer needs access.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode>

□  **dbmc** 2 months ago

Correct, and was on exam today.

upvoted 3 times

□  **mfarhat1994** 2 months ago

how was the exam and were these questions in the exam ?

upvoted 2 times

□  **EmnCours** 3 months, 3 weeks ago

Users:Guest 3 Only

Valid: 30 minutes

upvoted 1 times

□  **EmnCours** 4 months, 2 weeks ago

Users:Guest 3 Only

Valid: 30 minutes

When a guest user redeems an invitation or uses a link to a resource that has been shared with them, they'll receive a one-time passcode if:

They don't have an Azure AD account.

They don't have a Microsoft account.

The inviting tenant didn't set up federation with social (like Google) or other identity providers.

They don't have any other authentication method or any password-backed accounts.

Email one-time passcode is enabled.

One-time passcodes are valid for 30 minutes. After 30 minutes, that specific one-time passcode is no longer valid, and the user must request a new one.

upvoted 2 times

□  **dule27** 5 months, 3 weeks ago

Users:Guest 3 Only

Valid: 30 minutes

upvoted 3 times

□  **Pedro2021** 11 months, 1 week ago

Guest 3 and 30 minutes

upvoted 3 times

□  **[Removed]** 11 months, 4 weeks ago

Answers correct.

upvoted 1 times

□  **kk1** 1 year, 1 month ago

It is correct for 30 min. access

upvoted 1 times

□  **gwajwara** 1 year, 3 months ago

Guest 3 Only, 30 minutes: <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode#when-does-a-guest-user-get-a-one-time-passcode>

upvoted 3 times

□  **BRoald** 11 months ago

Great link! The given answers are correct in this case

upvoted 1 times

□  **existingname** 1 year, 3 months ago

correct, in the exam today

upvoted 4 times

You have a Microsoft 365 tenant.

You currently allow email clients that use Basic authentication to connect to Microsoft Exchange Online.

You need to ensure that users can connect to Exchange only from email clients that use Modern authentication protocols.

What should you implement?

- A. an OAuth policy in Microsoft Defender for Cloud Apps
- B. a conditional access policy in Azure Active Directory (Azure AD)
- C. a compliance policy in Microsoft Endpoint Manager
- D. an application control profile in Microsoft Endpoint Manager

**Correct Answer: D**

*Community vote distribution*

B (95%) 5%

 **curtmcgirt** 2 weeks, 6 days ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **Nyamnyam** 3 weeks, 6 days ago

**Selected Answer: B**

Hahaha, Examtopics must be kidding.

B for sure.

D is impossible, because:

there's no such thing as "application control profile in Microsoft Endpoint Manager"

the nearest is "application control policy", but this is "designed to protect devices against malware and other untrusted software".

upvoted 1 times

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: B**

B. a conditional access policy in Azure Active Directory (Azure AD)

Conditional access policies in Azure AD allow you to control access to resources based on conditions such as user location, device compliance, and client application type. By creating a conditional access policy that enforces Modern authentication protocols and blocks Basic authentication, you can achieve the desired security outcome. This will ensure that only email clients supporting Modern authentication are allowed to connect to Exchange Online.

Options A, C, and D are not directly related to enforcing the use of Modern authentication protocols for Exchange Online and would not achieve the goal of blocking Basic authentication.

upvoted 4 times

 **OutLawTheBoyzz** 3 months, 2 weeks ago

WOW, so many different answers.. I am going with B

<https://o365reports.com/2022/07/20/disable-basic-authentication-office-365/>

upvoted 2 times

 **EmnCours** 4 months, 2 weeks ago

**Selected Answer: B**

Correct Answer: D

upvoted 2 times

 **dule27** 5 months, 3 weeks ago

**Selected Answer: B**

B. a conditional access policy in Azure Active Directory (Azure AD)

upvoted 3 times

 **Aidanjl** 5 months, 3 weeks ago

**Selected Answer: D**

Hi - I think you guys are incorrect. This question is asking to specifically block 'BASIC' Authentication in Exchange Online, not 'LEGACY' Authentication. Microsoft specifically details how to do this here:

<https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online>  
upvoted 1 times

□ **Aidanjl** 5 months, 3 weeks ago  
Sorry I think I'm incorrect... just realised D doesn't line up to the guidance in the MS article  
upvoted 3 times

□ **TomasValtor** 6 months ago

B is correct  
The easiest way to block legacy authentication across your entire organization is by configuring a Conditional Access policy that applies specifically to legacy authentication clients and blocks access.  
upvoted 1 times

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

**Selected Answer: B**

B is correct

upvoted 1 times

□ **sbnpj** 7 months, 4 weeks ago

**Selected Answer: B**

Conditional access policy is used for blocking legacy auth.

upvoted 1 times

□ **Guestie** 9 months, 1 week ago

**Selected Answer: B**

The question says nothing about what type of device or what the application being used is so setting an App control policy will not do anything. CA policies allow legacy auth to be blocked regardless of device.

upvoted 1 times

□ **wsrudmen** 10 months, 2 weeks ago

**Selected Answer: B**

B also

upvoted 1 times

□ **Oknip** 10 months, 2 weeks ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

upvoted 1 times

□ **ydecac** 10 months, 2 weeks ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

upvoted 2 times

□ **Halwagy** 10 months, 2 weeks ago

**Selected Answer: B**

as you can block legacy connection to Exchange from CA

upvoted 1 times

□ **RobbieBoyBlue** 10 months, 3 weeks ago

B for me

upvoted 1 times

□ **natazar** 10 months, 3 weeks ago

**Selected Answer: B**

Why not B tho?

upvoted 2 times

□ **kevin\_office** 10 months, 3 weeks ago

Why B? I think you should explain to why you would choose B instead of just asking a question friend :)

upvoted 1 times

□ **fuzzilogic** 9 months ago

Because in AAD you can create CA to block legacy authentication.

upvoted 1 times

You have an Azure subscription that contains an Azure SQL database named db1.

You deploy an Azure App Service web app named App1 that provides product information to users that connect to App1 anonymously.

You need to provide App1 with access to db1. The solution must meet the following requirements:

- Credentials must only be available to App1.
- Administrative effort must be minimized.

Which type of credentials should you use?

- A. a system-assigned managed identity
- B. an Azure Active Directory (Azure AD) user account
- C. a SQL Server account
- D. a user-assigned managed identity

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **mali1969** Highly Voted 5 months, 2 weeks ago

To provide App1 with access to db1 while minimizing administrative effort and ensuring that credentials are only available to App1, you should use a system-assigned managed identity.

A system-assigned managed identity is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Azure AD tenant that's trusted by the subscription of the instance

This way, you don't need to create or manage any secrets or credentials for your application. The identity is automatically managed by Azure and enables you to authenticate to any service that supports Azure AD authentication without having any credentials in your code

upvoted 6 times

 **haazybanj** Most Recent 4 weeks ago

**Selected Answer: A**

The best answer is A. a system-assigned managed identity.

A system-assigned managed identity is a type of managed identity that is automatically created and assigned to an Azure resource when it is created. System-assigned managed identities are easy to use and manage, and they can be used to access resources in Azure, including Azure SQL databases.

D. a user-assigned managed identity: A user-assigned managed identity is a type of managed identity that is created and managed by the user. User-assigned managed identities can be used to access resources in Azure, but they are more complex to use and manage than system-assigned managed identities.

upvoted 1 times

 **EmnCours** 4 months, 2 weeks ago

**Selected Answer: A**

Correct Answer: A

upvoted 1 times

 **dule27** 5 months, 3 weeks ago

**Selected Answer: A**

A. a system-assigned managed identity

upvoted 1 times

 **ShoaibPKDXB** 6 months, 3 weeks ago

**Selected Answer: A**

A is correct

upvoted 1 times

 **chikorita** 8 months, 1 week ago

A is correct: system assigned MI

upvoted 1 times

 **Oknip** 10 months, 2 weeks ago

**Selected Answer: A**

A is correct

upvoted 2 times

 **Halwagy** 10 months, 2 weeks ago

**Selected Answer: A**

Anser is correct

upvoted 2 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

You have an Azure subscription that contains the custom roles shown in the following table.

| Name  | Type                                   |
|-------|----------------------------------------|
| Role1 | Azure Active Directory (Azure AD) role |
| Role2 | Azure subscription role                |

You need to create a custom Azure subscription role named Role3 by using the Azure portal. Role3 will use the baseline permissions of an existing role.

Which roles can you clone to create Role3?

- A. Role2 only
- B. built-in Azure subscription roles only
- C. built-in Azure subscription roles and Role2 only
- D. built-in Azure subscription roles and built-in Azure AD roles only
- E. Role1, Role2, built-in Azure subscription roles, and built-in Azure AD roles

**Correct Answer: C**

*Community vote distribution*

C (76%) A (24%)

 **haskelatchi** Highly Voted 6 months, 3 weeks ago

I have cleared 3 certifications and can confirm the answer is F  
upvoted 12 times

 **UKG** 4 months ago

loooooool  
upvoted 3 times

 **voituredecourse** Highly Voted 5 months ago

I have cleared 19 certifications, it is definitely C  
upvoted 7 times

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

am I the only one thinking that the 2 answers in C are the same?  
Maybe I misunderstand the question  
upvoted 1 times

 **Alscoran** 1 week ago

They are not. Role 2 is a custom Azure subscription role. Now they are asking what you can CLONE. The answer you can clone one of the Built-in Azure subscription roles or Role 2 (which is a custom one, not a built-in one).  
upvoted 2 times

 **kijken** 2 days, 11 hours ago

Thank you for clarifying. Now I understand the question and answer is C :)  
upvoted 1 times

 **haazybanj** 4 weeks ago

I have cleared 29 certifications but can't confirm the answer.  
upvoted 1 times

 **dule27** 5 months, 3 weeks ago

**Selected Answer: C**

C. built-in Azure subscription roles and Role2 only  
upvoted 4 times

 **kmk\_01** 7 months, 4 weeks ago

**Selected Answer: C**

I have passed AZ-104 & AZ-305, I would go for Option C too.  
upvoted 5 times

 **chikorita** 8 months, 1 week ago

i have cleared 2 certifications  
i can confirm its C: built-in Azure subscription roles and Role2 only  
upvoted 3 times

 **topzz** 8 months ago

thanks for confirming that you cleared 2 certs, otherwise your statement wouldn't have been as valuable.  
upvoted 9 times

 **kmk\_01** 7 months, 4 weeks ago

LOL. I have passed AZ-104 & AZ-305, I would go for Option C too.  
upvoted 3 times

 **Zak366** 9 months, 2 weeks ago

**Selected Answer: C**

I tested in a very clean tenant:

1. Went to create a custom role and in the drop down I saw all azure built-in roles
  2. Created a custom role (test-custom) and went to create a custom role again, this time in drop down, I could also see test-custom
- upvoted 4 times

 **dejo** 9 months, 3 weeks ago

**Selected Answer: C**

It's unclear if the question asks which roles can be cloned from a single action or in general, but I'd say the latter. So, both custom and Azure built-in roles can be cloned - <https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#clone-a-role>

upvoted 3 times

 **wsrudmen** 10 months, 2 weeks ago

**Selected Answer: A**

I think it's Role2 only as the option to clone is only for custom existing role.  
After you can copy paste the JSON of a built-in role, but it's not native.  
It's a little bit ambiguous...  
upvoted 3 times

 **Kuneho** 10 months, 2 weeks ago

The answer is correct. C. tested in the lab. You can clone Role2 (CustomRole) and Azure Built-in Roles  
upvoted 5 times

 **Halwagy** 10 months, 2 weeks ago

**Selected Answer: A**

it is not clear,  
but Role2 only or Built-in Azure subscription role only not both of them  
upvoted 2 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. Windows Hello for Business
- B. an app password
- C. security questions
- D. email

**Correct Answer: B**

*Community vote distribution*

A (78%) R (22%)

 **kevin\_office** Highly Voted 10 months, 3 weeks ago

Should be A. Windows Hello for business > app password. This question comes up several times and many users indicate that Windows hello for business is what should be the answer.

upvoted 8 times

 **Holii** Highly Voted 5 months, 4 weeks ago

I swear if I see this question again with the selected answer being "An App Password" im gonna scream  
upvoted 6 times

 **rohitrc8521** 1 month, 4 weeks ago

loooooooooool  
upvoted 1 times

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

It is Hello for Business, the other 3 answers are not even possible forms of verification.

The following additional forms of verification can be used with Microsoft Entra multifactor authentication:

Microsoft Authenticator

Authenticator Lite (in Outlook)

Windows Hello for Business

FIDO2 security key

OATH hardware token (preview)

OATH software token

SMS

Voice call

upvoted 1 times

 **dule27** 5 months, 3 weeks ago

**Selected Answer: A**

A. Windows Hello for Business

upvoted 1 times

 **ShoaibPKDXB** 6 months, 3 weeks ago

**Selected Answer: A**

A is correct

upvoted 1 times

 **Ignaci0s** 8 months, 3 weeks ago

Widows Hello is not considered a 2nd Factor it's only the first step to authenticate a user. In this case the answer would be app password.  
upvoted 2 times

 **Ruslan23** 8 months, 2 weeks ago

Windows Hello for Business IS considered an MFA take a look to official FAQ <https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-faq#is-windows-hello-for-business-considered-multi-factor-authentication>  
upvoted 4 times

✉ **kmk\_01** 7 months, 4 weeks ago

That told Nacho.  
upvoted 4 times

✉ **mayleni** 10 months, 1 week ago

**Selected Answer: A**

WHFB!! Totally  
upvoted 1 times

✉ **faeem** 10 months, 1 week ago

**Selected Answer: A**

Should be A Windows Hello for business > app password. This question comes up several times and many users indicate that Windows hello for business is what should be the answer.

upvoted 1 times

✉ **Oknip** 10 months, 2 weeks ago

**Selected Answer: R**

Windows Hello for Business  
upvoted 2 times

✉ **chikorita** 8 months, 3 weeks ago

R? lol

upvoted 3 times

✉ **ydecac** 10 months, 2 weeks ago

**Selected Answer: A**

This question comes up several times and many users indicate Windows hello  
upvoted 1 times

✉ **Halwagy** 10 months, 2 weeks ago

**Selected Answer: A**

Windows Hello for Business  
upvoted 2 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. voice
- B. Windows Hello for Business
- C. email
- D. security questions

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **Holii** Highly Voted 5 months, 4 weeks ago

WFHB \*internal screaming\*  
upvoted 10 times

 **gusherinos** 3 months, 3 weeks ago

Best answer!  
upvoted 2 times

 **Nabgre** Highly Voted 10 months, 3 weeks ago

Selected Answer: B  
Given response is not correct. The right response is B  
upvoted 6 times

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

Who the fuck is answering this questions?  
upvoted 2 times

 **dule27** 5 months, 3 weeks ago

Selected Answer: B  
B. Windows Hello for Business  
upvoted 1 times

 **Selvaraj\_Rajan** 7 months, 1 week ago

Selected Answer: B  
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted>

As per the above link, the following are MFA methods for Azure

Windows Hello for Business

Microsoft Authenticator app

FIDO2 security key (preview)

OATH hardware tokens (preview)

OATH software tokens

SMS verification

Voice call verification

upvoted 1 times

 **Schuiram** 7 months, 2 weeks ago

Selected Answer: B  
<https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-faq>

<https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-faq>  
upvoted 1 times

 **Ignaci0s** 8 months, 3 weeks ago

Windows Hello is just the first step to authenticate a User so the answer should be "voice".

upvoted 2 times

 **Ruslan23** 8 months, 2 weeks ago

Windows Hello for Business IS an MFA: <https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-faq#is-windows-hello-for-business-considered-multi-factor-authentication>

upvoted 1 times

 **PaianIT** 9 months, 3 weeks ago

The answer is A = Voice -

you can let the call go to a landline number (because there is no mobile phone connection)

NO B: Windows Hello is NO MFA, it is only the first step and needs a second factor afterwards

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

NO D: it is ~~only~~ a method for SSPR not for Sign-in

No B: it is no secure method in Microsoft MFA

upvoted 2 times

 **Zak366** 9 months, 2 weeks ago

You have the right logic, but unfortunately MS exam logic doesn't work that way, if it doesn't say there IS a landline available, then answer is B, Windows Hello for Business

upvoted 1 times

 **Laxmesh** 10 months, 1 week ago

**Selected Answer: B**

Windows Hello for Business

upvoted 3 times

 **Oknip** 10 months, 2 weeks ago

**Selected Answer: B**

Windows Hello for Business

upvoted 2 times

 **ydecac** 10 months, 2 weeks ago

**Selected Answer: B**

mobile phone connectivity = No Voice

upvoted 3 times

 **chikorita** 8 months, 1 week ago

upvote maxxxxxxxxxxx

upvoted 1 times

 **Halwagy** 10 months, 2 weeks ago

**Selected Answer: B**

Windows Hello for Business

upvoted 2 times

**HOTSPOT**

You have an Azure subscription that contains the following virtual machine:

- Name: V1
- Azure region: East US
- System-assigned managed identity: Disabled

You create the managed identities shown in the following table.

| Name     | Location |
|----------|----------|
| Managed1 | East US  |
| Managed2 | East US  |
| Managed3 | West US  |

You perform the following actions:

- Assign Managed1 to V1.
- Create a resource group named RG1 in the West US region.

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 assign Managed2 to V1.

You can assign Managed3 to V1.

You can assign VM1 the Owner role for RG1.

**Answer Area**

| Statements | Yes | No |
|------------|-----|----|
|------------|-----|----|

**Correct Answer:** You can assign Managed2 to V1.

You can assign Managed3 to V1.

You can assign VM1 the Owner role for RG1.

YYN.

You can use user assigned managed identities in more than one Azure region.

upvoted 11 times

✉ **wooyourdaddy** 10 months, 1 week ago

Correct regarding managed identities and regions:

<https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identities-faq#can-the-same-managed-identity-be-used-across-multiple-regions>

upvoted 4 times

✉ **AK\_1234** Most Recent 1 month, 3 weeks ago

- Y

- Y

- N

upvoted 2 times

✉ **Obyte** 1 month, 4 weeks ago

YYN

Ref first two questions - both are Y because you can assign managed identity to a VM regardless of which region the identity or VM is located - I tested it.

Ref the third one - I think N. The catch here is that you cannot assign a role directly to a VM but only to an identity, system or user managed.

upvoted 2 times

✉ **Nyamnyam** 3 weeks, 6 days ago

Good point on case 3. Initially I thought it should be YYY, but the Identity you assign an owner permission, and not the Virtual Machine. And again, it is even wrongly written: VM1 instead of V1, as in case 1 and 2.

upvoted 1 times

✉ **EmnCours** 3 months, 3 weeks ago

YES

YES

YES

upvoted 1 times

✉ **nils241** 4 months ago

The first two are definite yes / yes. For the third, it depends on the scenario;

Scenario 1:

I give one of the user assinged identities the owner role. Problem: Every service with the identity would be owern. This would possibly contradict the principle of least privilege. But then it would be Y/ Y /Y

Scenario 2:

I want only the VM to be Owner and assume that I don't want to give the permission to a User assigned Identity. I don't have a System Assinged Identity, so then: Y /Y / N

Since it is not directly stated here whether the assignment of the authorization to a Managed Identity (User assigned) is allowed, I assume an authorization of the VM directly. Therefore I feel more comfortable with Y /Y / N.

upvoted 1 times

✉ **mali1969** 5 months, 2 weeks ago

You can assign Managed2 to V1 (Yes), but you cannot assign Managed3 to V1 (No).

You can assign the owner role for RG1 to V1 (Yes), but there is no VM1 mentioned in the message.

upvoted 1 times

✉ **dule27** 5 months, 3 weeks ago

YES

YES

YES

upvoted 1 times

✉ **ITAdmin2019** 6 months, 4 weeks ago

Just tested this in my lab - the answer is YYY:

vm1 created with system assigned identity off (vm1 is in North Europe)

useridentity1 created in NorthEurope can be assigned to the VM

useridentity2 created in EastUS can be assigned to the VM

Adding useridentity1 as an owner to a resource group in Brazil worked fine

upvoted 4 times

✉ **cris\_exam** 8 months, 1 week ago

As long as the system-assigned managed identity is disabled on an Azure VM resource, then there is no way to add any user-assigned managed identity.

However, the question does tell us that managed-assigned identities get created which it doesn't specify, but they should be USER-assigned managed identities (system-assigned identities cannot be created as stand-alone they are tied to a resource that you deploy), anyhow, then we are told that Managed1 is added to the VM which would mean that the system-assigned identity has been enabled (otherwise it wouldn't work). If so, then all 3 Managed Identities can be added to the VM.

Regarding the last statement, it's YES, you can assign the VM with the owner role for the RG, it doesn't impact due to region.

In conclusion I say it should be YYY.

upvoted 2 times

✉️ **nils241** 4 months ago

You can add "user assigned identitys" without enable "system assigned" on the VM

upvoted 1 times

✉️ **chikorita** 8 months, 1 week ago

i feel the same too

upvoted 1 times

✉️ **cris\_exam** 8 months, 1 week ago

As long as the system-assigned managed identity on the VM is disabled and there is no other subscription/tenant level policy that would deny adding the owner role to a VM.

If anybody has a better research, please correct me.

upvoted 1 times

✉️ **chikorita** 8 months, 1 week ago

can anyone help me understand why 3rd box is marked as NO?

i mean it doesn't make sense but its possible to have VM's MI to have roles of its own  
correct me if wrong plz

upvoted 1 times

✉️ **Arjanussie** 9 months, 1 week ago

bad question the table does not see if it is user or system assigned and that makes the difference

cross region is only supported for user-assigned since with system assigned each region would have to create its own identity since it's tied to the resource itself

upvoted 2 times

✉️ **hieverbody** 10 months, 2 weeks ago

I believe VM1 should be Managed 1 here. So answer is No.

upvoted 1 times

✉️ **natazar** 10 months, 3 weeks ago

I think it should be YNN

upvoted 1 times

✉️ **kevin\_office** 10 months, 3 weeks ago

please dont just say it should be this and that. u need to justify why it should be YNN so that other users see if u are right or not. u end up confusing people by just saying what u think without stating why!

upvoted 45 times

## HOTSPOT

You have an Azure subscription that contains the key vaults shown in the following table.

| Name      | In resource group | Number of days to retain deleted key vaults | Purge protection |
|-----------|-------------------|---------------------------------------------|------------------|
| KeyVault1 | RG1               | 15                                          | Enabled          |
| KeyVault2 | RG1               | 10                                          | Disabled         |

The subscription contains the users shown in the following table.

| Name   | Role                           |
|--------|--------------------------------|
| Admin1 | Key Vault Administrator        |
| Admin2 | Key Vault Contributor          |
| Admin3 | Key Vault Certificates Officer |
| Admin4 | Owner                          |

On June 1, Admin4 performs the following actions:

- Deletes a certificate named Certificate1 from KeyVault1
- Deletes a secret named Secret1 from KeyVault2

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 recover Secret1 on June 7.     | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin2 can purge Certificate1 on June 12. | <input type="radio"/>            | <input checked="" type="radio"/> |
| Admin3 can purge Certificate1 on June 14. | <input type="radio"/>            | <input checked="" type="radio"/> |

## Answer Area

| Statements                                            | Yes                              | No                               |
|-------------------------------------------------------|----------------------------------|----------------------------------|
| Correct Answer: Admin1 can recover Secret1 on June 7. | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin2 can purge Certificate1 on June 12.             | <input type="radio"/>            | <input checked="" type="radio"/> |
| Admin3 can purge Certificate1 on June 14.             | <input type="radio"/>            | <input checked="" type="radio"/> |

wsrudmen Highly Voted 10 months, 2 weeks ago

Yes - Key Vault Administrator can perform all data plane operations on a key vault.  
and purge protection is disabled for KeyVault2.

NB: Purge protection is an optional Key Vault behavior and is not enabled by default.  
Do not mismatch with soft-delete

No - We are still in the Purge protection remaining period.

NB: Also the Key Vault contributor role doesn't allow to get access to certificate

No - We are still in the Purge protection remaining period.

Even if the Certificate Officer role allow to get access to certificate

upvoted 15 times

Holii 5 months, 4 weeks ago

Correct, even though the Purge Protection doesn't have a specified retention period, the minimum time you can specify is 7 days, which is more than the dates specified.

<https://learn.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview#purge-protection>

upvoted 1 times

Holii 5 months, 4 weeks ago

Forgive me, I am blind. There are dates quite literally listed in the question. Still the same.

upvoted 3 times

Markus Highly Voted 10 months, 3 weeks ago

Correct. When purge protection is on, a vault or an object in the deleted state cannot be purged until the retention period has passed.

upvoted 6 times

EmnCours Most Recent 4 months, 1 week ago

Yes - Key Vault Administrator can perform all data plane operations on a key vault.  
and purge protection is disabled for KeyVault2.

NB: Purge protection is an optional Key Vault behavior and is not enabled by default.  
Do not mismatch with soft-delete

No - We are still in the Purge protection remaining period.

NB: Also the Key Vault contributor role doesn't allow to get access to certificate

No - We are still in the Purge protection remaining period.

Even if the Certificate Officer role allow to get access to certificate

upvoted 2 times

EmnCours 4 months, 2 weeks ago

Is correct

Y

N

N

Generally, only the subscription owner will be able to purge a key vault.

upvoted 1 times

dule27 5 months, 2 weeks ago

YES

NO

NO

upvoted 1 times

OK2020 6 months ago

<https://learn.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview>

upvoted 1 times

OK2020 6 months ago

<https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli>

upvoted 1 times

You have an Azure AD tenant.

You open the risk detections report.

Which risk detection type is classified as a user risk?

- A. password spray
- B. anonymous IP address
- C. unfamiliar sign-in properties
- D. Azure AD threat intelligence

**Correct Answer: D**

*Community vote distribution*

D (100%)

👤 **ThotSlayer69** Highly Voted 10 months, 2 weeks ago

**Selected Answer: D**

\*\*Sign-in Risk policies cover:\*\*

- Anonymous IP address
- Additional Risk detected
- Admin confirmed user compromised
- Anomalous token
- Atypical travel
- Azure AD threat intelligence
- Impossible travel
- Malicious IP
- Malware linked IP
- Mass Access to sensitive files
- New country
- Password spray
- Suspicious browser
- Suspicious inbox forwarding
- Suspicious inbox manipulation rules
- token issuer anomaly
- Unfamiliar sign-in properties

\*\*User risk policies cover:\*\*

- Additional risk detected
- Anomalous user activity
- Azure AD threat intelligence
- Leaked credentials
- Possible attempt to access Primary Refresh Token (PRT)

upvoted 15 times

👤 **AK\_1234** Most Recent 1 month, 4 weeks ago

User Risk - D

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

upvoted 1 times

👤 **EmnCours** 4 months, 2 weeks ago

**Selected Answer: D**

- D. Azure AD threat intelligence

upvoted 1 times

👤 **dule27** 5 months, 3 weeks ago

**Selected Answer: D**

- D. Azure AD threat intelligence

upvoted 1 times

👤 **ShoaibPKDXB** 6 months, 3 weeks ago

**Selected Answer: D**

D correct

upvoted 1 times

👤 **wsrudmen** 10 months, 2 weeks ago

**Selected Answer: D**

Correct

upvoted 2 times

 **Halwagy** 10 months, 2 weeks ago

**Selected Answer: D**

Correct

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

upvoted 4 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

You have an Azure Active Directory (Azure AD) tenant.

You configure self-service password reset (SSPR) by using the following settings:

- Require users to register when signing in: Yes
- Number of methods required to reset: 1

What is a valid authentication method available to users?

- A. a smartcard
- B. a mobile app code
- C. a mobile app notification
- D. an email to an address outside your organization

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉️ 🚑 Guestie Highly Voted 9 months, 1 week ago

There should be an option for multiple answers. When configuring SSPR for a single method to reset there are two options - Mobile app code AND Email  
upvoted 7 times

✉️ 🚑 Nyamnyam Most Recent 3 weeks, 6 days ago

Oh well, same question in page 13 had a proper answer 'D'.  
What to say? If you selected mobile app as auth method AND only one method for verification, then indeed only CODE is possible.  
BUT what if the admin has selected Email, Mobile phone, and Security questions as only allowed auth methods?  
upvoted 1 times

✉️ 🚑 roman\_cat 3 months, 2 weeks ago

D. an email address outside your organization.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

"The Authenticator app can't be selected as the only authentication method when only one method is required." READ: when only one method is required.

- A. Smart Card- not an option in SSPR
  - B. Mobile app code- available in Microsoft authenticator.
  - C. a mobile app notification - not available as an option for single method
  - D. email outside the organization - available option (in fact default) in SSPR
- upvoted 1 times

✉️ 🚑 Shri96 2 months, 2 weeks ago

If require registration was set to No, I believe you'd be correct. As we have registration required, and only a single authentication method defined, the App Code registered becomes the default.  
Answer should be B in this case due to the "require registration" requirement.

upvoted 3 times

✉️ 🚑 EmnCours 4 months, 2 weeks ago

Selected Answer: B

Correct Answer: B  
upvoted 1 times

✉️ 🚑 dule27 5 months, 3 weeks ago

Selected Answer: B

B. a mobile app code  
upvoted 1 times

✉️ 🚑 JN\_311 6 months ago

Selected Answer: B

When administrators require one method be used to reset a password, verification code is the only option available.  
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#mobile-app-and-sspr>  
upvoted 1 times

roman\_cat 3 months, 2 weeks ago  
question is asking for users, not administrators  
upvoted 1 times

kanew 7 months ago  
This isn't as straight forward as it seems and from what I can read it depends on whether the converged registration method(MFA & SSPR) is being used. If using the current SSPR registration then the answer would be D as you can't use the App when only one method is required because it is not an available method on sign-up.

"This requirement is because the current SSPR registration experience doesn't include the option to register the authenticator app. The option to register the authenticator app is included with the new combined registration experience."  
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#authentication-methods>

It's the other way around if the combined registration is used as email is only valid for SSPR and users won't be required to register it on sign up. It can be a secondary method. I can't tell from the question whether it's SSPR or combined registration. maybe someone else can? Guess I'll go with the consensus of B but ...?

upvoted 1 times

francescoc 8 months, 1 week ago  
**Selected Answer: B**  
B is Correct  
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>  
upvoted 1 times

divyakanth 10 months, 1 week ago  
**Selected Answer: B**  
correct explanation by wooyou  
upvoted 1 times

Halwagy 10 months, 2 weeks ago  
D also a valid option  
upvoted 1 times

wooyourdaddy 10 months, 1 week ago  
It is only if 2 authentication methods are required.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#mobile-app-and-sspr>

When using a mobile app as a method for password reset, like the Microsoft Authenticator app, the following considerations apply:

- When administrators require one method be used to reset a password, verification code is the only option available.
- When administrators require two methods be used to reset a password, users are able to use notification OR verification code in addition to any other enabled methods.

upvoted 3 times

kevin\_office 10 months, 2 weeks ago  
yeah but D comes when B is not available  
upvoted 2 times

You create a new Microsoft 365 E5 tenant.

You need to ensure that when users connect to the Microsoft 365 portal from an anonymous IP address, they are prompted to use multi-factor authentication (MFA).

What should you configure?

- A. a sign-in risk policy
- B. a user risk policy
- C. an MFA registration policy

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **BRoald** Highly Voted 10 months, 2 weeks ago

Sign-in risk is correct.

Examples for Sign-In Risk:

Anonymous IP address  
Atypical travel  
Malware linked IP address  
Unfamiliar sign-in properties  
Leaked credentials  
Password spray  
upvoted 6 times

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

**Selected Answer: A**

A. a sign-in risk policy  
upvoted 1 times

 **dule27** 5 months, 3 weeks ago

**Selected Answer: A**

A. a sign-in risk policy  
upvoted 1 times

 **ShoaibPKDXB** 6 months, 4 weeks ago

**Selected Answer: A**

A correct  
upvoted 1 times

 **rajbne** 7 months, 1 week ago

its "new" tenancy so could be C as well  
upvoted 1 times

 **bda92b3** 8 months, 4 weeks ago

Correct  
upvoted 1 times

 **Jotest** 10 months, 2 weeks ago

sign-in risk policy seems to be correct  
upvoted 2 times

## HOTSPOT

You have a Microsoft 365 tenant.

You configure a conditional access policy as shown in the Conditional Access policy exhibit. (Click the Conditional Access policy tab.)

Home > ContosoAzureAD > Security > Conditional access policies

## Policy1 Created: 2023-01-01 10:00 UTC ...

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*  
Policy1

Assignments

Users and groups (1)  
All users

Cloud apps or actions (1)  
All cloud apps

Conditions (0)  
0 conditions selected

Access controls

Grant (1)  
1 control selected

Session (0)  
0 controls selected

Enable policy

Report-only  On  Off

## Grant

Control user access enforcement to block or grant access. [Learn more](#)

Block access  
 Grant access

Require multi-factor authentication (1)  
 Require device to be marked as compliant (1)  
 Require Hybrid Azure AD joined device (1)  
 Require approved client app (1)  
[See list of approved client apps](#)  
 Require app protection policy (1)  
[See list of policy protected client apps](#)  
 Require password change (1)

For multiple controls

Require all the selected controls  
 Require one of the selected controls

You view the User administrator role settings as shown in the Role setting details exhibit. (Click the Role setting details tab.)

## Role setting details - User Administrator

Privileged Identity Management | Azure AD roles



Edit

### Activation

| Setting                                  | State                |
|------------------------------------------|----------------------|
| Activation maximum duration (hours)      | 8 hour(s)            |
| Require justification on activation      | Yes                  |
| Require ticket information on activation | No                   |
| On activation, require Azure MFA         | Yes                  |
| Require approval to activate             | Yes                  |
| Approvers                                | 1 Member(s), 0 Group |

### Assignment

| Setting                                                        | State      |
|----------------------------------------------------------------|------------|
| Allow permanent eligible assignment                            | No         |
| Expire eligible assignments after                              | 15 day(s)  |
| Allow permanent active assignment                              | No         |
| Expire active assignments after                                | 1 month(s) |
| Require Azure Multi-Factor Authentication on active assignment | No         |
| Require justification on active assignment                     | No         |

You view the User administrator role assignments as shown in the Role assignments exhibit. (Click the Role assignments tab.)

## User Administrator | Assignments

Privileged Identity Management | Azure AD roles



Add assignments

Settings

Refresh

Export

Got feedback?

Eligible assignments

Active assignments

Expired assignments

Search by member name or principal name

Name Principal name

Type Scope

Membership

User Administrator

Admin1 Admin1@m365x629615.onmicrosoft.com User Directory Direct

Admin2 Admin2@m365x629615.onmicrosoft.com User Directory Direct

Admin3 Admin3@m365x629615.onmicrosoft.com User Directory Direct

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

NOTE: Each correct selection is worth one point.

| Statements                                                                                                                                                                                               | Yes                   | No                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.                                                                             | <input type="radio"/> | <input type="radio"/> |
| Admin2 can request activation of the User administrator role for a period of two hours.                                                                                                                  | <input type="radio"/> | <input type="radio"/> |
| If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice. | <input type="radio"/> | <input type="radio"/> |

店铺：专业认证88

| Statements                                                                                                                                                                                               | Yes                                 | No                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|-------------------------------------|
| Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.                                                                             | <input checked="" type="checkbox"/> | <input type="radio"/>               |
| Correct Answer: Admin2 can request activation of the User administrator role for a period of two hours.                                                                                                  | <input checked="" type="checkbox"/> | <input type="radio"/>               |
| If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice. | <input type="radio"/>               | <input checked="" type="checkbox"/> |

Halwagy Highly Voted 10 months, 2 weeks ago

Correct

upvoted 10 times

chikorita Highly Voted 8 months, 1 week ago

i think it should be YYY

cuz if admin 3 signs-in first, conditional access policy is applied first- which enforces MFA later, during role activation, MFA is required to activate the role so MFA authentication is done TWICE

upvoted 6 times

Holii 5 months, 4 weeks ago

Tested in my own tenant. Settings replicated to match the User Administrator MFA requirements and Conditional Access Policy MFA requirements.

User did not need to authenticate using MFA twice. This is part of Microsoft's approach to reduce MFA exhaustion, the Primary Refresh Token (PRT) for the user will still contain the MFA information.

upvoted 3 times

cris\_exam 8 months, 1 week ago

I would also go with YYY as you explained, it makes sense.

upvoted 1 times

cris\_exam 8 months, 1 week ago

take back what I said - Require MFA on Active assignment is set to NO. so it's YYN.

upvoted 3 times

chikorita 8 months, 1 week ago

thats for Active assignment but Admin3 falls under Eligible assignment

well, for eligible users to activate roles; we need to check "on activation, require Azure MFA" which is set to YES.

i still believe its YYY

upvoted 3 times

jinxie 5 months ago

If you have already validated with the correct MFA before then you will not be asked again. The exception to this is if you use Authentication Strengths and have a higher MFA requirement for that MFA role then you logged in with. e.g. you performed SMS MFA, enabled the role but the Conditional Access role expects users with that role to have use MSAuthenticator, then you would get another MFA request but that is not the case here so YYN

upvoted 1 times

Nivos23 Most Recent 1 month ago

Correct

upvoted 1 times

EmnCours 4 months, 2 weeks ago

Yes Yes No

upvoted 3 times

 **Heshan** 4 months, 4 weeks ago

On the exam, 09/07/2023

upvoted 2 times

 **dule27** 5 months, 3 weeks ago

Yes

Yes

No

upvoted 3 times

 **217f3c9** 7 months, 2 weeks ago

It is YYN. The first conditional access screen shows that every user MUST provide MFA. This is stored in the token. If the same user is asked for MFA it will be provided by the token non-interactively.

upvoted 5 times

 **Holii** 5 months, 4 weeks ago

Tested and confirmed. YYN.

upvoted 1 times

 **f2bf85a** 7 months, 3 weeks ago

Its Yes Yes No

User may not be prompted for multi-factor authentication if they authenticated with strong credentials, or provided multi-factor authentication earlier in this session.

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings#on-activation-require-multi-factor-authentication>

upvoted 2 times

## HOTSPOT

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

| Name  | User risk level |
|-------|-----------------|
| User1 | Low             |
| User2 | Medium          |
| User3 | High            |

You have the Azure AD Identity Protection policies shown in the following table.

| Type                | Users     | User risk     | Sign-in risk | Controls     |
|---------------------|-----------|---------------|--------------|--------------|
| User risk policy    | All users | Low and above | Unconfigured | Block access |
| Sign-in risk policy | All users | Unconfigured  | High         | Block access |

You review the Risky users report and the Risky sign-ins report and perform actions for each user as shown in the following table.

| User  | Action                   |
|-------|--------------------------|
| User1 | Confirm user compromised |
| User2 | Confirm sign-in safe     |
| User3 | Dismiss user risk        |
| User2 | Confirm user compromised |

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

NOTE: Each correct selection is worth one point.

| Statements                                                    | Yes                   | No                    |
|---------------------------------------------------------------|-----------------------|-----------------------|
| User1 can sign in by using multi-factor authentication (MFA). | <input type="radio"/> | <input type="radio"/> |
| User2 can sign in by using multi-factor authentication (MFA). | <input type="radio"/> | <input type="radio"/> |
| User3 can sign in from an anonymous IP address.               | <input type="radio"/> | <input type="radio"/> |

| Statements                                                                    | Yes                                 | No                                  |
|-------------------------------------------------------------------------------|-------------------------------------|-------------------------------------|
| User1 can sign in by using multi-factor authentication (MFA).                 | <input checked="" type="checkbox"/> | <input type="radio"/>               |
| Correct Answer: User2 can sign in by using multi-factor authentication (MFA). | <input checked="" type="checkbox"/> | <input type="radio"/>               |
| User3 can sign in from an anonymous IP address.                               | <input type="radio"/>               | <input checked="" type="checkbox"/> |

 **doch**  10 months, 2 weeks ago

N N N

User 1 No  
The User Risk = Low. Then User risk policy blocked access.

User 2 No  
The Sign-in Risk = Unknown. But it is Confirm Safe so we can ignore this.  
The User risk = Medium. The user risk policy block access.

User 3 No

User 3 User Risk is dismissed, but anonymous IP address risk (this is Sign-in Risk) is still at High level. Hence the sign-in risk policy blocked the access.

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#nonpremium-sign-in-risk-detections>

upvoted 17 times

 **ExamStudy68** 8 months ago

I think NNY - User 3 sign in report shows dismiss user risk <https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock#risk-remediation>

upvoted 1 times

 **c18525f** 9 months, 2 weeks ago

This question might be deprecated. In Azure activity logs, activity from an anonymous IP address would typically be classified as a medium or high severity event, depending on the specific circumstances. However there I could not find information about the circumstances anymore. Machine learning stuff :/ - what do you think ?

upvoted 1 times

 **ThotSlayer69** Highly Voted 10 months, 2 weeks ago

User1 can sign in by using multi-factor authentication (MFA): No

- Blocked access prevents self-remediation through password resets & Azure AD MFA

User2 can sign in by using multi-factor authentication (MFA): No

- Blocked access prevents self-remediation through password resets & Azure AD MFA

User3 can sign in from an anonymous IP address: Yes

- Anonymous IP address sign-in risk is Medium

upvoted 11 times

 **Shena2021** Most Recent 2 months, 2 weeks ago

1. User1 can sign in by using multi-factor authentication (MFA).

- No: User1's status is "Confirm user compromised," so access is blocked.

2. User2 can sign in by using multi-factor authentication (MFA).

- No: User2's status is "Confirm sign-in safe," which means their access is allowed without MFA.

3. User3 can sign in from an anonymous IP address.

- Yes: User3's status is "Dismiss user risk," and there's no mention of IP restrictions, so they can sign in from an anonymous IP address.

upvoted 6 times

 **Nivos23** 1 month ago

I agree, thanks for the explanation

N

N

y

upvoted 2 times

 **Nivos300** 3 weeks, 5 days ago

I agree

N

N

Y

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

N

N

Y

upvoted 1 times

 **Tweety1972** 4 months, 3 weeks ago

Box 1: No - User canNOT sign in. The status is "Confirm user compromised".

Upon receiving this feedback, we move the sign-in and user risk state to Confirmed compromised and risk level to High.

Box 2: No - User can sign in. The status is "Confirm sign-in safe".

Upon receiving this feedback, we move the sign-in (not the user) risk state to Confirmed safe and the risk level to None.

BUT the last line says "Confirm user compromised".

If the user is already remediated, don't select Confirm compromised because it moves the sign-in and user risk state to Confirmed compromised and risk level to High.

Box 3: Yes - User CAN sign in

A Dismiss user risk on the user level closes the user risk and all past risky sign-ins and risk detections.

upvoted 3 times

□  **b233f0a** 5 months, 1 week ago

My thoughts

User 1 - No

User Risk Action is "Confirm user compromised"

User 2 - Yes

User risk action is "Confirmed sign-in safe" Upon receiving Confirm Safe feedback Identity Protection sets Risk Level to None - <https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/troubleshooting-identity-protection-faq#how-do-the-feedback-mechanisms-in-identity-protection-work>

User 3 - Yes

User Risk action is "Dismiss user risk" so this is good. What level of Sign-in risk is assigned to Anonymous IP is not known, but I'm guessing that this should not be High "Microsoft doesn't provide specific details about how risk is calculated." <https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#risk-levels>

upvoted 3 times

□  **dule27** 5 months, 3 weeks ago

No

No

Yes

upvoted 2 times

□  **wsrudmen** 10 months, 2 weeks ago

NO - User1 is now at High risk level after confirming user is compromised.

Then User risk policy blocked access.

NO - Sign-in of User 2 is safe. So we can bypass Sign-in risk policy

Risk level of User2 is High due to the last action, so User risk policy block the access

YES - User3 has "Dismiss risk User" so User Risk policy is bypassed.

anonymous IP address is a risk, but context is missing to know if it's considered as an high risk.

Maybe it's an outdated question when there were fix values defined by Microsoft for risk type.

Anonymous IP was ranked as medium.

Now we don't know how Microsoft calculates the risk level.

<https://www.rebeladmin.com/2020/11/step-by-step-guide-how-to-configure-sign-in-risk-based-azure-conditional-access-policies/>

upvoted 6 times

□  **topzz** 8 months ago

agree with this

upvoted 1 times

□  **dobriv** 9 months, 2 weeks ago

OK, but Anonymous IP is Sign-in Risk, not User Risk, so I think the third should be NO.

upvoted 2 times

□  **dobriv** 7 months ago

Correction - The risk level for this risk event type is "Medium" because in itself an anonymous IP is not a strong indication of an account compromise. So, the 3-rd one is YES.

upvoted 1 times

□  **Halwagy** 10 months, 2 weeks ago

the user risk policy is block access

N N Y

upvoted 4 times

You have an Azure subscription that contains a user named User1.

You need to meet the following requirements:

- Prevent User1 from being added as an owner of newly registered apps.
- Ensure that User1 can manage the application proxy settings.
- Ensure that User1 can register apps.
- Use the principle of least privilege.

Which role should you assign to User1?

- A. Application developer
- B. Cloud application administrator
- C. Service support administrator
- D. Application administrator

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **Shena2021** 2 months, 2 weeks ago

A. Application developer

This role provides the necessary permissions for managing application proxy settings and registering apps, while it doesn't grant the owner role, aligning with the principle of least privilege preventing User1 from being added as an owner of newly registered apps

upvoted 2 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: D**

D. Application administrator

upvoted 1 times

 **dule27** 5 months, 3 weeks ago

**Selected Answer: D**

D. Application administrator

upvoted 1 times

 **dejo** 9 months, 3 weeks ago

How can you prevent User1 from being added as the owner of newly created applications if you grant him the application administrator role?

As User1 should be able to register applications, when he does that, he will automatically be assigned the owner role of those apps.

upvoted 3 times

 **Studytime2023** 20 hours, 37 minutes ago

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

upvoted 1 times

 **dobriv** 9 months, 2 weeks ago

From the doch's link :

Application Administrator

Users in this role can create and manage all aspects of enterprise applications, application registrations, and application proxy settings. Note that users assigned to this role are not added as owners when creating new application registrations or enterprise applications.

Application Developer

Users in this role can create application registrations when the "Users can register applications" setting is set to No. This role also grants permission to consent on one's own behalf when the "Users can consent to apps accessing company data on their behalf" setting is set to No. Users assigned to this role are added as owners when creating new application registrations.

D is the right one.

upvoted 8 times

 **doch** 10 months, 2 weeks ago

**Selected Answer: D**

Application Administrator is correct.

Application Administrator = Can create and manage all aspects of app registrations and enterprise apps.

Cloud Application Administrator = Can create and manage all aspects of app registrations and enterprise apps \*\*\*except App Proxy\*\*\*.

Service Support Administrator = Can read service health information and manage support tickets.

Application Developer = Can create application registrations independent of the 'Users can register applications' setting.

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

upvoted 4 times

 **Halwagy** 10 months, 2 weeks ago

**Selected Answer: D**

Correct Answer given

upvoted 4 times

## DRAG DROP

You have a Microsoft 365 E5 subscription and an Azure subscription.

You need to meet the following requirements:

- Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials.
- Delegate the ability to create new virtual machines.

What should you use for each requirement? 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                                                                                       |
|----------------------------------------------|---------------------------------------------------------------------------------------------------|
| Azure AD built-in roles                      | Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials: |
| Azure AD managed identities                  |                                                                                                   |
| Azure role-based access control (Azure RBAC) | Delegate the ability to create new virtual machines:                                              |

**Correct Answer:**

Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials:  Azure role-based access control (Azure RBAC)

Delegate the ability to create new virtual machines:  Azure AD built-in roles

 **dobriv** Highly Voted  7 months ago

There is no Azure AD built in role, which can create virtual machine.  
Only some Azure built in roles can do it.  
So I vote for both Azure RBAC.  
upvoted 10 times

 **mancio** Highly Voted  6 months, 3 weeks ago

1. Azure RBAC  
<https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows#configure-role-assignments-for-the-vm>  
2. Azure Built in Roles  
<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#classic-virtual-machine-contributor>  
upvoted 5 times

 **Hull** 3 months, 2 weeks ago

Careful, the provided option is Azure AD built-in roles, not Azure built-in roles. If it was only Azure, I'd agree, but given that it's Azure AD, both should be RBAC.  
upvoted 2 times

 **Foggy31** Most Recent  1 month, 3 weeks ago

Both RBAC There is no Azure AD build in roles to delegate creation of VM's that's in Azure built in Roles (without AD ;))  
upvoted 1 times

 **stack120566** 6 months, 3 weeks ago

In order to log on with 365 creds. The computers must be ad joined. in turn This implies device administrator role. < Azure -AD -devices- device settings - device administrators >  
1= active directory role

2. custom RBAC role fashioned upon the vm contributor role  
upvoted 3 times

 **f2bf85a** 7 months, 3 weeks ago

1. Azure RBAC  
<https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows#configure-role-assignments-for-the-vm>  
upvoted 1 times

 **ThotSlayer69** 10 months, 2 weeks ago

Delegation is handled via using the built-in roles in the Azure Virtual Desktop RBAC, very confusing but that means it's not built-in AD roles, so I'd say they're both Azure RBAC

upvoted 4 times

✉ **Zak366** 9 months, 2 weeks ago

You are right, to shed light on first options, following the links for azure role assignments, you can see in instructions the "Role: Virtual Machine User Login" from portal.azure.com>ResourceGroup (that contains VM)>IAM>add role, once this role is selected, you can assign members within tenant that are O365 users (technically)

upvoted 1 times

✉ **oscarpopi** 10 months, 2 weeks ago

Given answer is correct.

1. Azure RBAC

<https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows#configure-role-assignments-for-the-vm>

2. Azure Built in Roles

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

upvoted 2 times

✉ **Techfall** 10 months, 1 week ago

Azure Built in Roles is not one of the options. It shows Azure \_AD\_ Built in Roles:

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

upvoted 2 times

✉ **Halwagy** 10 months, 2 weeks ago

Azure AD managed Identities

Azure Role-based access control

upvoted 3 times

✉ **Halwagy** 10 months, 2 weeks ago

My mistake,

both of them is Azure Role-based access control

<https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows#configure-role-assignments-for-the-vm>

upvoted 10 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a notification through the Microsoft Authenticator app
- B. SMS
- C. email
- D. Windows Hello for Business

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **Ikazimirs** Highly Voted 4 months, 2 weeks ago

why is this question repeated so many times - this is the 5th or 6th time im seeing this.  
upvoted 6 times

 **Anonymous1312** Most Recent 1 month, 3 weeks ago

Hello? Is it this question you're looking for?  
upvoted 1 times

 **roman\_cat** 3 months, 2 weeks ago

I don't think we can use Windows Hello for Business' in mobile phones (unless the phones are using windows OS?).

Question is vague. If for Windows laptop, then WHFB

upvoted 1 times

 **Eunson** 3 months, 2 weeks ago

No mobile service or WiFi is available. The only Internet connectivity mentioned is wired. So, the question is not concerned with methods available to authenticate the mobile device only that you cannot use auth methods that require the mobile device to have an Internet connection.

upvoted 1 times

 **EmnCours** 4 months, 1 week ago

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

 **dule27** 5 months, 3 weeks ago

**Selected Answer: D**  
D. Windows Hello for Business  
upvoted 3 times

## HOTSPOT

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant. The AD DS domain contains the organizational units (OUs) shown in the following table.

| Name | Description                        |
|------|------------------------------------|
| OU1  | Syncs with Azure AD                |
| OU2  | Does <b>NOT</b> sync with Azure AD |

You need to create a break-glass account named BreakGlass.

Where should you create BreakGlass, and which role should you assign to BreakGlass? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Location:

Azure AD  
OU1  
OU2

Role:

Billing Administrator  
Global Administrator  
Owner  
Privileged Role Administrator

**Answer Area**

Correct Answer:

Location:

Azure AD  
**OU1**  
OU2

Role:

Billing Administrator  
**Global Administrator**  
Owner  
Privileged Role Administrator

DoMing Highly Voted 8 months ago

AzureAD and Global Admin

<https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access#how-to-create-an-emergency-access-account>  
upvoted 24 times

topzz 8 months ago

break-glass account = emergency access account

upvoted 3 times

kmk\_01 Highly Voted 7 months, 4 weeks ago

<https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access>

Create emergency access accounts

Create two or more emergency access accounts. These accounts should be cloud-only accounts that use the \*.onmicrosoft.com domain and that are not federated or synchronized from an on-premises environment.

upvoted 5 times

kijken Most Recent 2 weeks, 4 days ago

Sorry, but a break glass account for what? For Azure or for on prem AD?

upvoted 1 times

norkis97 1 month ago

Break glass account must be only azure ad account !

Break glass account also must be Global Administrator

upvoted 1 times

sherifhamed 2 months, 1 week ago

What is a break-glass account in azure?

A "break-glass" account, in the context of Azure and security, refers to a special or emergency account with elevated permissions that is used as a last resort to access and troubleshoot Azure resources in situations where normal access methods or credentials are unavailable or compromised. The term "break-glass" implies that this account is only to be used in emergency situations, just like breaking the glass to access a fire alarm or emergency tool.

upvoted 1 times

sgfurgi 3 months, 1 week ago

OU1? Really? And what happens if for some reason you get the OU1 unsynced or the account is deleted or moved from that OU? You ALWAYS need to have the admin accounts with azure ad or 365 roles Cloud Only.

upvoted 3 times

StarMe 3 months, 2 weeks ago

The breakglass account should be created in Azure AD and not OU1. Please correct the answer. And assign Global Admin privileges with MFA exempt for at least one such account.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access#exclude-at-least-one-account-from-conditional-access-policies>

upvoted 2 times

EmnCours 4 months, 1 week ago

AzureAD and Global Admin

upvoted 1 times

dule27 5 months, 3 weeks ago

Azure AD

Global Admin

Break-glass account has emergency access

upvoted 2 times

caef525 7 months, 1 week ago

Create two or more emergency access accounts. These accounts should be cloud-only accounts that use the \*.onmicrosoft.com domain and that are not federated or synchronized from an on-premises environment.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access#how-to-create-an-emergency-access-account>

upvoted 1 times

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to ensure that users can request access to Site1. The solution must meet the following requirements:

- Automatically approve requests from users based on their group membership.
- Automatically remove the access after 30 days.

What should you do?

- A. Create a Conditional Access policy.
- B. Create an access package.
- C. Configure Role settings in Azure AD Privileged Identity Management.
- D. Create a Microsoft Defender for Cloud Apps access policy.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **kmk\_01** Highly Voted 7 months, 4 weeks ago

**Selected Answer: B**

B (Access Packages) is the correct answer - <https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create>  
upvoted 6 times

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

**Selected Answer: B**

B. Create an access package.  
upvoted 1 times

 **dule27** 5 months, 1 week ago

**Selected Answer: B**

B. Create an access package.  
upvoted 1 times

**HOTSPOT**

You have an Azure subscription.

You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

- Users that are assigned Role1 can manage application security groups.
- Users that are assigned Role2 can manage Azure Firewall.

Which resource provider permissions are required for each role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area****Role1:**

Microsoft.App  
Microsoft.Computer  
Microsoft.Network  
Microsoft.Security

**Role2:**

Microsoft.App  
Microsoft.Management  
Microsoft.Network  
Microsoft.Security

**Answer Area****Role1:**

Microsoft.App  
Microsoft.Computer  
**Microsoft.Network**  
Microsoft.Security

Correct Answer:

**Role2:**

Microsoft.App  
Microsoft.Management  
**Microsoft.Network**  
Microsoft.Security

 **DoMing** Highly Voted 8 months ago

Correct

<https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork>

upvoted 12 times

 **kmk\_01** 7 months, 4 weeks ago

Thanks for providing the link.

upvoted 3 times

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

Role1: Microsoft.Network  
Role2: Microsoft.Network  
upvoted 2 times

dule27 5 months ago

Role1: Microsoft.Network  
Role2: Microsoft.Network  
upvoted 2 times

Question #53

Topic 2

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. voice
- B. an app password
- C. security questions
- D. a verification code from the Microsoft Authenticator app

**Correct Answer: D**

*Community vote distribution*

D (100%)

EmnCours 4 months, 1 week ago

**Selected Answer: D**

D. a verification code from the Microsoft Authenticator app  
upvoted 1 times

dule27 5 months, 3 weeks ago

**Selected Answer: D**

D. a verification code from the Microsoft Authenticator app  
upvoted 1 times

ahmedkmicha 6 months ago

**Selected Answer: D**

The Microsoft Authenticator app can generate verification codes offline, without needing a Wi-Fi or mobile data connection.  
upvoted 3 times

sbettani 6 months, 2 weeks ago

without internet ... D? We answer to 10 question with app password. Then B  
upvoted 3 times

## DRAG DROP

You have a Microsoft 365 E5 tenant.

You purchase a cloud app named App1.

You need to enable real-time session-level monitoring of App1 by using Microsoft Defender for Cloud Apps.

In which order should you perform the actions? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

**Actions****Answer Area**

Publish App1 in Azure AD.

Create a conditional access policy that has session controls configured.

From Microsoft Defender for Cloud Apps, create a session policy.

From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1.

**Answer Area**

Publish App1 in Azure AD.

From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1.

From Microsoft Defender for Cloud Apps, create a session policy.

Create a conditional access policy that has session controls configured.

**Correct Answer:**

DoMing Highly Voted 8 months ago

1. Publish App1.
2. Create a conditional access policy that has session controls configured.
3. From MCAS modify the Connected apps settings
4. From MCAS create a session policy

Reference - <https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-blocking-data-downloads-via-microsoft-cloud-app/ba-p/326357>

upvoted 22 times

EmnCours Most Recent 4 months, 1 week ago

1. Publish App1.
2. Create a conditional access policy that has session controls configured.
3. From MCAS modify the Connected apps settings
4. From MCAS create a session policy

Reference - <https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-blocking-data-downloads-via-microsoft-cloud-app/ba-p/326357>

upvoted 1 times

dule27 5 months ago

1. Publish App1 in Azure AD.
2. Create a conditional access policy that has session controls configured.
3. From Microsoft Defender for Cloud Apps modify the Connected apps settings for app1
4. From Microsoft Defender for Cloud Apps create a session policy

upvoted 1 times



## HOTSPOT

### Case Study

#### Overview

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

#### Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | None                              |
| User2 | None                              |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner | Members                        |
|-------------|----------|-----------------|-------|--------------------------------|
| IT_Group1   | Security | Assigned        | None  | All users in the IT department |
| AdatumUsers | Security | Assigned        | None  | User1, User2                   |

#### Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

#### Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.

- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

#### Requirements. Planned Changes

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

#### Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You implement the planned changes for SSPR.

What occurs when User3 attempts to use SSPR? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

Number of authentication methods required:

1  
2  
3  
4

Authentication methods that can be used:

Microsoft Authenticator only  
Security questions only  
Email and phone only  
Phone and Microsoft Authenticator only  
Email, phone, and Microsoft Authenticator only  
Email, phone, Microsoft Authenticator, and security questions

**Answer Area**

Number of authentication methods required:

  
2  
3  
4**Correct Answer:**

Authentication methods that can be used:

- Microsoft Authenticator only
- Security questions only
- Email and phone only
- Phone and Microsoft Authenticator only
- Email, phone, and Microsoft Authenticator only
- Email, phone, Microsoft Authenticator, and security questions**

  **marsot** Highly Voted 4 months, 2 weeks ago

User 3 is a User Admin. So,

Box 1: 2

Why: By default, administrator accounts are enabled for self-service password reset, and a strong default two-gate password reset policy is enforced.

Box 2: Email, phone and Microsoft Authenticator only

Why: The two-gate policy requires two pieces of authentication data, such as an email address, authenticator app, or a phone number, and it prohibits security questions.

A two-gate policy applies in the following circumstances:

....

Security administrator

Service support administrator

SharePoint administrator

Skype for Business administrator

User administrator

Source:<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences>

upvoted 10 times

  **hw121693** Most Recent 4 months, 2 weeks ago

I think authen methods should be 2, password + one of those MFA methods

upvoted 1 times

  **Peeeedor** 4 months, 2 weeks ago

I would go for:

Number of authentication methods required : 1

Authentication methods that can be used: Email, phone and MS authenticator

I picked this option because admins are prohibited from using the "security questions option"

Source:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences>

Read this part:

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. 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.

The two-gate policy requires two pieces of authentication data, such as an email address, authenticator app, or a phone number, and it prohibits security questions.

upvoted 1 times

  **JckD4Ni3L** 1 month, 1 week ago

You are contradicting yourself :)

upvoted 2 times

  **marsot** 4 months, 2 weeks ago

Box 1: 2

Box 2: Email, phone and Microsoft Authenticator only

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.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences>

upvoted 2 times

## HOTSPOT

### Case Study

#### Overview

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

#### Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | None                              |
| User2 | None                              |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner | Members                        |
|-------------|----------|-----------------|-------|--------------------------------|
| IT_Group1   | Security | Assigned        | None  | All users in the IT department |
| AdatumUsers | Security | Assigned        | None  | User1, User2                   |

#### Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

#### Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.

- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

#### Requirements. Planned Changes

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

#### Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You need to support the planned changes and meet the technical requirements for MFA.

Which feature should you use, and how long before the users must complete the registration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Feature:

An authentication method policy  
A Conditional Access policy  
An MFA registration policy  
The Multi-Factor Authentication Server settings

Grace period:

7 days  
14 days  
28 days

### Answer Area

Correct Answer:

Feature:

An authentication method policy  
A Conditional Access policy  
**An MFA registration policy**  
The Multi-Factor Authentication Server settings

Grace period:

7 days  
**14 days**  
28 days

 **marsot** Highly Voted 4 months, 2 weeks ago

agree

Box1: MFA registration policy

Box2: 14 days

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. 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'll be required to register before they can complete the sign-in process.

Source: <https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy#user-experience>

upvoted 6 times

 **JckD4Ni3L** Most Recent 1 month, 1 week ago

Answer is Correct !

upvoted 1 times

## DRAG DROP

## Case Study

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

## Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | None                              |
| User2 | None                              |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner | Members                        |
|-------------|----------|-----------------|-------|--------------------------------|
| IT_Group1   | Security | Assigned        | None  | All users in the IT department |
| AdatumUsers | Security | Assigned        | None  | User1, User2                   |

## Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

## Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.

- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

#### Requirements. Planned Changes

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

#### Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You need to resolve the recent security incident issues.

What should you configure for each incident? To answer, drag the appropriate policy types to the correct issues. 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                                                           |
|---------------------------------|-----------------------------------------------------------------------|
| An authentication method policy | Leaked credentials: <input type="text"/>                              |
| A Conditional Access policy     | A sign-in from a suspicious browser: <input type="text"/>             |
| A sign-in risk policy           | Resources accessed from an anonymous IP address: <input type="text"/> |
| A user risk policy              |                                                                       |

Leaked credentials: [A user risk policy](#)

Correct Answer: A sign-in from a suspicious browser: [A sign-in risk policy](#)

Resources accessed from an anonymous IP address: [A sign-in risk policy](#)

ACSC 2 months, 1 week ago

Box 1: User risk policy

Box 2: Sign-in risk policy

Box 3: Sign-in risk policy

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#sign-in-risk-detections>  
upvoted 4 times

madysonwyman 2 months, 3 weeks ago

Get SC 300 free exam questions: <https://www.dumpsgeek.com/SC-300-pdf-dumps.html>

upvoted 1 times

thoemes 3 months ago

i think user risk, sign in risk & conditional Access for anonymous IP

upvoted 2 times

1c67a2c 4 months ago

It could be all conditional access policy. Microsoft is recommending to migrate user and sign in risk policies to conditional access.

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies#migrate-risk-policies-from-identity-protection-to-conditional-access>

upvoted 3 times

JckD4Ni3L 1 month, 1 week ago

You are right, however it depends on the references in the Exam, should you see Entra ID, means the exam is updated and it should conditional access policy, should you see Azure AD, then it would be Sign-in/User Risk policies... no?

upvoted 1 times

JckD4Ni3L 1 month, 1 week ago

Actually you can read on the SC-300 web page that this exam will be updated on Oct 30th 2023. So if you pass this exam after this point, it's safe to assume it's Conditional Access Policy.

Exam page: <https://learn.microsoft.com/en-us/credentials/certifications/exams/sc-300/>

The important notice states: "The English language version of this exam will be updated on October 30, 2023."

upvoted 2 times

penatuna 2 months, 3 weeks ago

So it could be either the suggested answer or Conditional access to all. I would use conditional access, but I suspect that in Microsoft's mind the suggested answer is correct one. Go figure...

upvoted 1 times

penatuna 2 months, 3 weeks ago

BTW, here's a good video about the subject.

[https://youtu.be/zV\\_MBngLND0](https://youtu.be/zV_MBngLND0)

upvoted 2 times

EmnCours 4 months, 1 week ago

Correct

upvoted 2 times

A user named User1 receives an error message when attempting to access the Microsoft Defender for Cloud Apps portal.

You need to identify the cause of the error. The solution must minimize administrative effort.

What should you use?

- A. Log Analytics
- B. sign-in logs
- C. audit logs
- D. provisioning logs

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **haazybanj** 4 weeks ago

**Selected Answer: B**

The correct answer is B. sign-in logs.

Sign-in logs provide information about all sign-in attempts to Microsoft Defender for Cloud Apps, including successful and unsuccessful sign-in attempts. By reviewing the sign-in logs, you can identify the cause of the error message that User1 is receiving.

upvoted 1 times

 **AlfaExamPro** 1 month, 1 week ago

Correct, Sign-in Logs for Msft Defender for Cloud Apps

upvoted 1 times

 **rohitrc8521** 1 month, 4 weeks ago

absolutely correct

upvoted 2 times

 **ServerBrain** 3 months, 1 week ago

**Selected Answer: B**

Correct

upvoted 3 times

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps and Yammer.

You need prevent users from signing in to Yammer from high-risk locations.

What should you do in the Microsoft Defender for Cloud Apps portal?

- A. Create an access policy.
- B. Create an activity policy.
- C. Unsanction Yammer.
- D. Create an anomaly detection policy.

**Correct Answer: A**

*Community vote distribution*

A (67%)

D (33%)

✉ **Nyamnyam** 3 weeks, 6 days ago

OK, it sounds a bit heretical, but:  
I can configure named locations for high-risk countries and create a CAP for Yammer cloud app specifically.  
Where is this setting in Defender Cloud Apps? I can configure Cloud Apps access policy and specify Location, but I cannot specify Yammer as the only target app in scope.

upvoted 1 times

✉ **JimboJones99** 1 month, 2 weeks ago

**Selected Answer: A**

A - Access Policy

upvoted 1 times

✉ **Anonymous1312** 1 month, 3 weeks ago

**Selected Answer: D**

Anomaly detection

as per:

<https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy>

upvoted 1 times

✉ **Anonymous1312** 1 month, 3 weeks ago

disregard my comment.

Given answer is CORRECT.

Not anomaly detection between that does not prevent users from signing-in! '

upvoted 1 times

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

**Selected Answer: A**

correct

upvoted 1 times

✉ **1c67a2c** 4 months ago

seems correct <https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad>

upvoted 1 times

✉ **Anonymous1312** 1 month, 3 weeks ago

I would say in MCAS this is part of Conditional Access policies, rather than threat detection. The keyword in the question being "risky". Hence I would go for D "Anomaly Detection" since that covers locations and risky IPs, as per the documentation

<https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy>

upvoted 1 times

✉ **Anonymous1312** 1 month, 3 weeks ago

disregard my comment.

Given answer is CORRECT.

Not anomaly detection between that does not prevent users from signing-in! '

upvoted 1 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. SMS
- B. email
- C. security questions
- D. a verification code from the Microsoft Authenticator app

**Correct Answer: D**

*Community vote distribution*

D (67%)

A (33%)

 **MacDanorld** 2 weeks, 6 days ago

**Selected Answer: A**

The correct answer is A

upvoted 1 times

 **ServerBrain** 3 months, 1 week ago

**Selected Answer: D**

i think this is appearing for the 5th time.

upvoted 2 times

You have an Azure Active Directory (Azure AD) tenant.

You open the risk detections report.

Which risk detection type is classified as a user risk?

- A. impossible travel
- B. anonymous IP address
- C. malicious IP address
- D. Azure AD threat intelligence

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **ServerBrain** 3 months, 1 week ago

**Selected Answer: D**

corrcet

upvoted 1 times

 **Charlie33** 3 months, 3 weeks ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: D**

Correct Answer: D

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant.

You configure self-service password reset (SSPR) by using the following settings:

- Require users to register when signing in: Yes
- Number of methods required to reset: 1

What is a valid authentication method available to users?

- A. an email to an address outside your organization
- B. a mobile app notification
- C. an FIDO2 security token
- D. an email to an address in your organization

**Correct Answer: A**

*Community vote distribution*

A (63%)

B (38%)

✉️ **MacDanorld** 2 weeks, 6 days ago

**Selected Answer: A**

A is correct.

Mobile app notification is not available when one method is required for SSPR

upvoted 1 times

✉️ **norkis97** 1 month ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#mobile-app-and-sspr>

"When administrators require one method be used to reset a password, verification code is the only option available." Cit. Microsoft Doc  
upvoted 1 times

✉️ **Nyamnyam** 3 weeks, 6 days ago

OMG, we had this question 1000 times.

To summarize:

Notification is not Code.

When you require only 1 method it gets tricky based on what other auth methods the admin has allowed.

But in general, if you have enabled Mobile Code AND Email, the Code will win.

BUT if the questions asks you to select between Notification and Email, well the only possible answer is Email.

upvoted 2 times

✉️ **Obyte** 1 month, 2 weeks ago

**Selected Answer: A**

All available authentication methods are

Mobile app notification

Mobile app code

Email

Mobile phone

Office phone

Security questions

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#authentication-methods>

However, when only one authentication method is required the option for Mobile App Notification is grayed out. From the left options though only one matching is email and it cannot be the internal org email, so it leaves us with A.

upvoted 2 times

✉️ **syougun200x** 2 months, 2 weeks ago

Is there any chance this question is out of date? Anyone tested in their lab?

As long as I saw, SMS, Auth app and email is all available once each of them is registered as the account's auth method.

upvoted 1 times

✉️ **Wicke** 2 months, 3 weeks ago

**Selected Answer: B**

B: According to MS: <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#mobile-app-and-sspr>

upvoted 1 times

 **Anonymous1312** 2 months, 2 weeks ago

the question says 1 method. The documentation says only code is available then.

Clearly A

upvoted 2 times

 **Leon1969** 2 months, 3 weeks ago

It's B: "When administrators require one method be used to reset a password, verification code is the only option available."  
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

upvoted 1 times

 **Leon1969** 2 months, 1 week ago

Sorry, it must be A as B is app NOTIFICATION...

upvoted 1 times

 **ServerBrain** 3 months, 1 week ago

**Selected Answer: B**

will go with B

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: A**

Correct answer

upvoted 2 times

Question #63

Topic 2

You have an Azure AD Tenant.

You configure self-service password reset (SSPR) by using the following settings:

- Require users to register when signing in: Yes
- Number of methods required to reset: 1

What is a valid authentication method available to users?

- A. an FIDO2 security token
- B. a mobile app code
- C. a Microsoft Teams chat
- D. a Windows Hello PIN

**Correct Answer: B**

 **Anonymous1312** 1 month, 3 weeks ago

Correct

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#authentication-methods>

upvoted 2 times

**HOTSPOT**

You have an Azure subscription.

From Entitlement management, you plan to create a catalog named Catalog1 that will contain a custom extension.

What should you create first, and what should you use to distribute Catalog1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

First create:

- A managed account
- An Azure Automation account
- An Azure logic app

Distribute Catalog1 by using:

- A playbook
- A workflow
- An access package

**Answer Area**

First create:

- A managed account
- An Azure Automation account
- An Azure logic app

Correct Answer:

Distribute Catalog1 by using:

- A playbook
- A workflow
- An access package

 **Anonymous1312** 1 month, 3 weeks ago

Seems to be correct:

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-logic-apps-integration>

upvoted 3 times

 **OrangeSG** 3 weeks, 4 days ago

Demo video on YouTube:

Creating Azure AD Entitlement Management Custom Extensions for Access Packages

[https://www.youtube.com/watch?v=tI1GZ\\_JGMBk&ab\\_channel=CloudIdentity%7CJefTek](https://www.youtube.com/watch?v=tI1GZ_JGMBk&ab_channel=CloudIdentity%7CJefTek)

upvoted 2 times

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

| Name  | Role                   |
|-------|------------------------|
| User1 | User Administrator     |
| User2 | Password Administrator |
| User3 | Security Reader        |
| User4 | User                   |

You enable self-service password reset (SSPR) for all the users and configure SSPR to require security questions as the only authentication method.

Which users must use security questions when resetting their password?

- A. User4 only
- B. User3 and User4 only
- C. User1 and User4 only
- D. User1, User3, and User4 only
- E. User1, User2, User3, and User4

**Correct Answer: B**

*Community vote distribution*

B (88%) 13%

 **0byte** Highly Voted 1 month, 2 weeks ago

**Selected Answer: B**

Correct answer.

Basically, some administrative roles, by design can only use strong, two-gate password reset policy, regardless of SSPR settings. User Administrator and Password Administrator will be always forced to use two methods and cannot use security questions.

Security Reader and User will use whatever is set under SSPR, so security questions in this case.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences>  
upvoted 5 times

 **be9z** Most Recent 1 week, 5 days ago

Administrator accounts can't use security questions as verification method with SSPR. Answer is B. <https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-security-questions>

upvoted 1 times

 **Naya24** 2 weeks, 3 days ago

**Selected Answer: B**

Security reader not listed in 2 gate admin accounts

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy#administrator-reset-policy-differences>  
upvoted 1 times

 **haazybanj** 2 weeks, 3 days ago

**Selected Answer: A**

Shouldn't it be A since Security Reader is an Admin and Admins can't use security questions?

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-security-questions>  
upvoted 1 times

 **Nivos23** 1 month ago

**Selected Answer: B**

I agree with 0byteThe answer is b

upvoted 1 times

 **Lekong** 1 month, 2 weeks ago

I think it should be Username only

upvoted 1 times

 **Lekong** 1 month, 2 weeks ago

I mean User 4 only. A  
upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

Administrator accounts can't use security questions as verification method with SSPR.  
upvoted 1 times

 **Trappie** 2 months ago

Correct:  
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-security-questions>  
upvoted 1 times

Question #66

*Topic 2*

You have an Azure AD tenant.

You need to implement smart lockout with a lockout threshold of 10 failed sign-ins.

What should you configure in the Azure AD admin center?

- A. Authentication strengths
- B. Password protection
- C. User risk policy
- D. Sign-in risk policy

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **0byte** 1 month, 2 weeks ago

**Selected Answer: B**

Correct answer.  
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout#manage-microsoft-entra-smart-lockout-values>  
upvoted 2 times

 **e1ec325** 1 month, 4 weeks ago

**Selected Answer: B**

Correct  
upvoted 1 times

You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.

You need to ensure that you can control access to Microsoft 365 resources by using conditional access policies.

What should you do first?

- A. Disable Security defaults.
- B. Configure password protection for the Azure AD tenant.
- C. Configure a multi-factor authentication (MFA) registration policy.
- D. Disable the User consent settings.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 JimboJones99 1 month, 2 weeks ago

**Selected Answer: A**

Correct as the tenant is new and security defaults will be on by default.

upvoted 2 times

You have a Microsoft 365 tenant.

An on-premises Active Directory domain is configured to sync with the Azure AD tenant. The domain contains the servers shown in the following table.

| Name    | Operating system    | Configuration     |
|---------|---------------------|-------------------|
| Server1 | Windows Server 2019 | Domain controller |
| Server2 | Windows Server 2016 | Domain controller |
| Server3 | Windows Server 2019 | Azure AD Connect  |

The domain controllers are prevented from communicating to the internet.

You implement Azure AD Password Protection on Server1 and Server2.

You deploy a new server named Server4 that runs Windows Server 2022.

You need to ensure that Azure AD Password Protection will continue to work if a single server fails.

What should you implement on Server4?

- A. Azure AD Connect
- B. Azure AD Application Proxy
- C. Password Change Notification Service (PCNS)
- D. the Azure AD Password Protection proxy service

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **0byte** 1 month, 1 week ago

**Selected Answer: D**

Correct answer

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad-on-premises#how-microsoft-entra-password-protection-works>

upvoted 2 times

 **JCkD4Ni3L** 1 month, 1 week ago

**Selected Answer: D**

Answer is correct.

upvoted 3 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. voice
- B. email
- C. security questions
- D. a verification code from the Microsoft Authenticator app

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **JcKD4Ni3L** 1 month, 1 week ago

**Selected Answer: D**

Correct Answer, since there is no internet on mobile devices the only method available is the authenticator code.

upvoted 1 times

## HOTSPOT

You have an Azure subscription that contains the resources shown in the following table.

| Name   | Type            |
|--------|-----------------|
| User1  | User            |
| User2  | User            |
| Vault1 | Azure Key Vault |

You need to configure access to Vault1. The solution must meet the following requirements:

- Ensure that User1 can manage and create keys in Vault1.
- Ensure that User2 can access a certificate stored in Vault1.
- Use the principle of least privilege.

Which role should you assign to each user? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

User1:

Key Vault Certificates Officer

Key Vault Crypto Officer

Key Vault Secrets Officer

User2:

Key Vault Certificates Officer

Key Vault Crypto Officer

Key Vault Secrets Officer

## Answer Area

Correct Answer:

User1:

Key Vault Certificates Officer

**Key Vault Crypto Officer**

Key Vault Secrets Officer

User2:

**Key Vault Certificates Officer**

Key Vault Crypto Officer

Key Vault Secrets Officer

penatuna 1 month ago

Correct.

Key Vault Certificates Officer  
DataActions:  
- Microsoft.KeyVault/vaults/certificates/\*  
- Microsoft.KeyVault/vaults/certificates/\*  
- Microsoft.KeyVault/vaults/certificatecontacts/write

Key Vault Crypto Officer

DataActions:

- Microsoft.KeyVault/vaults/keys/\*
- Microsoft.KeyVault/vaults/keyrotationpolicies/\*

Key Vault Secrets Officer

DataActions:

- Microsoft.KeyVault/vaults/secrets/\*

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#key-vault-certificates-officer>

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#key-vault-crypto-officer>

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#key-vault-secrets-officer>

upvoted 1 times

 **JCKD4Ni3L** 1 month, 1 week ago

Correct

upvoted 1 times

 **AK\_1234** 1 month, 3 weeks ago

- Key Vault Crypto Officer
- Key Vault Certificates Officer

upvoted 1 times

 **Julesy** 1 month, 4 weeks ago

Looks good according to docs: <https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide#azure-built-in-roles-for-key-vault-data-plane-operations>

User1: manage and create keys in Vault1 - Key Vault Crypto Officer

User2: access a certificate stored in Vault1 - Key Vault Certificates Officer

upvoted 4 times

You have an Azure AD tenant that has multi-factor authentication (MFA) enforced and self-service password reset (SSPR) enabled.

You enable combined registration in interrupt mode.

You create a new user named User1.

Which two authentication methods can User1 use to complete the combined registration process? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. a FIDO2 security key
- B. a hardware token
- C. a one-time passcode email
- D. Windows Hello for Business
- E. the Microsoft Authenticator app

**Correct Answer: CE**

*Community vote distribution*

AE (57%)

CE (43%)

 **Nyamnyam** 3 weeks, 5 days ago

AE is NOT correct. CE is the only possibility. Why?

- A. FIDO2 security keys, can only be added in Manage mode
- B. Hardware tokens cannot be used in combined registration.
- C. Windows Hello for business cannot be used in combined registration. In fact, this is a passwordless authentication platform (with PIN and biometric methods)

Read the table and the Notes sections here:

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-registration-mfa-sspr-combined#methods-available-in-combined-registration>

upvoted 2 times

 **penatuna** 1 month ago

**Selected Answer: CE**

- A. FIDO2 security keys, can only be added in Manage mode. Question says "You enable combined registration in interrupt mode."
- B. Hardware token – You cannot register with hardware token.
- C. Email is supported.
- D. Windows Hello for Business is not supported.
- E. Microsoft Authenticator app is supported.

upvoted 3 times

 **JcKD4Ni3L** 1 month, 1 week ago

**Selected Answer: AE**

As per Microsoft's documentation, A and E in the available choices.

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-registration-mfa-sspr-combined#methods-available-in-combined-registration>

upvoted 1 times

 **JcKD4Ni3L** 1 month, 1 week ago

I stand corrected, A is not valid, as stated by others, FIDO2 security keys, can only be added in Manage mode on <https://aka.ms/mysecurityinfo>. So correct Answer would be C & E.

upvoted 1 times

 **syougun200x** 1 month, 3 weeks ago

I think the answer C & E is correct.

On the link page, it goes like this.

FIDO2 security keys, can only be added in Manage mode on <https://aka.ms/mysecurityinfo>.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-registration-mfa-sspr-combined>

Meaning I think through the combined registration process the user cannot choose FIDO2 but only on their own 365 security page.

upvoted 2 times

□  **cgonIT** 1 month, 3 weeks ago

As per the official documentation: <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-registration-mfa-sspr-combined>

- Hardware token is not an option to register.
- a one-time passcode email is not even listed.
- Windows Hello for Business is not even listed.

Correct responses:

- A. a FIDO2 security key
- E. the Microsoft Authenticator app

upvoted 3 times

□  **JimboJones99** 1 month, 2 weeks ago

Agree with this based off the documentation

upvoted 1 times

□  **666Forest** 2 months ago

**Selected Answer: AE**

A. a FIDO2 security key: Users can use a FIDO2 security key, which is a hardware device that provides strong authentication, typically in the form of a USB key or a biometric-enabled key.

E. the Microsoft Authenticator app: Users can use the Microsoft Authenticator app, which supports multi-factor authentication (MFA) and can generate one-time passcodes or be used for push notifications for MFA approval.

So, User1 can use these two methods to complete the combined registration process.

upvoted 3 times

## DRAG DROP

You have an Azure AD tenant that contains a user named Admin1.

Admin1 uses the Require password change for high-risk users policy template to create a new Conditional Access policy.

Who is included and excluded by default in the policy assignment? To answer, drag the appropriate options to the correct target. Each option 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

**Options**

Admin1

All guest and external users

All users

Directory roles

None

**Answer Area**

Include:

Exclude:

**Answer Area**

Correct Answer: Include: All users

Exclude: None

 **penatuna** Highly Voted 1 month ago

Include: All users

Exclude: Admin1

These are the settings for the Require Password Change for High-Risk Users template:  
Users: All Users are Included – The current user creating the policy will be excluded

Apps: All apps

User Risk: Risk levels: High

Access Control: Grant access – Require multifactor authentication AND Require password change

Conditional Access template policies will exclude only the user creating the policy from the template. If your organization needs to exclude other accounts, you will be able to modify the policy once they are created. You can find these policies in the Microsoft Entra admin center > Protection > Conditional Access > Policies. Select a policy to open the editor and modify the excluded users and groups to select accounts you want to exclude.

<https://scmentor.com/2023/03/26/just-dropped-in-to-see-what-condition-my-conditional-access-rule-was-in-part-6-require-password-change-for-high-risk-users/>

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policy-common?tabs=zero-trust#template-categories>

upvoted 5 times

 **Nyamnyam** 3 weeks, 5 days ago

Nice catch!

upvoted 1 times

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

-All users

-All guest and external users

My thinking:

The reason for excluding these is because they login with external credentials! We do not manage their identity and therefore cannot enforce a PW reset?

Also in the real world I would exclude the breakglass account also (as mentioned in ms documentation)  
upvoted 1 times

 **AK\_1234** 1 month, 1 week ago

- All users
  - All guest and external users
- upvoted 2 times

 **F\_Dias** 1 month, 2 weeks ago

The correct is:

Include: All Users

Exclude: Current User (Admin1 in this example)

upvoted 3 times

 **DasChi\_cken** 1 month, 3 weeks ago

All User & none... Microsoft even warns you in their Docs to Test CAPs in Report only Mode before you Lock yourself Out

And logically If you say all User in the First place you cant say anything Else the none as 2nd answer because the First answer wouldnt be all the ;)  
upvoted 2 times

 **AK\_1234** 1 month, 3 weeks ago

- All users
  - All guest and external users
- upvoted 1 times

 **cgonIT** 1 month, 3 weeks ago

Wrong answer.

Include: All Users

Exclude: Current User (Admin1 in this case)

Tested in lab.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk-user>  
upvoted 4 times

 **agittunc** 1 month, 1 week ago

This is wrong, your link also doesn't say admin is excluded.

All users

guest/external as they are not managed by the specific tenant.

upvoted 1 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. SMS
- B. Windows Hello for Business
- C. voice
- D. a notification through the Microsoft Authenticator app

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **JCkD4Ni3L** 1 month, 1 week ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **cgonIT** 1 month, 3 weeks ago

B. Windows Hello for Business.

It's the only option when no internet connectivity or access to a mobile phone device.

upvoted 2 times

You have a Microsoft 365 tenant.

You currently allow email clients that use Basic authentication to connect to Microsoft Exchange Online.

You need to ensure that users can connect to Exchange Online only from email clients that use Modern authentication protocols.

What should you implement?

- A. a conditional access policy in Azure AD
- B. a compliance policy in Microsoft Intune
- C. an OAuth policy in Microsoft Defender for Cloud Apps
- D. an application control profile in Microsoft Intune

**Correct Answer: D**

*Community vote distribution*

A (100%)

 **Nyamnyam** 3 weeks, 5 days ago

**Selected Answer: A**

Exactly. A. And in the previous occurrence, we clarified that "app control" is for approved apps. This will not block basic auth from, e.g. personal computers ;)

upvoted 1 times

 **0byte** 1 month, 1 week ago

**Selected Answer: A**

Agree. A is the correct answer

<https://learn.microsoft.com/en-gb/entra/identity/conditional-access/howto-conditional-access-policy-block-legacy>

upvoted 1 times

 **JCkD4Ni3L** 1 month, 1 week ago

**Selected Answer: A**

A, Conditional Access Policy that blocks Legacy Authentication Clients apps (Exchange ActiveSync and Other clients).

upvoted 1 times

 **JimboJones99** 1 month, 2 weeks ago

**Selected Answer: A**

a conditional access policy in Azure AD

upvoted 2 times

 **DasChi\_cken** 1 month, 3 weeks ago

**Selected Answer: A**

Should be A, this question was mentioned a couple of questions before as well

upvoted 2 times

 **666Forest** 1 month, 3 weeks ago

**Selected Answer: A**

The correct answer is A

upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

The correct answer is A. a conditional access policy in Azure AD.

upvoted 1 times

You plan to deploy a new Azure AD tenant.

Which multifactor authentication (MFA) method will be enabled by default for the tenant?

- A. Microsoft Authenticator
- B. SMS
- C. voice call
- D. email OTP

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉ **iduard15** 3 weeks, 1 day ago

D, OTP email

upvoted 1 times

✉ **penatuna** 1 month ago

**Selected Answer: A**

It's a new Azure tenant, so security defaults are enabled. With security defaults, Microsoft Authenticator is the default authentication method.

"Security defaults users are required to register for and use multifactor authentication using the Microsoft Authenticator app using notifications. Users might use verification codes from the Microsoft Authenticator app but can only register using the notification option. Users can also use any third party application using OATH TOTP to generate codes."

<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#authentication-methods>

upvoted 1 times

✉ **JCkD4Ni3L** 1 month, 1 week ago

**Selected Answer: A**

Security Defaults are usually turned on on new tenants, therefore Microsoft Authenticator is the correct Answer.

upvoted 1 times

✉ **rikiem** 1 month, 3 weeks ago

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

upvoted 1 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      |
|-------|----------------|
| User1 | Group1         |
| User2 | Group2         |
| User3 | Group1, Group2 |

The users have the devices shown in the following table.

| Name    | Platform   | Azure AD join type  |
|---------|------------|---------------------|
| Device1 | Windows 11 | None                |
| Device2 | Windows 10 | Azure AD joined     |
| Device3 | Android    | Azure AD registered |

You create the following two Conditional Access policies:

- Name: CAPolicy1
- 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: Block access
      - Session: 0 controls selected
      - Enable policy: On

- Name: CAPolicy2
- Assignments
  - Users or workload identities: Group2
  - Cloud apps or actions: Office 365 SharePoint Online
  - Conditions: 0 conditions selected
  - Access controls
    - Grant: Grant access
    - Require multifactor authentication
    - Session: 0 controls selected
    - Enable policy: On

All users confirm that they can successfully authenticate using MFA.

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

NOTE: Each correct selection is worth one point.

### Statements

User1 can access Site1 from Device1.

Yes

No

User2 can access Site1 from Device2.

User3 can access Site1 from Device3.

店铺：专业认证88

店铺：专业认证88

### Statements

User1 can access Site1 from Device1.

Yes

No

Correct Answer:

User2 can access Site1 from Device2.

Yes

No

User3 can access Site1 from Device3.

Florian74 Highly Voted 1 month, 2 weeks ago

If the CAPolicy1 included the filtered devices it would be YNY. But the policy exclude them. So YYY for me  
upvoted 6 times

Sorrynotsorry Most Recent 2 weeks, 6 days ago

NYY. CAP1 can't read device1 name so will block access.  
upvoted 1 times

Nyamnyam 3 weeks, 5 days ago

YYY definitely. Consider this:  
CAP1 is a blocking policy, but with Exclusion condition. This is very clear: any device from Group1 will be blocked, EXCEPT the ones starting with "Device". Haha, User1 and 3 are thus always allowed no matter the device join type or compliance state.  
CAP2 is a simple MFA enforcement policy for Group2. User2 will be able to access the site (once he was registered for MFA) independent from what device (1,2,3) he accesses Site2.  
Trust me, I work with CAPs in real life for years.  
upvoted 3 times

Peeeedor 1 month ago

I am a little confused? How can user 1 be in group 1 and successfully using MFA while not being entra ID joined or registered?  
upvoted 1 times

Nivos300 4 weeks ago

I agree with you .

In my opinion the answer is

N

Y

Y

upvoted 1 times

vaaws 1 month ago

Azure Conditional Access policies can only apply to devices that are registered or joined in Azure Active Directory. If a device is not registered or joined, the policy will not be able to read the device name.  
N Y Y  
upvoted 2 times

Obyte 1 month, 1 week ago

Hmm... NYY for me  
Here is my thinking - have to say haven't tested it yet :-)

User1 will be blocked because its device is neither AzureAD-joined nor Registered and device's name cannot be evaluated. The CAPolicy1 will block it.

User2 will be allowed as it doesn't fall under any of the two policies.

User3 will be excluded from blocking by CAPolicy1 (because of device name) and will be allowed by CAPolicy2 because of membership in Group2.

upvoted 1 times

□ **JCKD4Ni3L** 1 month, 1 week ago

YYY, as all devices are "excluded" from CAPolicy1, and since CAPolicy2 only triggers MFA, all users can access from any devices through MFA.  
upvoted 1 times

□ **MarkElliott** 1 month, 1 week ago

Wrong, look at the Syntax rule, exclude device name that starts with Device.

Correct answer given

upvoted 1 times

□ **MarkElliott** 1 month, 1 week ago

Infact just checked, it says exclude devices from the rule, so it is YYY

upvoted 2 times

□ **JCKD4Ni3L** 1 month, 1 week ago

Hmm since Device1 has no Azure AD joined/Registered state it cannot report it's name and will be blocked by CAPolicy1. I would there force state NYY.

upvoted 2 times

□ **DasChi\_cken** 1 month, 3 weeks ago

User1 and User3 are in group1 and there devicenames Starts with "Device" --- Access blocked

User2 IS in group2 and will only ne prompt to MFA

upvoted 1 times

□ **Intrudire** 1 month, 2 weeks ago

Devices that start with "Device" are excluded from being blocked:

Filter for devices: Exclude filtered devices from the policy

Rule syntax: device.displayName -startsWith "Device"

upvoted 2 times

□ **shuhaidawahab** 1 month, 3 weeks ago

Explanation:

User1 is a member of Group1, which is assigned to CAPolicy1. This policy blocks access to SharePoint Online for any device that starts with "Device". Since Device1 has this prefix, User1 cannot access Site1 from Device1.

User2 is a member of Group2, which is assigned to CAPolicy2. This policy grants access to SharePoint Online with MFA for any device. Since User2 has confirmed MFA, they can access Site1 from Device2.

User3 is not a member of any group that is assigned to a Conditional Access policy. Therefore, they have the default access level to SharePoint Online, which is none. User3 cannot access Site1 from Device3.

upvoted 1 times

□ **cgonIT** 1 month, 3 weeks ago

At the very beginning I was telilng N, N, N. But then I decided to test in lab.

- Created 2 AAD Security user groups.
- Created 3 users, and added to ech group.
- Created 2 Conditional Access.

Tested with WhatIf... and that's surprised me.

Y, Y, Y.

- User 1, no Conditional Access is detected to be applied.
- User 2 and 3, MFA will be required.

So all 3 are Yes.

upvoted 1 times

□ **agittunc** 1 month, 1 week ago

you do realize that device 1 isn't even AD joined right?

N, Y, Y

upvoted 2 times

You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3 and a Microsoft SharePoint Online site named Site1.

The subscription contains the devices shown in the following table.

| Name    | Azure AD   | Compliance     |
|---------|------------|----------------|
| Device1 | Joined     | Noncompliant   |
| Device2 | Registered | Compliant      |
| Device3 | None       | Not applicable |

The users sign in to the devices as shown in the following table.

| User  | Device  |
|-------|---------|
| User1 | Device1 |
| User2 | Device2 |
| User3 | Device3 |

You have a Conditional Access policy that has the following settings:

- Name: CA1
- Assignments
  - Users and groups: User1, User2, User3
  - Cloud apps or actions: SharePoint - Site1
- Access controls
  - Session: Use app enforced restrictions

From the SharePoint admin center, you configure Access control for unmanaged devices to allow limited, web-only access.

Which users will have full access to Site1?

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

**Correct Answer: B**

*Community vote distribution*

A (75%)

B (25%)

 **jibrandes** 2 weeks, 4 days ago

**Selected Answer: A**

Only Joined devices are managed.

<https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-managed-unmanaged-devices?view=o365-worldwide&tabs=Managed>

upvoted 3 times

 **Nivos300** 4 weeks ago

**Selected Answer: B**

B. User2 only

Here's the reasoning:

The Conditional Access policy (CA1) is assigned to User1, User2, and User3. The policy's access control is set to "Session: Use app enforced restrictions." Now, let's look at the device compliance status and user-device assignments:

Device1 is joined but noncompliant.

Device2 is registered and compliant.

Device3 is none (not applicable).

Since the access control is set to "Session: Use app enforced restrictions," unmanaged or noncompliant devices will have limited, web-only access.

Device1 is noncompliant, so User1 (Device1) will have limited access. Device3 is not applicable, so User3 (Device3) is not relevant to this scenario.

upvoted 2 times

✉️ **Nivos300** 4 weeks ago

Continued

User2 (Device2) is using a registered and compliant device, so User2 will have full access to Site1.

Therefore, User2 (full access) will be the only user with full access to Site1, while User1 and User3 will have limited access or not be affected by the Conditional Access policy.

upvoted 1 times

✉️ **vaww** 1 month ago

The users who will have full access to Site1 are User1 and User2 only. The Conditional Access policy is configured to include User1, User2, and User3, but the Access control for unmanaged devices in the SharePoint admin center allows only limited, web-only access. Therefore, only User1 and User2, who sign in from managed devices, will have full access to Site1.

The correct answer is D. User1 and User2 only.

upvoted 4 times

✉️ **JckD4Ni3L** 1 month, 1 week ago

**Selected Answer: A**

Only User1 will have full access since Device1 is the only Azure AD Joined device (Managed)

upvoted 3 times

✉️ **einkaufacs** 1 month, 1 week ago

A registered device, which is also integrated and compliant in Intune should work here. So the answer seems plausible to me.

<https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

upvoted 1 times

✉️ **Intrudire** 1 month, 2 weeks ago

None of them?

"you can block or limit access to SharePoint and OneDrive content from unmanaged devices (those not hybrid AD joined or compliant in Intune)"

<https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

upvoted 2 times

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

| Name      | Description               |
|-----------|---------------------------|
| Au1       | Administrative unit       |
| CAPolicy1 | Conditional Access policy |
| Package1  | Access package            |

You create a user named Admin1.

You need to ensure that Admin1 can enable Security defaults for contoso.com.

What should you do first?

- A. Delete Package1.
- B. Delete CAPolicy1.
- C. Assign Admin1 the Authentication Administrator role for Au1.
- D. Configure Identity Governance.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **OrangeSG** 3 weeks, 1 day ago

**Selected Answer: B**

To configure security defaults in your directory, you must be assigned at least the Security Administrator role. By default the first account in any directory is assigned a higher privileged role known as Global Administrator.

Organizations that choose to implement Conditional Access policies that replace security defaults must disable security defaults. (Imply that Conditional Access policies has conflict with security defaults)

<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>

upvoted 1 times

 **dumpsowner** 1 month, 1 week ago

Answer: B is correct.

DumpsOwner : The study material that I have used has been excellent. It is well-written, organized, and informative. The material covers all of the topics that I need to know in a comprehensive and easy-to-understand way.

upvoted 1 times

 **JCkD4Ni3L** 1 month, 1 week ago

**Selected Answer: B**

B is Correct.

upvoted 1 times

 **DasChi\_cken** 1 month, 3 weeks ago

**Selected Answer: B**

To enable capolicies you need to disable Security defaults therefore you need to do it viceversa If you want to Go back to Security defaults  
upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

The correct answer is B. Delete CAPolicy1.

To enable Security defaults for contoso.com, Admin1 must be assigned at least the Security Administrator role1. However, this role is not available in the list of roles for Au1, which is the only authentication method for contoso.com. This is because Au1 has a Conditional Access policy named CAPolicy1 that blocks legacy authentication protocols2. Security defaults also block legacy authentication protocols, so they cannot be enabled if there is an existing Conditional Access policy that does the same3.

Therefore, to enable Security defaults, Admin1 must first delete CAPolicy1 from Au1. This will allow Admin1 to sign in to contoso.com using a legacy authentication protocol and then assign themselves the Security Administrator role. After that, Admin1 can enable Security defaults for contoso.com.

upvoted 1 times

 **dumps4azure** 1 month, 3 weeks ago

Answer: B is correct.

Dumps4Azure SC-300 PDFs helped me ace my certification exam. Their verified questions and answers were spot on!

upvoted 2 times

 **cgonIT** 1 month, 3 weeks ago

**Selected Answer: B**

A. Delete Package1 --> no sense for me.

C. Assign Admin1 the Authentication Administrator role for Au1. --> The role needed on that case, is Security Administrator role.

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/security-defaults#enabling-security-defaults>

D. Configure Identity Governance. --> no sense for me.

So B. Delete CAPolicy1 is the correct one.

upvoted 1 times

 **LC\_90** 2 months ago

**Selected Answer: B**

Correct

upvoted 2 times

## DRAG DROP

You have an Azure subscription that is linked to an Azure AD tenant named contoso.com. The subscription contains a group named Group1 and a virtual machine named VM1.

You need to meet the following requirements:

- Enable a system-assigned managed identity for VM1.
- Add VM1 to Group1.

How should you complete the PowerShell script? To answer, drag the appropriate cmdlets to the correct targets. Each cmdlet 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.

## Cmdlets

```
Get-AzADGroup
Get-AzADServicePrincipal
Get-AzVM
Update-AzADServicePrincipal
Update-AzVM
```

## Answer Area

```
$vm = [Cmdlet] -ResourceGroupName myResourceGroup -Name vm1
Update-AzVM -ResourceGroupName myResourceGroup -VM $vm -IdentityType SystemAssigned
$displayname = [Cmdlet] -displayname "vm1"
$group = Get-AzADGroup -searchstring "group1"
Add-AzureADGroupMember -ObjectId $group.id -RefObjectId $displayname.id
```

## Correct Answer:

```
Answer Area
$vm = [Get-AzVM] -ResourceGroupName myResourceGroup -Name vm1
Update-AzVM -ResourceGroupName myResourceGroup -VM $vm -IdentityType SystemAssigned
$displayname = [Get-AzADServicePrincipal] #displayname "vm1"
$group = Get-AzADGroup -searchstring "group1"
Add-AzureADGroupMember -ObjectId $group.id -RefObjectId $displayname.id
```

 **Studytime2023** 1 day ago

Correct. <https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/qs-configure-powershell-windows-vm>  
upvoted 1 times

 **DasChi\_cken** 1 month, 3 weeks ago

Its correct, you want to save the Powershell objects in a variable first and Last step is Putting all things together  
upvoted 2 times

 **cgonIT** 1 month, 3 weeks ago

Seems to be correct.

- Get-AzVM  
- Get-AzADServicePrincipal  
upvoted 3 times

You have an Azure AD tenant.

You deploy a new enterprise application named App1.

When users attempt to provide App1 with access to the tenant, the attempt fails.

You need to ensure that the users can request admin consent for App1. The solution must follow the principle of least privilege.

What should you do first?

- A. Enable admin consent requests for the tenant.
- B. Designate a reviewer of admin consent requests for the tenant.
- C. From the Permissions settings of App1, grant App1 admin consent for the tenant.
- D. Create a Conditional Access policy for App1.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 haazybanj 1 month ago

**Selected Answer: A**

To ensure that users can request admin consent for App1 in your Azure AD tenant, you should first enable admin consent requests for the tenant.

Enabling admin consent requests allows users to initiate the process of requesting admin consent for applications that require it. By default, users do not have the ability to grant admin consent for applications. Enabling this feature ensures that users can request admin consent for App1 without having to rely on an administrator to initiate the process.

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.

You have a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Azure Active Directory admin center, you configure the Block/unblock users settings for multi-factor authentication (MFA).

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **OrangeSG** 3 weeks, 1 day ago

**Selected Answer: B**

Report suspicious activity and the legacy Fraud Alert implementation can operate in parallel. You can keep your tenant-wide Fraud Alert functionality in place while you start to use Report suspicious activity with a targeted test group.

If Fraud Alert is enabled with Automatic Blocking, and Report suspicious activity is enabled, the user will be added to the blocklist and set as high-risk and in-scope for any other policies configured. These users will need to be removed from the blocklist and have their risk remediated to enable them to sign in with MFA.

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-mfasettings#report-suspicious-activity-and-fraud-alert>  
upvoted 1 times

 **haazybanj** 1 month ago

**Selected Answer: B**

To meet the goal of automatically blocking users when they report an unauthorized MFA request, you would need to implement additional measures such as monitoring and alerting, conditional access policies, or security policies to detect and respond to suspicious MFA activity.

Therefore, the correct answer is B. No.

upvoted 1 times

**Topic 3 - Question Set 3**

**HOTSPOT -**

You have a Microsoft 365 tenant and an Active Directory domain named adatum.com.

You deploy Azure AD Connect by using the Express Settings.

You need to configure self-service password reset (SSPR) to meet the following requirements:

- ☞ When users reset their password, they must be prompted to respond to a mobile app notification or answer three predefined security questions.

- ☞ Passwords must be synced between the tenant and the domain regardless of where the password was reset.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

From the Password reset blade in the Azure Active Directory admin center, configure:

|                        |
|------------------------|
| Authentication methods |
| Notifications          |
| Properties             |
| Registration           |

From Azure AD Connect, enable:

|                                                              |
|--------------------------------------------------------------|
| Federation with Active Directory Federation Services (AD FS) |
| Pass-through authentication                                  |
| Password hash synchronization                                |
| Password writeback                                           |

Correct Answer:

**Answer Area**

From the Password reset blade in the Azure Active Directory admin center, configure:

|                        |
|------------------------|
| Authentication methods |
| Notifications          |
| Properties             |
| Registration           |

From Azure AD Connect, enable:

|                                                              |
|--------------------------------------------------------------|
| Federation with Active Directory Federation Services (AD FS) |
| Pass-through authentication                                  |
| Password hash synchronization                                |
| Password writeback                                           |

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-security-questions>

 **girikedar** Highly Voted 2 years ago

Both The Answer is Correct

- 1) You have Go to Azure active directory > under Manage section Password reset blade > Authentication methods & check the Security Questions
- 2) Inorder to sync password between Domain & tenant either you have to do password hash sync & Pass through authentication with password writeback enable in Azure Ad Connect.

upvoted 19 times

 **Jun143** Highly Voted 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 10 times

 **jimmyjose** 1 month, 2 weeks ago

Answering this particular question correctly or incorrectly does not dictate your exam result. Please refrain from answering this way; it adds no value to edam takers, please.

I request the moderator of examtopics from submitting such responses unless I am missing a point here.  
upvoted 1 times

✉ **g2s** 1 year, 5 months ago

useless comment  
upvoted 22 times

✉ **KrisDeb** 11 months, 3 weeks ago

No, it's not, I would like to know if the question showed up on the exam, that means it's not outdated and still relevant. Also, this shows the person made an effort AFTER the exam and shared it with us, not many people are doing that, I'm not, after the exam I'm not even looking here, so I appreciate someone else's efforts.

upvoted 24 times

✉ **jimmyjose** 2 months, 2 weeks ago

The fact that the candidate passed the exam does not translate to this particular question being correctly answered.  
upvoted 2 times

✉ **ThotSlayer69** 10 months, 1 week ago

They could have mentioned whether the given answer is correct or not, just weird that they went out of their way and put in 99% of the work just to give us 50% of the info desired. Adding on that extra part would take 10 seconds but really increase the value of their comment

upvoted 3 times

✉ **hellboycze** 9 months, 1 week ago

if he didn't hit 100% score he cannot be 100% sure  
upvoted 8 times

✉ **EmnCours** [Most Recent] 4 months, 1 week ago

1. Authentication methods  
2. Password writeback  
upvoted 3 times

✉ **dule27** 5 months, 2 weeks ago

1. Authentication methods  
2. Password writeback  
upvoted 1 times

✉ **Pedro2021** 11 months, 1 week ago

Correct  
upvoted 1 times

✉ **[Removed]** 11 months, 4 weeks ago

Answers are correct.  
upvoted 1 times

✉ **zmlapq99** 1 year, 10 months ago

On exam few days ago.  
upvoted 4 times

✉ **gills** 2 years, 4 months ago

Express install of AD Connect does not allow Password Write back as an option.  
Only Password Hash Sync is.

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-select-installation>  
upvoted 3 times

✉ **bizquit** 2 years, 3 months ago

Yes, but from the same link:  
Options where you can still use Express:  
You want to enable one of the features in Azure AD Premium, such as Password writeback. First go through express to get the initial installation completed. Then run the installation wizard again and change the configuration options.

Password hash sync is definitely not doing the sync between Azure and on-prem, the other answers are also not correct so it must be "Password Write Back"

upvoted 3 times

✉ **Bloembar** 2 years, 4 months ago

Incorrect express does support password writeback  
upvoted 5 times

✉ **cdizzle** 2 years, 3 months ago

The exhibit says "You deploy Azure AD Connect by using the Express Settings." I would take that to mean the actions you have to complete are done AFTER the successful deployment. Meaning you could then enable "Password Write Back".  
upvoted 7 times

✉ **melatocaroca** 2 years, 4 months ago

Questions can be used during the self-service password reset (SSPR) process to confirm who you are. Administrator accounts can't use security questions as verification method with SSPR.

When users register for SSPR, they're prompted to choose the authentication methods to use. If they choose to use security questions, they pick from a set of questions to prompt for and then provide their own answers.

Password writeback can be used to synchronize password changes in Azure AD back to your on-premises AD DS environment. Azure AD Connect provides a secure mechanism to send these password changes back to an existing on-premises directory from Azure AD.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-security-questions>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr-writeback>

upvoted 4 times

□ **ArielReyes27** 2 years, 5 months ago

Correct.

upvoted 1 times

□ **Domza** 2 years, 5 months ago

Also, Express setting in Azure Connect\* = password writeback

upvoted 1 times

□ **Domza** 2 years, 5 months ago

Nop, i take it back - Custom Settings = pass writeback

upvoted 3 times

□ **Sugarrose** 2 years, 3 months ago

Hello friend, do you have exam dump for sc300

upvoted 1 times

□ **AS007** 2 years, 6 months ago

Password writeback can be used to synchronize password changes in Azure AD back to your on-premises AD DS environment.

Answer look good

upvoted 1 times

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.

Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.

You plan to manage access to external applications by using Azure AD.

You need to use the firewall logs to create a list of unmanaged external applications and the users who access them.

What should you use to gather the information?

- A. Application Insights in Azure Monitor
- B. access reviews in Azure AD
- C. Cloud App Discovery in Microsoft Cloud App Security
- D. enterprise applications in Azure AD

**Correct Answer: C**

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports#using-traffic-logs-for-cloud-discovery>

Community vote distribution

C (100%)

 **zed01** Highly Voted 2 years, 6 months ago

C is correct according to the link provided.  
upvoted 9 times

 **tatendazw** 2 years, 1 month ago

Correct, <https://docs.microsoft.com/en-us/cloud-app-security/discovered-apps>  
upvoted 1 times

 **haazybanj** Most Recent 1 month ago

**Selected Answer: C**

To gather information about unmanaged external applications and the users who access them, you should use Cloud App Discovery in Microsoft Cloud App Security.

Cloud App Discovery is a feature of Microsoft Cloud App Security that allows you to discover and gain visibility into the cloud applications being used in your organization. It provides insights into the usage of both managed and unmanaged applications, including information about the users accessing those applications.

upvoted 1 times

 **EmnCours** 4 months, 1 week ago

**Selected Answer: C**

Correct Answer: C  
upvoted 1 times

 **OK2020** 5 months ago

A question to the wider community, why did you all thought of MCAS when teh questions says " need to use the firewall logs" referring to the on-prem FW appliance! The question didn't open teh door/option to use external FW service. In MPOV, it's teh Azure monitor that can used to collect logs from teh existing FW and analysed to achieve teh requesed outcome. Have a look at this link:

Can Azure Monitor also monitor on-premises resources?

Yes. In addition to collecting monitoring data from Azure resources, Azure Monitor can collect data from virtual machines and applications in other clouds and on-premises. See Sources of monitoring data for Azure Monitor.

<https://learn.microsoft.com/en-us/azure/azure-monitor/faq>

My suggested answer is" Azure Monitor"

upvoted 2 times

 **cgonIT** 1 month, 3 weeks ago

To add more information to your comment: <https://learn.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview?tabs=net>

"Firewall settings must be adjusted for data to reach ingestion endpoints". But here is the most reasonable answer. MCASB can only monitor accesses to "unmanaged external applications" but can't see on-prem FW logs, that is the question.

upvoted 1 times

 **dule27** 5 months, 2 weeks ago

**Selected Answer: C**

C. Cloud App Discovery in Microsoft Cloud App Security  
upvoted 1 times

 **ANDRESCB1988** 1 year ago

C is correct  
upvoted 1 times

 **estyj** 1 year, 1 month ago

Correct C: Cloud App Discovery in MCAS  
upvoted 1 times

 **brlojaexpress** 1 year, 3 months ago

MCAS is correct answer  
upvoted 1 times

 **kakakayayaya** 1 year, 6 months ago

It is Defender fro Cloud Apps now. Does MS still use legacy name in exam?  
upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022  
upvoted 1 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.  
upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022  
upvoted 2 times

 **scotty\_123** 1 year, 9 months ago

On the exam today... MCAS option was renamed to "Microsoft Defender for Cloud Apps"  
upvoted 2 times

 **Xyz\_40** 1 year, 6 months ago

Renamed to MDA.  
upvoted 1 times

 **stromnessian** 1 year, 9 months ago

**Selected Answer: C**

It's C.

upvoted 2 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.  
upvoted 2 times

 **Eltooth** 2 years, 6 months ago

MCAS is correct answer.  
upvoted 3 times

**HOTSPOT -**

You have an on-premises datacenter that contains the hosts shown in the following table.

| Name      | Description                                                                                       |
|-----------|---------------------------------------------------------------------------------------------------|
| Server1   | Domain controller that runs Windows Server 2019                                                   |
| Server2   | Server that runs Windows Server 2019 and has Azure AD Connect deployed                            |
| Server3   | Server that runs Windows Server 2019 and has a Microsoft ASP.NET application named App1 installed |
| Server4   | Unassigned server that runs Windows Server 2019                                                   |
| Firewall1 | Hardware firewall connected to the internet that blocks all traffic unless explicitly allowed     |

The Active Directory forest syncs to an Azure Active Directory (Azure AD) tenant. Multi-factor authentication (MFA) is enforced for Azure AD.

You need to ensure ~~that~~ you can publish App1 to Azure AD users.

What should you configure on Server4 and Firewall1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Service to install on Server4:

- Azure AD Application Proxy
- The Azure AD Password Protection DC agent
- The Azure AD Password Protection proxy service
- Web Application Proxy in Windows Server

Rule to configure on Firewall1:

- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- Allow outbound HTTPS connections from Server4 to Azure AD.
- Allow outbound IPsec connections from Server4 to Azure AD.

**Answer Area**

Service to install on Server4:

- Azure AD Application Proxy
- The Azure AD Password Protection DC agent
- The Azure AD Password Protection proxy service
- Web Application Proxy in Windows Server

Correct Answer:

Rule to configure on Firewall1:

- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- Allow outbound HTTPS connections from Server4 to Azure AD.
- Allow outbound IPsec connections from Server4 to Azure AD.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy>

 **EmnCours** 3 months, 3 weeks ago

Correct

upvoted 1 times

 **dule27** 5 months ago

Azure AD Application Proxy

Allow outbound HTTPS connections from Server4 to Azure AD

upvoted 2 times

 **haskelatchi** 6 months, 3 weeks ago

Correct.

upvoted 1 times

 **mcas** 1 year ago

you don't install an Application Proxy on the on-prem server. you install a connector

The connector is a lightweight agent that runs on a Windows Server inside your network. The connector manages communication between the Application Proxy service in the cloud and the on-premises application.

<https://learn.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy#how-application-proxy-works>  
upvoted 3 times

□ **ANDRESCB1988** 1 year ago

correct

upvoted 1 times

□ **estyj** 1 year, 1 month ago

Correct. Application Proxy is an Azure AD service you configure in the Azure portal. It enables you to publish an external public HTTP/HTTPS URL endpoint in the Azure Cloud, which connects to an internal application server URL in your organization

upvoted 1 times

□ **Bjarki2330** 1 year, 3 months ago

Correct.

upvoted 1 times

□ **d3j4n** 1 year, 4 months ago

Correct

upvoted 2 times

□ **sapien45** 1 year, 5 months ago

Correct.

upvoted 1 times

□ **kaenegē** 1 year, 6 months ago

Correct

upvoted 1 times

□ **themrcox** 1 year, 6 months ago

Correct.

upvoted 1 times

**HOTSPOT -**

You have an Azure Active Directory (Azure AD) tenant that has the default App registrations settings. The tenant contains the users shown in the following table.

| Name   | Role                            |
|--------|---------------------------------|
| Admin1 | Application administrator       |
| Admin2 | Application developer           |
| Admin3 | Cloud application administrator |
| User1  | User                            |

You purchase two cloud apps named App1 and App2. The global administrator registers App1 in Azure AD.

You need to identify who can assign users to App1, and who can register App2 in Azure AD.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Can assign users to App1:

|                                   |
|-----------------------------------|
| Admin1 only                       |
| Admin3 only                       |
| Admin1 and Admin3 only            |
| Admin1, Admin2, and Admin3 only   |
| Admin1, Admin2, Admin3, and User1 |

Can register App2 in Azure AD:

|                                   |
|-----------------------------------|
| Admin1 only                       |
| Admin3 only                       |
| Admin1 and Admin3 only            |
| Admin1, Admin2, and Admin3 only   |
| Admin1, Admin2, Admin3, and User1 |

**Answer Area**

Can assign users to App1:

|                                   |
|-----------------------------------|
| Admin1 only                       |
| Admin3 only                       |
| Admin1 and Admin3 only            |
| Admin1, Admin2, and Admin3 only   |
| Admin1, Admin2, Admin3, and User1 |

Correct Answer:

Can register App2 in Azure AD:

|                                   |
|-----------------------------------|
| Admin1 only                       |
| Admin3 only                       |
| Admin1 and Admin3 only            |
| Admin1, Admin2, and Admin3 only   |
| Admin1, Admin2, Admin3, and User1 |

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users> <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

 **aboveidalimit** Highly Voted 2 years, 4 months ago

Yup, App Registration by any Users is enabled by default on a new directory. Question itself states default app registration, which means user in that directory including guest users can register applications. Answer is correct!

upvoted 18 times

 **BaderJ** Highly Voted 2 years, 2 months ago

Passed the exam today 23/09/2021

This question came in the exam.

upvoted 9 times

 **dule27** Most Recent 5 months, 2 weeks ago

Can assign users to App1: Admin1 and Admin3  
Can register App2 in Azure AD: Admin1, admin2, Admin3 and User1  
upvoted 3 times

□ **lme** 1 year, 2 months ago  
on the exam 09222022, i answered the same. Passed the exam, btw.  
upvoted 6 times

□ **Lion007** 1 year, 4 months ago  
Correct answers.  
Only administrators (Admin1 - Application Administrator & Admin3 - Cloud application administrator) can manage/configure apps.

Name: Cloud application administrator  
Description: Users in this role can add, manage, and configure enterprise applications, app registrations but will not be able to configure or manage on-premises like app proxy.

Azure AD - User settings - App registration: default is Yes (If this option is set to yes, then non-admin users may register custom-developed applications for use within this directory.)  
upvoted 1 times

□ **rachee** 1 year, 5 months ago  
<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>  
upvoted 1 times

□ **Jun143** 1 year, 8 months ago  
just pass the exam today. This came in the question.  
upvoted 2 times

□ **GPerez73** 1 year, 9 months ago  
Correct for me  
upvoted 2 times

□ **zmlapq99** 1 year, 10 months ago  
On exam few days ago.  
upvoted 2 times

□ **Pravda** 1 year, 10 months ago  
On the exam 1/20/2022  
upvoted 1 times

□ **AYap** 2 years, 5 months ago  
Correct answers. App Registration in User Settings is enabled by default.  
upvoted 5 times

□ **JerryGolais** 2 years, 6 months ago  
First answer is correct.  
Second answer is correct if App Registration under AD User Settings is set to Yes but I can't remember which one is the default value.  
upvoted 3 times

□ **melatocaroca** 2 years, 4 months ago  
Assign the admins, App Registration any User, Settings is enabled by default.  
upvoted 1 times

□ **Beitran** 2 years, 6 months ago  
Seems correct  
upvoted 3 times

**HOTSPOT -**

You have a custom cloud app named App1 that is registered in Azure Active Directory (Azure AD).

App1 is configured as shown in the following exhibit.

**Save** | **Discard** | **Delete** | **Got feedback?**

Enabled for users to sign-in? **Yes** **No**

Name **App1**

Homepage URL **https://app1.m365x629615.onmicrosoft.com/**

Logo 

Select a file

User access URL **https://myapps.microsoft.com/signin/App1/09df58d6-d29d-40de-b0d...**

Application ID **09df58d6-d29d-40de-b0d0-321fdc63c665**

Object ID **03709d22-7e61-4007-a2a0-04dbdff269cd**

Terms of Service Url **Publisher did not provide this information**

Privacy Statement Url **Publisher did not provide this information**

Reply Url **https://contoso.com/App1/logon**

User assignment required? **Yes** **No**

Visible to users? **Yes** **No**

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.

Hot Area:

**Answer Area**

[answer choice] can access App1 from the homepage URL.

|                                                 |
|-------------------------------------------------|
| All users                                       |
| No one                                          |
| Only users listed on the Owners blade           |
| Only users listed on the Users and groups blade |

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

|                                                 |
|-------------------------------------------------|
| all users                                       |
| no one                                          |
| only users listed on the Owners blade           |
| only users listed on the Users and groups blade |

## Answer Area

[answer choice] can access App1 from the homepage URL.

|                                                 |
|-------------------------------------------------|
| All users                                       |
| No one                                          |
| Only users listed on the Owners blade           |
| Only users listed on the Users and groups blade |

Correct Answer:

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

|                                                 |
|-------------------------------------------------|
| all users                                       |
| no one                                          |
| only users listed on the Owners blade           |
| only users listed on the Users and groups blade |

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

✉  **MartiP** Highly Voted 2 years, 7 months ago

Actually I think correct answers are:

All users

Assigned user in users and groups blade

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-configure>

upvoted 69 times

✉  **GlenRMag16** 1 year, 10 months ago

Tested in my lab, this is the correct answer.

upvoted 10 times

✉  **Davidf** 1 year, 6 months ago

Correct - assignment is not required, so everyone can log in, but it won't appear in the my apps portal.  
Unless they have been assigned it, in which case it will appear in the my apps portal.

upvoted 5 times

✉  **aokisan** Highly Voted 2 years, 7 months ago

the answers are

all users

all users

upvoted 18 times

✉  **Dipronil** 2 years ago

Wrong.

<https://docs.microsoft.com/en-us/learn/modules/plan-design-integration-of-enterprise-apps-for-sso/6-configure-pre-integrated-gallery-saas-apps>

Yes no Yes -> Assigned users can see the app and sign in.Unassigned users cannot see the app but can sign in.

So only assigned user can see but unassigned users cannot see. According to the portal.

upvoted 5 times

✉  **EmnCours** Most Recent 4 months, 1 week ago

All users

Assigned user in users and groups blade

upvoted 4 times

✉  **dule27** 5 months, 2 weeks ago

All users

Only users listed on the users and groups blade

upvoted 2 times

✉  **Arjanussie** 9 months, 1 week ago

Enabled for users to sign in? Yes

User assignment required? No

Visible to users? Yes

Assigned users can see the app and sign in. Unassigned users can't see the app but can sign in

All users

Assigned user in users and groups blade

upvoted 4 times

✉  **LeTrinh** 9 months, 2 weeks ago

Wrong.

1/ Can access App1 -> All user

Because Users to sign in is enable AND user assignment require is NO.

2/ Only users listed on the Owner blade

- Visible to users is YES -> visible to assign users ONLY, which is the Owner.

<https://learn.microsoft.com/en-us/training/modules/plan-design-integration-of-enterprise-apps-for-sso/7-configure-pre-integrated-gallery-saas-apps>

upvoted 2 times

□ **LeTrinh** 9 months, 2 weeks ago

Correction: on the Users and Groups blade in the Microsoft Office 365 app launcher.

upvoted 2 times

□ **jack987** 11 months, 2 weeks ago

The answer is correct.

All users can access App1 from the homepage URL.

App1 will appear in the Microsoft O365 app launcher for no one.

When user assignment is not required, unassigned users don't see the app on their My Apps, but they can still sign in to the application itself (also known as SP-initiated sign-on) or they can use the User Access URL in the application's Properties page (also known as IDP-initiated sign on). For more information on requiring user assignment configurations, See Configure an application

This setting doesn't affect whether or not an application appears on My Apps. Applications appear on users' My Apps access panels once you've assigned a user or group to the application.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-access-management#requiring-user-assignment-for-an-app>

upvoted 3 times

□ **VeIN** 11 months, 1 week ago

If you check info mark in app properties for:

- "Assignment required": "This option does not affect whether or not an application appears on My Apps. To show the application there, assign an appropriate user or group to the application."

- "Visible to users": If this option is set to yes, then ASSIGNED users will see the application on My Apps and O365 app launcher.

So in summary correct 2nd part of answer will be "Only users listed on the Users and groups blade"

upvoted 3 times

□ **estyj** 1 year, 1 month ago

All users can access App1 from homepage URL

Only users listed on Users and groups- since not assigned will not appear in my apps portal.

upvoted 3 times

□ **Mesfer** 1 year, 2 months ago

1- All users

2- Only users listed on the users and groups blade.

for the second option

-User assignment required :- This option does not affect whether or not an application appears on My Apps. To show the application there, assign an appropriate user or group to the application.

upvoted 3 times

□ **Faheem2020** 1 year, 3 months ago

IMO, the two settings should be treated independently of each other

First question: All Users. If 'assignment required' set to no, any user can login using the app url

Second Question: Only users assigned in users and groups blade. If 'Visible to Users' is Yes, then assigned users will see the application on My Apps and O365 app launcher. If this set to no, then no users will see this application on their My Apps and O365 Launcher

upvoted 1 times

□ **RandomNickname** 1 year, 6 months ago

The link from user Dipronil helps to make sense of this.

1# All users, because "Enable for users to sign-in" is selected and "User assignment required" is set to No.

2# No one, because unless you are assigned to the app explicitly "as per URL: <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>" No one is able to see the app, this is irrespective if "Visible to user is specified".

upvoted 3 times

□ **sapien45** 1 year, 5 months ago

Agreed.

Assignment is not required meaning that the app will NOT appear user's My Apps

But Application is visible to users, meaning that it will appear through its homepage url

All users

None

upvoted 1 times

□ **zts** 1 year, 5 months ago

Confirmed, the answer is: All users, and none. You can review the same setup on this page 4 question 6. Most of the community answer is NO for the third question which it doesn't appear.

upvoted 1 times

□ **zts** 1 year, 5 months ago

apologies, it's page 4, question 9. - 3rd question is: App1 appears in the Microsoft Office 365 app launcher of user 4. - Most of the answers is No.

upvoted 1 times

✉ **dgeddes** 1 year, 6 months ago

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-access-management#requiring-user-assignment-for-an-app>

When user assignment is required, only those users you assign to the application (either through direct user assignment or based on group membership) are able to sign in. They can access the app on the My Apps portal or by using a direct link.

When user assignment is not required, unassigned users don't see the app on their My Apps, but they can still sign in to the application itself (also known as SP-initiated sign-on) or they can use the User Access URL in the application's Properties page (also known as IDP-initiated sign on). For more information on requiring user assignment configurations, See Configure an application

upvoted 2 times

✉ **Nilz76** 1 year, 7 months ago

This is purely based on the information we have on the question.

I just created an app called APP1. I created the app with the settings exactly as the graphic. I then created two new users Jessica and Bob. Assigned Jessica an M365 licence and Bob nothing.

I logged in as each user and APP1 was NOT visible in the app launcher.

So I think the answers are:

- 1) All Users
- 2) No one

I then granted Bob access to the app via Enterprise applications > APP1 > Users and Groups > None Selected > search for Bob > Select > Assign.

Waited 5 mins > logged out as Bob. Logged back in as Bob and the app was visible in the App Launcher.

upvoted 3 times

✉ **TP447** 1 year, 7 months ago

All Users + Users on the Users and Groups blade is correct for me.

Visible to Users is set to yes but this will only apply to users specified in Users and Groups - answer would be "No One" if the question showed this as blank.

upvoted 2 times

✉ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 3 times

✉ **AZ\_Student** 1 year, 9 months ago

1- Only users - 2 only users listed on the users and groups blad.

upvoted 1 times

✉ **xDinoKoalax** 1 year, 9 months ago

My personal opinion:

1. All users - I agree

2. App 1 will appear in Microsoft 365 App Launcher for "whom"? - The M365 App Launcher is portal.office.com, it is not myapps.microsoft.com - reference: <https://support.microsoft.com/en-us/office/meet-the-microsoft-365-app-launcher-79f12104-6fed-442f-96a0-eb089a3f476a> -> So the answer should be no one.

upvoted 1 times

✉ **xDinoKoalax** 1 year, 9 months ago

Correction - after testing, I think it should be only visible for assigned user. But, it's good that I can tell App Launcher is the same like the portal one.

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant.

You create an enterprise application collection named HR Apps that has the following settings:

- Applications: App1, App2, App3

- Owners: Admin1

- Users and groups: HRUsers

All three apps have the following Properties settings:

- Enabled for users to sign in: Yes

- User assignment required: Yes

Visible to users: Yes -

Users report that when they go to the My Apps portal, they only see App1 and App2.

You need to ensure that the users can also see App3.

What should you do from App3?

- A. From Users and groups, add HRUsers.
- B. From Single sign-on, configure a sign-on method.
- C. From Properties, change User assignment required to No.
- D. From Permissions, review the User consent permissions.

#### Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal> <https://docs.microsoft.com/en-us/azure/active-directory/user-help/my-applications-portal-workspaces>

Community vote distribution

A (100%)

✉  **abovedalimit** Highly Voted 2 years, 4 months ago

Correct Answer. I just tried this in my company's tenancy. User assignment and Visible to Users goes hand in hand for this.

If Visible to Users is set to Yes then this is the explanation from the 'i' next to it:

If this option is set to yes, then assigned users will see the application on My Apps and O365 app launcher. If this option is set to no, then no users will see this application on their My Apps and O365 launcher. Assigned User is the key here.

Unless the users are assigned to the app, then No one will see the application on their MyApp or O365 Launcher. Provided Answer is Correct!

upvoted 20 times

✉  **JLInF** Highly Voted 1 year, 6 months ago

This question has no sense for me... It sais that HRUsers are already in "users and groups" and the users have access to App1 and App2, so they should have access to App3 too. Someone can explain me?

upvoted 17 times

✉  **Techfall** 10 months, 1 week ago

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/access-panel-collections>

"A collection essentially applies a filter to the applications a user can already access, so the user sees only those applications in the collection that have been assigned to them."

App collections are just visual filters, they do not dictate access privileges to the app itself.

upvoted 4 times

✉  **sergioandresiq** 1 year, 4 months ago

You are right, The question is not correct.

The end-user should see the three apps or none, it doesn't make sense he can see app1, and app2 but not app3 which have the same configuration.

However, We have to provide an answer and the only that is related to seeing the app is the "User and groups"

upvoted 4 times

✉  **sherifhamed** Most Recent 2 months, 1 week ago

Selected Answer: A

To ensure that users can see App3 in the My Apps portal, you should do the following:

A. From Users and groups, add HRUsers.

This will add the HRUsers group to App3 and grant them access to see the application in the My Apps portal.

upvoted 1 times

□ **EmnCours** 4 months, 1 week ago

**Selected Answer: A**

Correct Answer: A

upvoted 2 times

□ **dule27** 5 months, 2 weeks ago

**Selected Answer: A**

A. From Users and groups, add HRUsers.

upvoted 2 times

□ **TomasValtor** 6 months ago

Correct answer: A

Your users can use the My Apps portal to view and start the cloud-based applications they have access to. By default, all the applications a user can access are listed together on a single page. To better organize this page for your users, if you have an Azure AD Premium P1 or P2 license you can set up collections. With a collection, you can group together applications that are related (for example, by job role, task, or project) and display them on a separate tab. A collection essentially applies a filter to the applications a user can already access, so the user sees only those applications in the collection that have been assigned to them.

upvoted 1 times

□ **Smallos** 6 months, 2 weeks ago

I have read this question over and over and it specifically says at the top all 3 apps have the same settings.

upvoted 4 times

□ **eleazarrd** 7 months, 3 weeks ago

**Selected Answer: A**

Para que los usuarios puedan ver App3 en el portal de Mis aplicaciones, es necesario realizar la opción A. Es decir, agregar el grupo HRUsers a la configuración de usuarios y grupos de la aplicación App3 en la colección HR Apps de Azure AD.

La opción B se refiere a la configuración de inicio de sesión único, que no está relacionada con la visibilidad de las aplicaciones en el portal de Mis aplicaciones.

La opción C se refiere a la configuración de asignación de usuario, que solo controla si un usuario puede acceder a la aplicación o no. Cambiar esta opción no afectará la visibilidad de la aplicación en el portal de Mis aplicaciones.

La opción D se refiere a los permisos de consentimiento del usuario, que tampoco están relacionados con la visibilidad de las aplicaciones en el portal de Mis aplicaciones.

upvoted 1 times

□ **Jhill777** 1 year ago

**Selected Answer: A**

Question/Answer doesn't make sense because it literally already says "Users and groups: HRUsers". You won't be able to add the same group that is already in there. The fact that they can see App1 and App2 make me think the correct answer is "Call MSFT".

upvoted 5 times

□ **BTL\_Happy** 1 year ago

this question came out in my test today.

upvoted 2 times

□ **makovec25** 1 year, 2 months ago

**Selected Answer: A**

Configuration in the question is for app collection not for apps itself. You must add users or groups to the app.

upvoted 2 times

□ **Faheem2020** 1 year, 3 months ago

Eliminating the more irrelevant answers, you are left with option A as the answer.

upvoted 1 times

□ **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

□ **nguyenhung1121990** 2 years, 4 months ago

so answer is??

upvoted 1 times

□ **airairo** 2 years, 2 months ago

From Users and groups, add HRUsers.

upvoted 4 times

□ **melatocaroca** 2 years, 4 months ago

When user assignment is required, only those users you explicitly assign to the application (either through direct user assignment or based on group membership) will be able to sign in. They can access the app on their My Apps page or by using a direct link.

When user assignment is not required, unassigned users don't see the app on their My Apps, but they can still sign in to the application itself (also known as SP-initiated sign-on) or they can use the User Access URL in the application's Properties page (also known as IDP-initiated sign on).

upvoted 4 times

✉  **melatocaroca** 2 years, 4 months ago

Managing user consent to apps in Microsoft 365

This setting controls whether users can give that consent to apps that use OpenID Connect and OAuth 2.0 for sign-in and requests to access data.

If you turn this setting on, those apps will ask users for permission to access your organization's data, and users can choose whether to allow it. If you turn this setting off, then admins must consent to those apps before users may use them. In this case, consider setting up an admin consent workflow in the Azure portal so users can send a request for admin approval to use any blocked app.

upvoted 1 times

✉  **melatocaroca** 2 years, 4 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-access-management>

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

upvoted 1 times

✉  **allgiga** 2 years, 5 months ago

Correct!

You must have permission on the app, even if you have a collection.

upvoted 5 times

You have an Azure Active Directory (Azure AD) tenant.  
For the tenant, Users can register applications is set to No.  
A user named Admin1 must deploy a new cloud app named App1.  
You need to ensure that Admin1 can register App1 in Azure AD. The solution must use the principle of least privilege.  
Which role should you assign to Admin1?

- A. Managed Application Contributor for Subscription1.
- B. Application developer in Azure AD.
- C. Cloud application administrator in Azure AD.
- D. App Configuration Data Owner for Subscription1.

**Correct Answer: B**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles>

*Community vote distribution*

B (100%)

✉ **abovedalimit** Highly Voted 2 years, 4 months ago

Correct and this provides the least access to register the app  
upvoted 13 times

✉ **tatendazw** 2 years, 1 month ago

Name: Application developer

Description: Users in this role will continue to be able to register app registrations even if the Global Admin has turned off the tenant level switch for "Users can register apps".  
upvoted 13 times

✉ **sherifhamed** Most Recent 2 months, 1 week ago

**Selected Answer: B**

B. Application developer in Azure AD.

This role grants the necessary permissions to create and manage Azure AD applications without overly broad permissions.  
upvoted 1 times

✉ **DasChi\_cken** 3 months, 1 week ago

**Selected Answer: B**

Only answer B and C could be right  
And answer B uses least privilege  
upvoted 2 times

✉ **EmnCours** 4 months, 1 week ago

**Selected Answer: B**

B. Application developer in Azure AD.  
upvoted 1 times

✉ **dule27** 5 months, 2 weeks ago

**Selected Answer: B**

B. Application developer in Azure AD.  
upvoted 1 times

✉ **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022  
upvoted 1 times

✉ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.  
upvoted 1 times

✉ **serbay39** 1 year, 9 months ago

definitely correct. B  
upvoted 1 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 2 times

 **melatocaroca** 2 years, 5 months ago

Application Developer Can create application registrations independent of the 'Users can register applications' setting.

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

upvoted 4 times

 **krustyk** 2 years, 6 months ago

Correct from documentation

upvoted 2 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

**HOTSPOT -**

You have a Microsoft 365 tenant that contains a group named Group1 as shown in the Group1 exhibit. (Click the Group1 tab.)

| PS C:\> Get-AzureADGroup -searchstring "group1"   Get-AzureADGroupowner                  |             |                                   |          |
|------------------------------------------------------------------------------------------|-------------|-----------------------------------|----------|
| ObjectId                                                                                 | DisplayName | UserPrincipalName                 | UserType |
| a7f7d405-636f-4493-b971-5c2b7a131b1c                                                     | Admin       | admin@M365x629615.onmicrosoft.com | Member   |
| PS C:\> Get-AzureADGroup -searchstring "group1"   GetAzureADGroupMember   ft displayname |             |                                   |          |
| Displayname                                                                              |             |                                   |          |
| -----                                                                                    |             |                                   |          |
| User1                                                                                    | 店铺：专业认证88   |                                   |          |
| User4                                                                                    | 店铺：专业认证88   |                                   |          |
| Group3                                                                                   | 店铺：专业认证88   |                                   |          |

You create an enterprise application named App1 as shown in the App1 Properties exhibit. (Click the App1 Properties tab.)

Dashboard > ContosoAzureAD > Enterprise applications > App1

**App1| Properties**  
Enterprise Application

Overview Deployment Plan Diagnose and solve problems

Manage

- Properties** (selected)
- Owners
- Roles and administrators (Prev.)
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-ins

Enabled for users to sign-in?  Yes  No

Name

Homepage URL

Logo

User access URL

Application ID

Object ID

Terms of Service Url

Privacy Statement Url

Reply URL

User assignment required?  Yes  No

Visible to users?  Yes  No

You configure self-service for App1 as shown in the App1 Self-service exhibit. (Click the App1 Self-service tab.)

**App1 | Self-service**

Enterprise application

« Save Discard

|                                   |                                                                                     |
|-----------------------------------|-------------------------------------------------------------------------------------|
| Overview                          | Allow users to request access to this application?  Yes  No                         |
| Deployment Plan                   | To which group should assigned users be added? <b>Group1</b>                        |
| Properties                        | Require approval before granting access to this application?  Yes  No               |
| Owners                            | Who is allowed to approve access to this application? <b>1 users selected</b>       |
| Roles and administrators (Pre...) | To which role should users be assigned in this application? * <b>Default Access</b> |
| Users and groups                  |                                                                                     |
| Single sign-on                    |                                                                                     |
| Provisioning                      |                                                                                     |
| Application proxy                 |                                                                                     |
| Self-service                      |                                                                                     |
| <b>Security</b>                   |                                                                                     |
| Conditional Access                |                                                                                     |
| Permissions                       |                                                                                     |

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

| Statements                                                                   | Yes                   | No                    |
|------------------------------------------------------------------------------|-----------------------|-----------------------|
| The members of Group3 can access App1 without first being approved by User1. | <input type="radio"/> | <input type="radio"/> |
| After you configure self-service for App1, the owner of Group1 is User1.     | <input type="radio"/> | <input type="radio"/> |
| App1 appears in the Microsoft Office 365 app launcher of User4.              | <input type="radio"/> | <input type="radio"/> |

**Select approvers**

Search

|                                                        |
|--------------------------------------------------------|
| User1<br>User1@m365x629615.onmicrosoft.com<br>Selected |
| User2<br>User2@m365x629615.onmicrosoft.com             |
| User3<br>User3@m365x629615.onmicrosoft.com             |
| User4<br>User4@m365x629615.onmicrosoft.com             |
| <b>Selected approvers</b>                              |
| User1<br>User1@m365x629615.onmicrosoft.com             |

Remove

**Answer Area**

| Statements                                                                                                                                    | Yes                              | No                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| The members of Group3 can access App1 without first being approved by User1.<br><b>Correct Answer:</b> without first being approved by User1. | <input type="radio"/>            | <input checked="" type="radio"/> |
| After you configure self-service for App1, the owner of Group1 is User1.                                                                      | <input type="radio"/>            | <input checked="" type="radio"/> |
| App1 appears in the Microsoft Office 365 app launcher of User4.                                                                               | <input checked="" type="radio"/> | <input type="radio"/>            |

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal> <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users>

d3N 2 years, 6 months ago

As the app is not visible for the users, I think the correct answer might be No, No, No.

For reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-configure>  
upvoted 31 times

J4U 2 years, 1 month ago

Just sharing my thoughts.

1. NO - Only direct members will have access. Approved users will be added to Group 1.
2. Yes - The approver will automatically become owner of the Group 1 after self service is configured.
3. NO - Visible to users is NO. So no one will be able to see the app.

upvoted 65 times

✉ **its\_tima** 10 months, 3 weeks ago

but how come number 2 is No?? My belief is it has yet to be added as the owner.

upvoted 1 times

✉ **existingname** 1 year, 3 months ago

On the exam today, NYN

upvoted 10 times

✉ **girikedar** Highly Voted 1 year, 12 months ago

Tested in tenant answer is NO, YES, YES

- 1) No : because Nesting is not supported
- 2) Yes : because approver user will automatically assigned as owner
- 3) Yes : because assigned user will always have app on myapplication.microsoft.com portal

upvoted 24 times

✉ **jack987** 11 months, 2 weeks ago

I agree with girikedar.

The correct answer is No - Yes - Yes.

upvoted 1 times

✉ **jack987** 11 months, 2 weeks ago

I did more research:

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/application-properties#visible-to-users>

Visible to users:

Makes the application visible in My Apps and the O365 Launcher

If this option is set to Yes, then assigned users see the application on the My Apps portal and O365 app launcher.

If this option is set to No, then no users see this application on their My Apps portal and O365 launcher.

So the correct answer is No, Yes, No.

upvoted 7 times

✉ **slick\_orange** 1 year, 3 months ago

For No.3. If you hover your mouse to 'Visible to users? (i)' icon, it says "If this option is set to yes, then assigned users will see the application on My Apps and O365 app launcher. If this option is set to no, then no users will see this application on their My Apps and O365 launcher." So that means no one can see the app.

upvoted 2 times

✉ **sergioandreslq** 1 year, 4 months ago

More support for 3 Yes:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-properties#visible-to-users>

"Regardless of whether assignment is required or not, only assigned users are able to see this application in the My Apps portal."

upvoted 4 times

✉ **Hot\_156** 1 year, 2 months ago

Assignment Required is something totally different than the "Visible to Users" option. Number 3 is No

upvoted 5 times

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

1. NO - Only direct members will have access. Approved users will be added to Group 1.
2. Yes - The approver will automatically become owner of the Group 1 after self service is configured.
3. NO - Visible to users is NO. So no one will be able to see the app.

upvoted 1 times

✉ **Nyamnyam** 3 weeks, 5 days ago

1. No - Nested groups are not supported

2. Yes - This was a hard one, because I couldn't find any online reference about it. But Selvaraj Rajan provided an experience from a test environment (s. below)

3. No - As many others have referenced, "Visible to users" = No wins over Assignment.

Read again: <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/application-properties#visible-to-users>

upvoted 1 times

✉ **EmnCours** 3 months, 3 weeks ago

- 1) No : because Nesting is not supported
- 2) Yes : because approver user will automatically assigned as owner
- 3) NO : because "not visible" option is toggled for assigned user

upvoted 2 times

✉ **OK2020** 5 months ago

- 1) No : because Nesting is not supported
- 2) Yes : because approver user will automatically assigned as owner
- 3) NO : because "not visible" option is toggled for assigned user

upvoted 3 times

✉ **dule27** 5 months, 2 weeks ago

NO

YES

NO

upvoted 4 times

✉ **OK2020** 5 months, 3 weeks ago

NYN

last NO: because "visible to users" is toggled as No, with this even assigned users won't see the app. Check the matrix in the link below:  
<https://learn.microsoft.com/en-us/training/modules/plan-design-integration-of-enterprise-apps-for-sso/7-configure-pre-integrated-gallery-saas-apps>

upvoted 2 times

✉ **haskelatchi** 6 months, 3 weeks ago

Good question, N,Y,N

upvoted 3 times

✉ **Selvaraj\_Rajan** 6 months, 3 weeks ago

2. Yes

When you create a self service and save it, you will see a warning like below.

Performing this action will replace any existing owners of the Group "XXXX" with the approver(s) you've selected.

Would you like to do this?

Yes No

upvoted 2 times

✉ **LeTrinh** 9 months, 2 weeks ago

NNN

1/ Very clear

2/ User1 can be an owner of the App1, not the owner of Group 1 which is Admin in the picture --> NO

3/ It is invisible to assign users -> NO

upvoted 2 times

✉ **0byte** 1 year, 1 month ago

N - Try adding a group to an app. There is a warning that only direct members will have access to the app. Nested groups are ignored  
Y - Try configuring self-service for any app - there is a message that any existing owners of the group will be replaced with the approver  
N - The whole point of this setting is to hide an app from users (as explained in info next to the setting). Some apps don't need to be visible, or require any interaction from users, to work.

upvoted 11 times

✉ **TV56\_** 1 year, 2 months ago

My answers will be N,Y,Y

1. Group 1 is assigned to App1
2. Admin is the owner of Group1
3. User4 is a member of Group1 according to the Powershell screenshot

upvoted 1 times

✉ **Yuki\_0916** 5 months, 2 weeks ago

So the second one should be N, right?

upvoted 1 times

✉ **Hot\_156** 1 year, 2 months ago

the configuration for the application is "Visible to Users" = No, so no one will be able to see the app even if they are assigned to it.

upvoted 1 times

✉ **brlojaexpress** 1 year, 3 months ago

N, Y, N,

upvoted 5 times

✉ **sapien45** 1 year, 5 months ago

NYN

I concur

upvoted 6 times

✉ **RandomNickname** 1 year, 6 months ago

No

Yes

No

Reading the information provided agree with the n,y,n group.

upvoted 7 times

✉ **TP447** 1 year, 7 months ago

No/Yes/No for me.

3rd question - No because "Visible to Users" is set to No which means No users will see the app.

upvoted 5 times

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection enabled.

You need to implement a sign-in risk remediation policy without blocking user access.

What should you do first?

- A. Configure access reviews in Azure AD.
- B. Enforce Azure AD Password Protection.
- C. Configure self-service password reset (SSPR) for all users.
- D. Implement multi-factor authentication (MFA) for all users.

**Correct Answer: D**

MFA and SSPR are both required. However, MFA is required first.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>

*Community vote distribution*

D (100%)

✉ **melatocaroca** Highly Voted 2 years, 4 months ago

to implement a sign-in risk remediation policy

When a sign in risk policy triggers:

Azure AD MFA can be triggered, allowing to user to prove it's them by using one of their registered authentication methods, resetting the sign in risk.

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>

upvoted 16 times

✉ **goape** Highly Voted 1 year, 5 months ago

MFA for sign-in risk, SSPR for user risk

upvoted 12 times

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

**Selected Answer: D**

Here a better link: <https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-remediate-unblock#self-remediation-with-risk-based-policy>

- perform MFA to self-remediate a sign-in risk
- perform secure password change to self-remediate a user risk

upvoted 1 times

✉ **EmnCours** 4 months, 1 week ago

**Selected Answer: D**

Correct Answer: D

upvoted 1 times

✉ **dule27** 5 months, 2 weeks ago

**Selected Answer: D**

D. Implement multi-factor authentication (MFA) for all users.

upvoted 1 times

✉ **estyj** 1 year, 1 month ago

D Correct need to setup MFA for all users first before SSPR

upvoted 1 times

✉ **existingname** 1 year, 3 months ago

On the exam today, D is correct

upvoted 2 times

✉ **TP447** 1 year, 7 months ago

Initially I selected C but makes sense - MFA would be configured before SSPR so D is correct :)

upvoted 1 times

✉ **martinods** 1 year, 1 month ago

MFA for sign-in risk, SSPR for user risk

upvoted 2 times

 **stromnessian** 1 year, 9 months ago

**Selected Answer: D**

D is right.

upvoted 5 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 2 times

 **NarenderSingh** 2 years, 2 months ago

Correct

upvoted 4 times

 **ArielReyes27** 2 years, 5 months ago

Correct.

upvoted 2 times

 **AS007** 2 years, 6 months ago

Correct

upvoted 3 times

**HOTSPOT -**

Your company has a Microsoft 365 tenant.

All users have computers that run Windows 10 and are joined to the Azure Active Directory (Azure AD) tenant.

The company subscribes to a third-party cloud service named Service1. Service1 supports Azure AD authentication and authorization based on OAuth. Service1 is published to the Azure AD gallery.

You need to recommend a solution to ensure that the users can connect to Service1 without being prompted for authentication. The solution must ensure that the users can access Service1 only from Azure AD-joined computers. The solution must minimize administrative effort.

What should you recommend for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Ensure that the users can connect to Service1 without being prompted for authentication:

- An app registration in Azure AD
- Azure AD Application Proxy
- An enterprise application in Azure AD
- A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

- Azure AD Application Proxy
- A compliance policy
- A conditional access policy
- An OAuth policy

**Answer Area**

Ensure that the users can connect to Service1 without being prompted for authentication:

- An app registration in Azure AD
- Azure AD Application Proxy
- An enterprise application in Azure AD
- A managed identity in Azure AD

**Correct Answer:**

Ensure that the users can access Service1 only from the Azure AD-joined computers:

- Azure AD Application Proxy
- A compliance policy
- A conditional access policy
- An OAuth policy

**Reference:**

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices>

 **NawafAli** Highly Voted 1 year, 11 months ago

Correct Answer.

Service1 support OAuth for Authentication & authorization, however service1 is published in Azure AD gallery, hence we will use An enterprise application in Azure AD blade to register for SSO.

for second point, we can use conditional Access policy to restrict.

upvoted 14 times

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

I would use Conditional Access -> Conditions -> Filter for devices -> Rule syntax:  
device.trustType -eq "AzureAD"

When creating Conditional Access policies, administrators have asked for the ability to target or exclude specific devices in their environment. The condition filter for devices gives administrators this capability. Now you can target specific devices using supported operators and properties for device filters and the other available assignment conditions in your Conditional Access policies.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-condition-filters-for-devices>

upvoted 1 times

✉ **EmnCours** 3 months, 3 weeks ago

Correct Answer.

upvoted 1 times

✉ **dule27** 5 months, 2 weeks ago

Ensure that the users can connect to Service1 without prompt for Authentication: AN Enterprise application in Azure AD

Ensure that users can access Service1 only from the Azure AD joined computers: A conditional access policy

upvoted 1 times

✉ **217f3c9** 7 months, 1 week ago

I am confused about the AzureAD joined devices. You cant use ad join as a requirement in conditional access.

upvoted 1 times

✉ **watapity** 6 months ago

You can, You add it as a device condition

upvoted 1 times

✉ **estyj** 1 year, 1 month ago

Correct: Enterprise App has option for SSO, App registration does not.

Conditional access policy - to ensure users access from Azure AD joined computers.

upvoted 4 times

✉ **sapien45** 1 year, 5 months ago

App registrations the app is preconfigured to use OpenID Connect (OIDC) & OAuth and it is not designed for SAML.

As per MS Document,

Both OpenID Connect and SAML are used to authenticate a user and are used to enable Single Sign On. SAML authentication is commonly used with identity providers such as Active Directory Federation Services (ADFS) federated to Azure AD and is therefore frequently used in enterprise applications. OpenID Connect is commonly used for apps that are purely in the cloud, such as mobile apps, web sites, and web APIs.

upvoted 1 times

✉ **jasonga** 1 year, 6 months ago

As they say gallery app it has to be enterprise app as gallery is not available from app registration blade. If doing a custom non gallery app using OAuth then you would use app registration blade, it's they gallery app part that is the trick as this is only in enterprise app blade

upvoted 3 times

✉ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 2 times

✉ **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 2 times

✉ **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 2 times

✉ **TP447** 1 year, 10 months ago

I think this is correct - App Registration is for first party or internal apps that required more configuration and Enterprise Apps is for 3rd party apps such as in this scenario.

upvoted 4 times

✉ **Povnello** 2 years ago

From my experience, to configure Oauth federated authentication you need to configure it from App registration Blade and not from Enterprise applications. So for me the answer is wrong.

upvoted 1 times

✉ **cbounds** 2 years, 2 months ago

If the application uses Oauth then its an Application Registration. Enterprise applications are used to configure SAML applications.

upvoted 1 times

✉ **J4U** 2 years, 1 month ago

IMO - Question didn't ask anything on authorization (OAuth). connect to Service1 without being prompted for authentication - which means they are asking to configure SSO using enterprise application and OpenID for authentication.

upvoted 2 times

✉ **BaderJ** 2 years, 2 months ago

Passed the exam today 23/09/2021

This question came in the exam.

upvoted 2 times

✉ **Discuss4certi** 2 years, 2 months ago

TL;DR. Answers seem correct to me,

From what i understand from the documentation you need a service principal which can be governed in the enterprise application section.

for the second part you can use Conditional access policies to check if the device is hybrid AZAD joined in the grant section of the conditional access policy.

upvoted 4 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

Your company requires that users request access before they can access corporate applications.

You register a new enterprise application named MyApp1 in Azure Active Directory (Azure AD) and configure single sign-on (SSO) for MyApp1.

Which settings should you configure next for MyApp1?

- A. Self-service
- B. Provisioning
- C. Application proxy
- D. Roles and administrators

**Correct Answer: A**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access>

Community vote distribution

|         |     |
|---------|-----|
| A (89%) | 11% |
|---------|-----|

✉ **TBRate3w254325** Highly Voted 2 years ago

Correct

upvoted 8 times

✉ **haazybanj** Most Recent 1 month ago

**Selected Answer: A**

To enable users to request access to corporate applications, you need to configure the self-service settings for the enterprise application. This allows users to initiate the access request process for MyApp1. By configuring self-service settings, you empower users to request access and reduce the administrative burden of managing access requests manually.

upvoted 1 times

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

The correct answer is A. Self-service.

To enable users to request access to corporate applications, you need to configure the self-service settings for the enterprise application. You can specify the users or groups who can request access, the approvers who can grant or deny access, and the access duration and expiration1.

Provisioning is used to automate the creation, maintenance, and removal of user identities and roles in an application2. Application proxy is used to publish on-premises applications to external users3. Roles and administrators are used to assign permissions to users or groups to manage Azure AD resources4. None of these settings are related to the access request scenario.

upvoted 2 times

✉ **Jzx** 2 months, 3 weeks ago

**Selected Answer: B**

CORRECT ANWER IS B:

Provisioning: Provisioning settings are essential to control how user accounts and their associated access to the application are managed. You should configure provisioning settings to manage user lifecycle activities such as creating, updating, and deleting user accounts in the application. This allows you to ensure that access is controlled and users need to request access before they can use the application.

upvoted 1 times

✉ **EmnCours** 4 months, 1 week ago

**Selected Answer: A**

Correct Answer: A

upvoted 1 times

✉ **dule27** 5 months, 2 weeks ago

**Selected Answer: A**

A. Self-service

upvoted 2 times

✉ **eleazarrd** 7 months, 3 weeks ago

**Selected Answer: A**

Después de configurar el inicio de sesión único (SSO) para MyApp1, debe configurar la opción A, Autoservicio, para permitir que los usuarios soliciten acceso a la aplicación. La opción Autoservicio permite que los usuarios soliciten acceso a la aplicación desde el portal de Azure AD, y los administradores pueden revisar y aprobar las solicitudes de acceso.

La opción B, Aprovisionamiento, se refiere a la sincronización de usuarios y grupos desde el directorio local o desde otros proveedores de identidad a Azure AD. No está relacionado con la configuración de acceso a la aplicación.

La opción C, Proxy de aplicación, se refiere a la publicación de aplicaciones detrás de una puerta de enlace de aplicaciones. No está relacionado con la configuración de acceso a la aplicación.

La opción D, Funciones y administradores, se refiere a la asignación de roles y permisos a los administradores y usuarios. No está relacionado con la configuración de acceso a la aplicación.

upvoted 2 times

 **estyj** 1 year, 1 month ago

Correct, users can self discover apps, users can request access for app, can configure list of individuals to approve or require business approval before granting access to application.

upvoted 2 times

 **sapien45** 1 year, 5 months ago

To require business approval before users are allowed access, set Require approval before granting access to this application

upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

 **stromnessian** 1 year, 9 months ago

**Selected Answer: A**

Seems like A could be right.

upvoted 2 times

 **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022

upvoted 1 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 1 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

**DRAG DROP -**

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

The company is developing a web service named App1.

You need to ensure that App1 can use Microsoft Graph to read directory data in 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.

Select and Place:

**Actions**

Add a group claim.

Create an app registration.

Grant admin consent.

Add delegated permissions.

Add app permissions.

**Answer Area**

店铺：专业认证88

**Actions**

Add a group claim.

**Answer Area**

Create an app registration.

Correct Answer:

Grant admin consent.

Add app permissions.

Add delegated permissions.

**1. Create an app registration:**

Your app must be registered with the Microsoft identity platform and be authorized by either a user or an administrator for access to the Microsoft Graph resources it needs.

**2. Grant admin consent:**

Higher-privileged permissions require administrator consent.

**3. Add app permissions:**

After the consents to permissions for your app, your app can acquire access tokens that represent the app's permission to access a resource in some capacity.

Encoded inside the access token is every permission that your app has been granted for that resource.

Reference:

<https://docs.microsoft.com/en-us/graph/auth/auth-concepts>

✉️ 🚩 **med4** Highly Voted 2 years, 1 month ago

you add app permission first and next admin consent  
upvoted 53 times

✉️ 🚩 **KrissB** 3 months, 3 weeks ago

proof: <https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis#application-permission-to-microsoft-graph>  
upvoted 1 times

✉ **Jacquesvz** 1 year, 10 months ago

100%  
First, we need to register a new application  
Then we need to add application permissions  
And then we need to grant admin consent  
upvoted 23 times

✉ **saybersec** 1 year, 7 months ago

I agree. Video on this link is the proof.  
<https://docs.microsoft.com/en-us/graph/permissions-reference>  
upvoted 9 times

✉ **girikedar** Highly Voted 2 years ago

Answer should be :-  
1) Create app registration  
2) App Permission  
3) Admin Consent  
upvoted 25 times

✉ **jack987** 11 months, 2 weeks ago

I agree with girikedar. The correct answer is:  
1. Create app registration  
2. App permission  
3. Admin consent

Video explaining: <https://youtu.be/yXYzgWWVdSM?t=145>

upvoted 5 times

✉ **Xyz\_40** 1 year, 5 months ago

You are absolutely right: Create App Registration, Add the permission for the Application using the Microsoft Graph, then, Create Admin Consent  
upvoted 3 times

✉ **Nivos300** Most Recent 4 weeks ago

GPT : To ensure that App1 can use Microsoft Graph to read directory data in contoso.com, you should perform the following actions in sequence:

Create an app registration: This is the first step to register your application with Azure AD.

Add app permissions: Specify the necessary permissions for App1 to access Microsoft Graph resources.

Grant admin consent: After specifying the permissions, an admin must grant consent for App1 to access the specified permissions.

The correct sequence is as follows:

Create an app registration.  
Add app permissions.  
Grant admin consent.  
Sources:

Microsoft Graph permissions reference  
Configure required Azure AD Graph permissions for an Overview of Microsoft Graph permissions  
upvoted 1 times

✉ **EmnCours** 3 months, 3 weeks ago

1: Create App registration.  
2: Add App Permission  
3: Grant Admin Consent  
upvoted 2 times

✉ **dule27** 5 months, 2 weeks ago

1. Create an app registration  
2. Add App permissions  
3. Grant Admin consent  
upvoted 2 times

✉ **mancio** 6 months, 2 weeks ago

1) Create app registration  
2) App Permission  
3) Admin Consent  
upvoted 1 times

✉ **sbnpj** 7 months, 4 weeks ago

First register app --->add permission -----> grant admin consent.  
upvoted 1 times

 **Taigr** 9 months, 2 weeks ago

I think that the answer is correct.

After Enterprise app registration you will go there in Security/Permissions and you will click on Grant admin consent. This will show popup for credentials and after you will see popup which API permissions app want and you can accept it. By this you added the API permissions.

upvoted 1 times

 **217f3c9** 7 months, 1 week ago

Only for default read permission. For others you need to grant admin again after adding them.

upvoted 1 times

 **kmk\_01** 7 months, 4 weeks ago

No the answer is not correct. I have done many of these app registrations in the past 3 years.

It's Register App -> Configure permissions -> Provide Admin consent

upvoted 1 times

 **Bjarki2330** 1 year, 3 months ago

As others said, 2 and 3 are the other way around.

- 1) Create app registration
- 2) Add app permissions
- 3) Grant admin consent

upvoted 4 times

 **sapien45** 1 year, 5 months ago

Great videos guys

- 1) Create app registration
- 2) App Permission
- 3) Admin Consent

upvoted 5 times

 **RandomNickname** 1 year, 5 months ago

As far as I can see given answer is wrong way round for 2, 3.

See MS article;

<https://docs.microsoft.com/en-us/graph/permissions-reference>

So agree with others.

- 1: Create App registration.
- 2: Add App Permission
- 3: Grant Admin Consent

upvoted 2 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 2 times

 **stromnessian** 1 year, 9 months ago

Supplied answer is incorrect; grant admin consent is the final step, and comes after selecting permissions. App registration is obviously first.

upvoted 1 times

 **Pravda** 1 year, 10 months ago

Link in question confirms answer is correct.

upvoted 1 times

 **007Ali** 1 year, 10 months ago

Answer listed is correct, validated in a lab :-

1. Create an app registration
2. Admin Consent (Click on "Grant admin consent" button)
3. App Permission (Click Accept on the "Permissions requested Review for your organisation" prompt)

upvoted 1 times

 **Dreamhaxx** 2 years ago

Agreed Swap app permissions with admin consent

upvoted 3 times

 **med4** 2 years, 1 month ago

consent is last

upvoted 3 times

You have an Azure Active Directory (Azure AD) tenant that contains cloud-based enterprise apps.

You need to group related apps into categories in the My Apps portal.

What should you create?

- A. tags
- B. collections
- C. naming policies
- D. dynamic groups

**Correct Answer: B**

Reference:

<https://support.microsoft.com/en-us/account-billing/customize-app-collections-in-the-my-apps-portal-2dae6b8a-d8b0-4a16-9a5d-71ed4d6a6c1d>

Community vote distribution

B (100%)

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: B**

The correct answer is B. collections.

According to the Microsoft Entra documentation, collections are a way to group related applications on the My Apps portal<sup>1</sup>. You can create collections and assign them to users or groups, and they will see a separate tab for each collection on the portal. Collections help you organize the applications for your users based on their job role, task, project, or any other criteria you choose.

upvoted 2 times

 **EmnCours** 4 months, 1 week ago

**Selected Answer: B**

Correct Answer: B

upvoted 1 times

 **penatuna** 5 months, 2 weeks ago

**Selected Answer: B**

Your users can use the My Apps portal to view and start the cloud-based applications they have access to. By default, all the applications a user can access are listed together on a single page. To better organize this page for your users, if you have an Azure AD Premium P1 or P2 license you can set up collections. With a collection, you can group together applications that are related (for example, by job role, task, or project) and display them on a separate tab. A collection essentially applies a filter to the applications a user can already access, so the user sees only those applications in the collection that have been assigned to them.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/access-panel-collections>

upvoted 1 times

 **dule27** 5 months, 2 weeks ago

**Selected Answer: B**

B. collections

upvoted 1 times

 **AAsif098** 10 months ago

**Selected Answer: B**

Confirmed, correct answer is B

When you look at Myapps, first instance it shows Collection as the default

upvoted 1 times

 **Jawad1462** 1 year, 1 month ago

**Selected Answer: B**

Is the correct answer

upvoted 3 times

 **wooyourdaddy** 1 year, 6 months ago

**Selected Answer: B**

In the My Apps portal, applications appear in default collections and your custom app collections. The Apps collection in My Apps is a default collection that contains all the applications that have been assigned to you, sorted alphabetically.

B is the correct answer based on the link provided.  
upvoted 3 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

The Azure Active Directory (Azure AD) tenant contains the groups shown in the following table.

| Name   | Type                  |
|--------|-----------------------|
| Group1 | Security              |
| Group2 | Distribution          |
| Group3 | Microsoft 365         |
| Group4 | Mail-enabled security |

In Azure AD, you add a new enterprise application named App1.

Which groups can you assign to App1?

- A. Group1 only
- B. Group2 only
- C. Group3 only
- D. Group1 and Group4
- E. Group1 and Group3

#### Correct Answer: E

Using Azure Active Directory (Azure AD) with an Azure AD Premium license plan, you can use groups to assign access to a SaaS application that's integrated with Azure AD. For example, if you want to assign access for the marketing department to use five different SaaS applications, you can create an Office 365 or security group that contains the users in the marketing department, and then assign that group to these five SaaS applications that are needed by the marketing department.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-saasapps>

#### Community vote distribution

|         |         |    |
|---------|---------|----|
| D (67%) | E (30%) | 4% |
|---------|---------|----|

✉  **HelloItsSam** Highly Voted 9 months, 3 weeks ago

MS documentation is not up to date! Just tested in my tenant, all the below groups are supported

- 1- Security
- 2- Microsoft 365
- 3- Mail-Enabled security Group

upvoted 8 times

✉  **oopspruu** 2 months, 4 weeks ago

Source:

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal?pivot=portal>

upvoted 1 times

✉  **f2bf85a** 7 months, 2 weeks ago

I was also able to add a distribution list as an assigned group to an enterprise app.

It seems like the prerequisite is the attribute "securityEnabled" is not necessary either.

If you create M365 from Microsoft Admin center, securityEnabled attribute is by default set to No, but if you create M365 groups from Azure AD portal or Entra, securityEnabled is set to Yes.

But nevertheless, I could add all groups as assignments to the enterprise App.

upvoted 2 times

✉  **Arjanussie** 9 months, 1 week ago

I did the same test and indeed Hello is right

upvoted 1 times

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

**Selected Answer: E**

E

according to <https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal?pivot=portal>

upvoted 1 times

✉  **ACSC** 2 months, 1 week ago

Answer: E

Group-based assignment requires Microsoft Entra ID P1 or P2 edition. Group-based assignment is supported for Security groups and Microsoft 365 groups whose SecurityEnabled setting is set to True only. Nested group memberships aren't currently supported.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal?pivot=portal>

upvoted 3 times

□ **oopspruu** 2 months, 4 weeks ago

**Selected Answer: E**

As of today, 9/6/2023:

"Group-based assignment requires Azure Active Directory Premium P1 or P2 edition. Group-based assignment is supported for Security groups and Microsoft 365 groups whose SecurityEnabled setting is set to True only."

Answer is correct.

upvoted 3 times

□ **dule27** 5 months ago

**Selected Answer: D**

Group1, Group3 and Group 4

upvoted 2 times

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

You can use this feature only after you start an Azure AD Premium trial or purchase Azure AD Premium license plan. Group-based assignment is supported only for security groups. Nested group memberships are not supported for group-based assignment to applications at this time.

upvoted 1 times

□ **JN\_311** 6 months ago

**Selected Answer: E**

I tested adding M365 Group, was able to add group to enterprise app. Also the doco states it as well.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal?pivot=portal>

Group-based assignment requires Azure Active Directory Premium P1 or P2 edition. Group-based assignment is supported for Security groups and Microsoft 365 groups whose SecurityEnabled setting is set to True only.

upvoted 2 times

□ **f2bf85a** 7 months, 2 weeks ago

Tested it in my lab:

Seems like the question is outdated...

I was able to add all four kinds of groups (mail-enabled security, security, M365, distribution)

upvoted 1 times

□ **penatuna** 7 months, 2 weeks ago

"Group-based assignment requires Azure Active Directory Premium P1 or P2 edition. Group-based assignment is supported for Security groups and Microsoft 365 groups whose SecurityEnabled setting is set to True only. Nested group memberships aren't currently supported."

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal?pivot=portal>

upvoted 1 times

□ **LeTrinh** 9 months, 3 weeks ago

Group 1 only.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal?pivot=portal>

When you assign a group to an application, only users in the group will have access. The assignment doesn't cascade to nested groups.

Group-based assignment requires Azure Active Directory Premium P1 or P2 edition. Group-based assignment is supported for Security groups only. Nested group memberships and Microsoft 365 groups aren't currently supported.

upvoted 1 times

□ **mayleni** 9 months, 3 weeks ago

**Selected Answer: D**

Docs says that "you can use this feature only after you start an Azure AD Premium trial or purchase Azure AD Premium license plan. Group-based assignment is supported only for security groups. Nested group memberships are not supported for group-based assignment to applications at this time."

upvoted 1 times

□ **dizarm** 10 months ago

Just testet, and able to add Security, Microsoft 365 both assigned and dynamic and Security Mail-enabled. Not able to answer correctly.

upvoted 2 times

□ **Halwagy** 10 months, 1 week ago

**Selected Answer: A**

Group 1 only, as you cannot add APP to Mail-enabled security group , as Mail-Enabled security group assignment is handled from Exchange not from Azure AD.

upvoted 1 times

□ **Halwagy** 10 months, 1 week ago

my Mistake,

I understood wrongly,

recently , the following groups can be assigned to the EnterpriseApp, tested:  
Security, M365 Group, Mail-Enabled Security group  
upvoted 1 times

 **doch** 10 months, 2 weeks ago

**Selected Answer: D**

Sure.

- Group-based assignment is supported for Security groups only.
- Nested group memberships and Microsoft 365 groups aren't currently supported.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal?pivot=portal>  
upvoted 2 times

 **shouro88** 10 months, 3 weeks ago

tested in lab, can add m365 group to an enterprise app  
upvoted 2 times

 **anuj530** 11 months, 1 week ago

**Selected Answer: E**  
Just tested this and you can indeed assign it to Security and MS365 groups. I also checked the access and users in the 365 groups do have access to the app.  
<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-saasapps>  
This article states "For example, if you want to assign access for the marketing department to use five different SaaS applications, you can create an Office 365 or security group that contains the users in the marketing department, and then assign that group to these five SaaS applications that are needed by the marketing department."  
upvoted 2 times

 **hellboycze** 11 months, 1 week ago

**Selected Answer: D**  
Only security groups and mail-enabled security groups.  
M365 groups are not allowed  
upvoted 2 times

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name   | Role                         |
|--------|------------------------------|
| User1  | None                         |
| User2  | None                         |
| Admin1 | Application administrator    |
| Admin2 | Authentication administrator |

The User settings for enterprise applications have the following configurations:

- Users can consent to apps accessing company data on their behalf: No
- Users can consent to apps accessing company data for the groups they own: No
- Users can request admin consent to apps they are unable to consent to: Yes

Who can review admin consent requests: Admin2, User2

User1 attempts to add an app that requires consent to access company data.

Which user can provide consent?

- A. User1
- B. User2
- C. Admin1
- D. Admin2

**Correct Answer: C**

To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow>

Community vote distribution

C (100%)

 **oopspruu** 2 months, 4 weeks ago

**Selected Answer: C**

As of 9/6/2023:

The selected reviewers can act on (review, block, deny) new admin consent requests. All users can block and deny admin consent requests, but only users with the Global, Application, or Cloud application administrator role can grant admin consent.

upvoted 3 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: C**

Correct Answer: C

upvoted 3 times

 **dule27** 5 months, 2 weeks ago

**Selected Answer: C**

C. Admin1

upvoted 2 times

 **jack987** 11 months, 2 weeks ago

**Selected Answer: C**

The answer is correct - C. Admin1 Application Administrator

To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow>

upvoted 4 times

 **Jhill777** 1 year ago

Wrong. As a reviewer, you can view all admin consent requests but you can only act on those requests that were created after you were designated as a reviewer.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/review-admin-consent-requests>

upvoted 1 times

 **Jhill777** 1 year ago

Stand corrected. Link I posted is missing vital information that is only shown in the portal when you try to assign reviewers.  
"The selected reviewers can act on (review, block, deny) new admin consent requests. All users can block and deny admin consent requests, but only users with the Global, Application, or Cloud application administrator role can grant admin consent.  
upvoted 4 times

 **ccaitlab** 1 year ago

I'm not sure, because admin1 is not added as reviewer  
upvoted 1 times

 **Jawad1462** 1 year, 1 month ago

**Selected Answer: C**

Correct

upvoted 2 times

 **existingname** 1 year, 3 months ago

C is correct. In the exam today.  
upvoted 3 times

You have a Microsoft 365 subscription. The subscription contains users that use Microsoft Outlook 2016 and Outlook 2013 clients.

You need to implement tenant restrictions. The solution must minimize administrative effort.

What should you do first?

- A. Configure the Outlook 2013 clients to use modern authentication.
- B. Upgrade the Outlook 2013 clients to Outlook 2016.
- C. From the Exchange admin center, configure Organization Sharing.
- D. Upgrade all the Outlook clients to Outlook 2019.

**Correct Answer: B**

From October 13, 2020 onward, only these versions of Office are supported for connecting to Microsoft 365 (and Office 365) services:

Microsoft 365 Apps for enterprise (previously named Office 365 ProPlus)

Microsoft 365 Apps for business (previously named Office 365 Business)

Office LTSC 2021, such as Office LTSC Professional Plus 2021

Office 2019, such as Office Professional Plus 2019

Office 2016, such as Office Standard 2016

Note:

Office 2019 and Office 2016 will be supported for connecting to Microsoft 365 (and Office 365) services until October 2023.

Note: Client software: To support tenant restrictions, client software must request tokens directly from Azure AD, so that the proxy infrastructure can intercept traffic. Browser-based Microsoft 365 applications currently support tenant restrictions, as do Office clients that use modern authentication (like OAuth 2.0).

Reference:

<https://docs.microsoft.com/en-us/deployoffice/endofsupport/microsoft-365-services-connectivity> <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/tenant-restrictions>

*Community vote distribution*

B (61%)

A (39%)

 **palito1980** Highly Voted 1 year, 2 months ago

This is a very Microsoft question. Vague. Taking into consideration options and the fact that Office 2013 will reach the end of support on April 11, 2023, still supported, I'd go B as well.

Office clients that use modern authentication (like OAuth 2.0) support tenant restrictions. O2013 natively does not. Easiest, least admin workload would be to upgrade.

You could also <https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/enable-modern-authentication?view=o365-worldwide>.

But more workload than upgrade.

upvoted 6 times

 **PandaTuga** Highly Voted 11 months, 3 weeks ago

**Selected Answer: A**

Microsoft Office 2013 on Microsoft Windows computers supports Modern authentication. But, to turn it on, you need to configure the following registry keys

<https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/enable-modern-authentication?view=o365-worldwide>

upvoted 5 times

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

To implement tenant restrictions, you need to ensure that all your Outlook clients use modern authentication. Modern authentication is a method of identity management that offers more secure user authentication and authorization. It is based on OAuth 2.0, which enables apps to access Microsoft Entra-protected resources such as Exchange Online and SharePoint Online1.

According to the web search results, Outlook 2016 supports modern authentication by default, but Outlook 2013 requires some registry settings to be configured2. Therefore, the first step you should do is to configure the Outlook 2013 clients to use modern authentication. This will minimize the administrative effort compared to upgrading the Outlook clients to a newer version.

upvoted 1 times

 **DasChi\_cken** 3 months, 1 week ago

**Selected Answer: B**

Upgrade to the next Outlook Version ist definitely less administrative effort than changing registry keys

upvoted 2 times

 **Logitech** 2 months, 1 week ago

Not really, upgrade Office has much more impact on the Clients. The user won't even notice changing the registry key. But I would take B anyways.

upvoted 1 times

⊕ **EmnCours** 3 months, 3 weeks ago

**Selected Answer: A**

A. Configure the Outlook 2013 clients to use modern authentication.

upvoted 1 times

⊕ **dule27** 4 months, 4 weeks ago

**Selected Answer: A**

A. Configure the Outlook 2013 clients to use modern authentication.

upvoted 1 times

⊕ **Logitech** 2 months, 1 week ago

you think this is a good answer for MS, if Outlook 2013 is not even supported?

<https://learn.microsoft.com/en-us/deployoffice/endofsupport/microsoft-365-services-connectivity>

Office version Supported for connecting until this date

Microsoft 365 Apps Supported as long as you're using a supported version.

Office LTSC 2021 October 13, 2026

Office 2019 October 10, 2023

Office 2016 October 10, 2023

upvoted 1 times

⊕ **dule27** 5 months, 2 weeks ago

**Selected Answer: B**

B. Upgrade the Outlook 2013 clients to Outlook 2016.

upvoted 2 times

⊕ **dule27** 4 months, 4 weeks ago

Correction. Definitely

A. Configure the Outlook 2013 clients to use modern authentication.

upvoted 1 times

⊕ **SITM** 8 months ago

**Selected Answer: B**

I'll go with B

upvoted 2 times

⊕ **mayleni** 9 months, 3 weeks ago

**Selected Answer: B**

Vote B because Office 2013 is not supported, if you try maybe you can achieve the goal but is not supported so is not right for Microsoft.  
<https://learn.microsoft.com/en-us/deployoffice/endofsupport/microsoft-365-services-connectivity>

upvoted 5 times

⊕ **BTL\_Happy** 1 year ago

this question came out in my test today.

upvoted 2 times

⊕ **Hot\_156** 1 year, 2 months ago

very vague question... it is hard to tell if it is true or not lol

upvoted 1 times

⊕ **BRoald** 10 months, 4 weeks ago

A is true, because adding some register keys (and probably by GPO) is by far the least effort to do. If you upgrade from 2013 > 2016, it costs more effort and more time. So I would go with A

upvoted 3 times

**Selected Answer: A**

⊕ **dejo** 10 months, 1 week ago

I think I'm with you on this one!

upvoted 1 times

You have a Microsoft 365 E5 subscription.

You need to create a Microsoft Defender for Cloud Apps session policy.

What should you do first?

- A. From the Microsoft Defender for Cloud Apps portal, select User monitoring.
- B. From the Microsoft Defender for Cloud Apps portal, select App onboarding/maintenance.
- C. From the Azure Active Directory admin center, create a Conditional Access policy.
- D. From the Microsoft Defender for Cloud Apps portal, create a continuous report.

**Correct Answer: A**

*Community vote distribution*

C (82%)      A (18%)

✉ **Halwagy** Highly Voted 10 months, 2 weeks ago

**Selected Answer: C**

what I should do first is:

From the Azure Active Directory admin center, create a Conditional Access policy.

upvoted 14 times

✉ **ultraRunningCA** 9 months, 2 weeks ago

One of the prerequisites to using a session policy is "The relevant apps should be deployed with Conditional Access App Control", which is done via the Azure AD Admin Center

<https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad#prerequisites-to-using-session-policies>

<https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-deployment-aad>

----

If you assume that has been done, and the question relates to first steps in creating the actual Session Policy, I would say you'd need to Monitor first, to see the impact of the policy prior to deploying - which would make the answer A

upvoted 4 times

✉ **CloudLife** 5 months, 1 week ago

The comment suggests that one of the prerequisites for using a session policy is to deploy the relevant apps with Conditional Access App Control, which is done via the Azure AD Admin Center.

While this information is accurate, it highlights the prerequisite for using session policies rather than the first step in creating a session policy. The comment doesn't specifically explain why option A is the correct first step.

upvoted 1 times

✉ **EmnCours** Most Recent 4 months, 1 week ago

**Selected Answer: C**

Correct Answer: C

upvoted 1 times

✉ **dule27** 4 months, 4 weeks ago

**Selected Answer: C**

C. From the Azure Active Directory admin center, create a Conditional Access policy.

upvoted 1 times

✉ **CloudLife** 5 months, 1 week ago

**Selected Answer: C**

Based on the provided comments, it seems that there is some confusion regarding the first step in creating a Microsoft Defender for Cloud Apps session policy. While user monitoring may be a part of the overall configuration, the initial step should be creating a Conditional Access policy from the Azure Active Directory admin center (option C)

upvoted 2 times

✉ **dule27** 5 months, 1 week ago

**Selected Answer: A**

A. From the Microsoft Defender for Cloud Apps portal, select User monitoring.

upvoted 2 times

✉ **dule27** 4 months, 4 weeks ago

Correction: C. From the Azure Active Directory admin center, create a Conditional Access policy.  
upvoted 1 times

 **b233f0a** 5 months, 4 weeks ago

**Selected Answer: A**  
I think A. <https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad> "In the Microsoft 365 Defender portal, under Cloud Apps, go to Policies -> Policy management. Then select the Conditional access tab." It is therefore NOT C as that says to create a CA in Azure AD Admin. Later in the same link "Then, under Conditional Access App Control select User monitoring and unselect the Notify users checkbox."  
upvoted 2 times

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name   | Role                            |
|--------|---------------------------------|
| Admin1 | Cloud application administrator |
| Admin2 | Application administrator       |
| Admin3 | Security administrator          |
| User1  | None                            |

You add an enterprise application named App1 to Azure AD and set User1 as the owner of App1. App1 requires admin consent to access Azure AD before the app can be used.

You configure the Admin consent requests settings as shown in the following exhibit.

**Admin consent requests**

Users can request admin consent to apps they are unable to consent to  Yes  No

Who can review admin consent requests

| Reviewer type    | Reviewers         |
|------------------|-------------------|
| Users            | 4 users selected. |
| Groups (Preview) | + Add groups      |
| Roles (Preview)  | + Add roles       |

Selected users will receive email notifications for requests  Yes  No

Selected users will receive request expiration reminders  Yes  No

Consent request expires after (days)  30

Admin1, Admin2, Admin3, and User1 are added as reviewers.

Which users can review and approve the admin consent requests?

- A. Admin1 only
- B. Admin1, Admin2 and Admin3 only
- C. Admin1, Admin2, and User1 only
- D. Admin1 and Admin2 only
- E. Admin1, Admin2, Admin3, and User1

**Correct Answer:** D

Community vote distribution

 **Techfall** Highly Voted  10 months, 1 week ago

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow>

"To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator. The reviewer must already have one of these admin roles assigned; simply designating them as a reviewer doesn't elevate their privileges."

upvoted 5 times

 **OrangeSG** Most Recent  3 weeks, 1 day ago

To approve requests, a reviewer must have the permissions required to grant admin consent for the application requested. Simply designating them as a reviewer doesn't elevate their privileges.

To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator. The reviewer must already have one of these admin roles assigned; simply designating them as a reviewer doesn't elevate their privileges.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow>

upvoted 1 times

 **OrangeSG** 3 weeks, 1 day ago

Please ignore. Duplicate.

upvoted 1 times

 **cgonIT** 1 month, 3 weeks ago

Selected Answer: D

I go with D.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

Selected Answer: D

D. Admin1 and Admin2 only

upvoted 1 times

 **dule27** 5 months, 2 weeks ago

Selected Answer: D

D. Admin1 and Admin2 only

upvoted 1 times

 **doch** 10 months, 2 weeks ago

Selected Answer: D

Cloud App Admin and App Admin can grant consent.

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

upvoted 2 times

 **Halwagy** 10 months, 2 weeks ago

Selected Answer: D

the answer is correct, as user 1 can review , block and deny but not approve.

upvoted 2 times

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to be notified if a user downloads more than 50 files in one minute from Site1.

Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

- A. session policy
- B. activity policy
- C. file policy
- D. anomaly detection policy

**Correct Answer: B**

*Community vote distribution*

|         |    |
|---------|----|
| B (91%) | 9% |
|---------|----|

 **OrangeSG** 3 weeks, 1 day ago

**Selected Answer: B**

High download rate

You can set your activity policy so that you receive an alert when there has been an unexpected or uncharacteristic level of downloading activity. To configure this sort of policy, under Rate parameters, choose the parameters to trigger the alert.

<https://learn.microsoft.com/en-us/defender-cloud-apps/user-activity-policies#custom-alerts>  
upvoted 1 times

 **haazybanj** 4 weeks ago

**Selected Answer: B**

The correct answer is B. activity policy.

Activity policies in Microsoft Defender for Cloud Apps allow you to detect and respond to risky behavior in your cloud apps. You can use an activity policy to be notified if a user downloads more than 50 files in one minute from Site1.

upvoted 1 times

 **Obyte** 1 month ago

**Selected Answer: B**

Correct answer: B

Activity policy for Mass download by a single user

<https://learn.microsoft.com/en-us/defender-cloud-apps/policy-template-reference#policy-template-highlights>  
upvoted 1 times

 **Jzx** 2 months, 3 weeks ago

**Selected Answer: C**

C. File policy:

File policies in Microsoft Defender for Cloud Apps allow you to define rules and conditions related to file activities, such as uploads, downloads, and sharing. You can set up a file policy to monitor and alert on specific file-related actions, like the number of files downloaded in a given time frame. In this case, you want to monitor the download activity from Site1, so a file policy is the appropriate choice.

upvoted 1 times

 **Julesy** 1 month, 4 weeks ago

<https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies#policies>

There is no mention of downloads. Don't know where you got that.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: B**

B. activity policy

upvoted 2 times

 **dule27** 5 months, 2 weeks ago

**Selected Answer: B**

B. activity policy

upvoted 2 times

 **ThotSlayer69** 10 months, 1 week ago

**Selected Answer: B**

Custom alerts in Activity policies

<https://learn.microsoft.com/en-us/defender-cloud-apps/user-activity-policies>

upvoted 3 times

 **MRDP1** 10 months, 2 weeks ago

B is correct

upvoted 2 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 hosts PDF files.

You need to prevent users from printing the files directly from Site1.

Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

- A. activity policy
- B. access policy
- C. file policy
- D. session policy

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **Halwagy** Highly Voted 10 months, 2 weeks ago

**Selected Answer: D**

Correct

<https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad>

upvoted 5 times

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

Session policies

Block specific activities

When Block activities is set as the Activity type, you can select specific activities to block in specific apps. All activities from selected apps are monitored and reported in the Activity log. The specific activities you select are blocked if you select the Block action. The specific activities you selected raise alerts if you select the Test action and have alerts turned on.

Examples of blocked activities include:

Send Teams message: Use it to block messages sent from Microsoft Teams, or block Teams messages containing specific content

Print: Use it to block Print actions

Copy: Use it to block copy to clipboard actions or only block copy for specific content

Block specific activities and apply it to specific groups to create a comprehensive read-only mode for your organization.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: D**

D. session policy

upvoted 1 times

 **dule27** 5 months, 2 weeks ago

**Selected Answer: D**

D. session policy

upvoted 1 times

 **Taigr** 9 months, 3 weeks ago

**Selected Answer: D**

Yep, D is correct.

upvoted 2 times

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps and Conditional Access policies.

You need to block access to cloud apps when a user is assessed as high risk.

Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

- A. access policy
- B. OAuth app policy
- C. anomaly detection policy
- D. activity policy

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: A**

A. access policy  
upvoted 1 times

 **dule27** 5 months, 2 weeks ago

**Selected Answer: A**

A. access policy  
upvoted 1 times

 **mohsanarfandanish** 8 months, 1 week ago

**Selected Answer: A**

Sign in to the Microsoft Defender for Cloud Apps portal.  
Click on the Access policies tab.  
Click Create policy.  
upvoted 2 times

 **mohsanarfandanish** 8 months, 1 week ago

Correct is A  
upvoted 1 times

 **Zak366** 9 months, 2 weeks ago

**Selected Answer: A**

Correct. A  
Microsoft Defender for Cloud Apps access policies enable real-time monitoring and control over access to cloud apps based on user, location, device, and app.  
<https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad>  
upvoted 2 times

You have a Microsoft 365 E5 subscription.

Users authorize third-party cloud apps to access their data.

You need to configure an alert that will be triggered when an app requires high permissions and is authorized by more than 20 users.

Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

- A. anomaly detection policy
- B. OAuth app policy
- C. access policy
- D. activity policy

**Correct Answer: D**

*Community vote distribution*

B (100%)

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: B**

The correct answer is B. OAuth app policy.

An OAuth app policy is a type of policy that allows you to control the permissions and access of third-party apps that use OAuth to connect to your cloud apps, such as Microsoft 365, Google Workspace, and Salesforce. You can create an OAuth app policy based on various criteria, such as the app name, the permission level, the number of users who authorized the app, and the group memberships of those users. You can also set an alert action for the policy, which will notify you when an app meets the conditions you specified. For example, you can create an OAuth app policy that will alert you when there are apps that require a high permission level and are authorized by more than 20 users.

upvoted 2 times

 **Jzx** 2 months, 3 weeks ago

**Selected Answer: B**

B. OAuth app policy:

OAuth app policies in Microsoft Defender for Cloud Apps allow you to control and manage permissions and access granted to third-party cloud apps. You can define policies to monitor or block apps with specific permissions or behaviors. In this scenario, you want to monitor and set an alert condition for apps with high permissions and a certain level of user authorization. OAuth app policies are designed for this kind of control and monitoring.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: B**

B. OAuth app policy

upvoted 1 times

 **CloudLife** 5 months, 1 week ago

**Selected Answer: B**

An OAuth app policy allows you to manage and control the permissions granted to third-party cloud apps that users authorize to access their data. By creating an OAuth app policy in the Microsoft Defender for Cloud Apps portal, you can define specific rules and conditions for app permissions and access.

Option B, OAuth app policy, is the most appropriate choice for this scenario, as it specifically focuses on managing the authorization and permissions of third-party cloud apps. You can configure the policy to trigger an alert when an app requires high permissions and is AUTHorized by more than 20 users, allowing you to monitor and manage the app permissions in your Microsoft 365 environment.

upvoted 4 times

 **Razur3** 5 months, 1 week ago

If everyone agrees that OAuth app policy is the correct answer, why does the solution then tell me the correct answer is D?  
Is there something i am missing here?

upvoted 1 times

 **dule27** 5 months, 2 weeks ago

**Selected Answer: B**

B. OAuth app policy

upvoted 1 times

 **Arold75** 6 months, 2 weeks ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/defender-cloud-apps/app-permission-policy>

Reason :In addition to the existing investigation of OAuth apps connected to your environment, you can set permission policies so that you get automated notifications when an OAuth app meets certain criteria. For example, you can automatically be alerted when there are apps that require a high permission level and were authorized by more than 50 users.

upvoted 1 times

 **Taigr** 9 months, 3 weeks ago

**Selected Answer: B**

In addition to the existing investigation of OAuth apps connected to your environment, you can set permission policies so that you get automated notifications when an OAuth app meets certain criteria. For example, you can automatically be alerted when there are apps that require a high permission level and were authorized by more than 50 users.

upvoted 2 times

 **AWS56** 9 months, 3 weeks ago

**Selected Answer: B**

B is the answer

upvoted 1 times

 **mayleni** 9 months, 3 weeks ago

**Selected Answer: B**

Answer B. You can consult these docs and see the answer in the first paragraph <https://learn.microsoft.com/en-us/defender-cloud-apps/app-permission-policy>

upvoted 2 times

 **Breza** 10 months, 1 week ago

**Selected Answer: B**

B - OAuth Policy

upvoted 2 times

 **faeem** 10 months, 2 weeks ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/defender-cloud-apps/app-permission-policy>

In addition to the existing investigation of OAuth apps connected to your environment, you can set permission policies so that you get automated notifications when an OAuth app meets certain criteria. For example, you can automatically be alerted when there are apps that require a high permission level and were authorized by more than 50 users

upvoted 3 times

 **Halwagy** 10 months, 2 weeks ago

**Selected Answer: B**

Correct Answer B

upvoted 2 times

 **Eden\_911** 10 months, 2 weeks ago

Correct Answer: OAuth App Policy

<https://learn.microsoft.com/en-us/defender-cloud-apps/app-permission-policy>

upvoted 3 times

Your company has an Azure AD tenant that contains the users shown in the following table.

| Name  | Role                            |
|-------|---------------------------------|
| User1 | Application administrator       |
| User2 | None                            |
| User3 | Exchange administrator          |
| User4 | Cloud application administrator |

You have the app registrations shown in the following table.

| App name | Used by      | Microsoft Graph permission                                                  |
|----------|--------------|-----------------------------------------------------------------------------|
| App1     | User1        | Calendars.Read of type Delegated                                            |
| App2     | User2        | Calendars.Read of type Delegated<br>Calendars.ReadWrite of type Application |
| App3     | User3, User4 | Calendars.Read of type Application                                          |

A company policy prevents changes to user permissions.

Which user can create appointments in the calendar of each user at the company?

- A. User1
- B. User2
- C. User3
- D. User4

**Correct Answer: B**

*Community vote distribution*

B (92%)

8%

 **ehommes** 1 month, 2 weeks ago

B. User 2. See: <https://learn.microsoft.com/en-us/graph/permissions-reference>  
upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

The correct answer is C. User3.

User3 can create appointments in the calendar of each user at the company because User3 has the Calendar.ReadWrite permission for the App1 app registration. This permission allows User3 to read and write events in all calendars that the app can access.

User1, User2, and User4 cannot create appointments in the calendar of each user at the company because they do not have the Calendar.ReadWrite permission for any app registration. User1 and User2 only have the User.Read permission for App1 and App2, respectively. This permission allows them to read basic user profile information, but not calendar events. User4 does not have any permissions for any app registration.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: B**

B. User2  
upvoted 2 times

 **dule27** 5 months, 2 weeks ago

**Selected Answer: B**

B. User2  
upvoted 3 times

 **geschbenscht** 8 months, 3 weeks ago

**Selected Answer: B**

User2 is the only one with write permission

upvoted 3 times

✉ **lfbservices** 9 months ago

**Selected Answer: B**

User2 has Application.write Permission

upvoted 3 times

✉ **Halwagy** 10 months, 2 weeks ago

**Selected Answer: A**

Correct Answer A , user 1 only as API will read only

upvoted 1 times

✉ **wsrudmen** 10 months, 1 week ago

For me correct answer is B

User2 is the only one who has access to Application.write for the calendar.

upvoted 7 times

✉ **Halwagy** 10 months, 2 weeks ago

my mistake , the given answer is correct, User2

upvoted 2 times

✉ **Grimstad** 9 months, 1 week ago

I think this is incorrect. User2 only has access for App2. The question asks for which user can write to calendar for all users. The other users aren't assigned to App 2, so User2 won't be able to write anything for them.

upvoted 3 times

✉ **kmk\_01** 7 months, 4 weeks ago

That's not how app permissions work. User2 will be able to use App2, which has permissions to write to all calendars in the tenant.

upvoted 2 times

You have an Azure AD tenant that contains a user named User1 and a registered app named App1.

User1 deletes the app registration of App1.

You need to restore the app registration.

What is the maximum number of days you have to restore the app registration from when it was deleted?

- A. 14
- B. 30
- C. 60
- D. 180

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: B**

Correct Answer: B  
upvoted 1 times

 **dule27** 5 months, 2 weeks ago

**Selected Answer: B**

B. 30 days  
upvoted 1 times

 **kmk\_01** 7 months, 4 weeks ago

**Selected Answer: B**

Yes, it's 30 days. <https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-restore-app>  
upvoted 4 times

 **rikicm** 1 month, 3 weeks ago

Neither you nor Microsoft customer support can restore a permanently deleted application or an application deleted more than 30 days ago.  
upvoted 1 times

**HOTSPOT**

You have a Microsoft 365 tenant.

Sometimes, users use external, third-party applications that require limited access to the Microsoft 365 data of the respective user. The users register the applications in Azure AD.

You need to receive an alert if a registered application gains read and write access to the users' email.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Tool to use:

- Azure AD Identity Protection
- Identity Governance
- Microsoft Defender for Cloud Apps
- Microsoft Endpoint Manager

Policy type to create:

- App discovery
- App protection
- Conditional access
- OAuth app
- Sign-in risk
- User risk

**Answer Area**

Tool to use:

- Azure AD Identity Protection
- Identity Governance
- Microsoft Defender for Cloud Apps
- Microsoft Endpoint Manager

Correct Answer:

Policy type to create:

- App discovery
- App protection
- Conditional access
- OAuth app
- Sign-in risk
- User risk

 **kmk\_01** Highly Voted  7 months, 4 weeks ago

The answer is correct - <https://learn.microsoft.com/en-us/defender-cloud-apps/app-permission-policy>  
upvoted 7 times

 **JCkD4Ni3L** Most Recent ⓘ 1 month, 1 week ago

Answer is correct !

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

Tool: Microsoft Defender for Cloud Apps

Policy type: OAuth app

upvoted 1 times

 **dule27** 5 months, 2 weeks ago

Tool: Microsoft Defender for Cloud Apps

Policy type: OAuth app

upvoted 2 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

## Case Study -

## Overview -

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

## Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | <i>None</i>                       |
| User2 | <i>None</i>                       |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner       | Members                        |
|-------------|----------|-----------------|-------------|--------------------------------|
| IT_Group1   | Security | Assigned        | <i>None</i> | All users in the IT department |
| AdatumUsers | Security | Assigned        | <i>None</i> | User1, User2                   |

## Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

## Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

## Requirements. Planned Changes -

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

## Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You need implement the planned changes for application access to organizational data.

What should you configure?

- A. authentication methods
- B. the User consent settings
- C. access packages
- D. an application proxy

**Correct Answer: B**

*Community vote distribution*

53% (53%)

47% (47%)

marot Highly Voted 4 months, 1 week ago

**Selected Answer: C**

Azure Portal > Azure AD > Identity Governance > (Entitlement Management Heading) Access Packages > + New Access Package (from the top bar) > (Resources tab) + Applications > (Requests tab) in the section "users who can requests" we check box " for users in your directory), and then "all members(incl. guests), and then in the section " approval, we select "Yes" ..etc

upvoted 7 times

Hull 3 months, 1 week ago

One moment, either I'm reading the question and requirement wrong or the answer isn't correct. The requirement is:

Require admin approval for application access to organizational data.

To deny user consent for Azure applications, that can be done via User consent settings.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent?pivot=portal>

That means answer should be B, not C. Someone please correct me if I'm missing this question completely.

upvoted 6 times

penatuna 2 months, 3 weeks ago

I'm with the Hull on this one. Correct me if I'm wrong.

Requirements. Planned Changes:

Require admin approval for application access to organizational data.

"Before an application can access your organization's data, a user must grant the application permissions to do so. Different permissions allow different levels of access."

"To allow users to request an administrator's review and approval of an application that the user isn't allowed to consent to, enable the admin consent workflow. For example, you might do this when user consent has been disabled or when an application is requesting permissions that the user isn't allowed to grant."

If i understand correctly, you should first go to Identity > Applications > Enterprise applications > Consent and permissions > User consent settings. Under User consent for applications, choose Do not allow user consent.

Then you should enable the admin consent workflow:

Browse to Identity > Applications > Enterprise applications > Consent and permissions > Admin consent settings.

Under Admin consent requests, select Yes for Users can request admin consent to apps they are unable to consent to.

upvoted 3 times

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

**Selected Answer: B**

Only User Consent makes sense here

upvoted 1 times

 **itismadu** 1 month, 1 week ago

**Selected Answer: B**

To implement the requirement of requiring admin approval for application access to organizational data, you should configure:

B. the User consent settings

Configuring the User consent settings allows you to control whether users can grant consent to applications themselves or if admin approval is required for application access. By setting the User consent settings to "Require admin approval," you ensure that users cannot grant consent to applications accessing organizational data without the approval of an administrator.

Options A, C, and D do not directly address the specific requirement of requiring admin approval for application access. Authentication methods, access packages, and application proxy are related to different aspects of identity and access management, but they do not directly pertain to user consent settings and approval requirements.

upvoted 1 times

 **JCKD4Ni3L** 1 month, 1 week ago

**Selected Answer: B**

"Require admin approval for application access to \*\*\*organizational data\*\*\*" This can only be done through Admin Consent...

upvoted 2 times

 **JimboJones99** 1 month, 2 weeks ago

**Selected Answer: B**

Answer is B. Look at the next question "You configure User consent settings to allow users to provide consent to apps from verified publishers"

upvoted 1 times

 **DasChi\_cken** 1 month, 2 weeks ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **SumitSahoo** 1 month, 4 weeks ago

.....approval for application access (to data) needed

hence user need admin consent for approval.

upvoted 1 times

 **LC\_90** 2 months ago

**Selected Answer: B**

I agree with Hull and Penatuna, this link talks about using the User consent settings to get admin approval <https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow>

upvoted 2 times

You have an Azure AD tenant.

You configure User consent settings to allow users to provide consent to apps from verified publishers.

You need to ensure that the users can only provide consent to apps that require low impact permissions.

What should you do?

- A. Create an enterprise application collection.
- B. Create an access review.
- C. Create an access package.
- D. Configure permission classifications.

**Correct Answer: A**

*Community vote distribution*

D (100%)

 **haazybanj** 4 weeks, 1 day ago

**Selected Answer: D**

To ensure that users can only provide consent to apps that require low impact permissions, you should configure permission classifications in your Azure AD tenant.

Configuring permission classifications allows you to classify the permissions requested by apps into different impact levels, such as low, medium, or high. By assigning the appropriate impact level to each permission, you can control which apps users are allowed to consent to based on the impact level of the requested permissions

upvoted 1 times

 **JCkD4Ni3L** 1 month, 1 week ago

**Selected Answer: D**

Configure permission classifications for this...

upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

The correct answer is D. Configure permission classifications.

To ensure that the users can only provide consent to apps that require low impact permissions, you need to configure permission classifications in Azure AD. Permission classifications allow you to identify the impact that different permissions have according to your organization's policies and risk evaluations.

upvoted 1 times

 **Jzx** 2 months, 3 weeks ago

**Selected Answer: D**

D. Configure permission classifications:

Azure AD allows you to classify the permissions requested by apps into three categories: low, medium, and high impact. By configuring these permission classifications, you can define which permissions fall into each category. This enables you to ensure that users can only provide consent to apps requesting permissions classified as "low impact." This approach helps control the level of access users can grant to apps, aligning with your requirement.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: D**

I go with D

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-permission-classifications?pivot=portal>

upvoted 2 times

 **KrissB** 3 months, 3 weeks ago

D looks like the better answer, when creating a custom app policy you need to define the Permissions Classification:

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/manage-app-consent-policies?pivot=ms-powershell>. However this is overly complex as it seems the easiest thing to do is just select the radial to allow user consent to apps from trusted publishers, default impact is low. <https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent?pivot=portal>

upvoted 2 times

 **northgaterebel** 3 months, 1 week ago

I agree. There should be an answer of "Do Nothing" because once you select "Allow user consent for apps from verified publishers" it is already configured as desired. Awful question.

upvoted 1 times

 **einkaufacs** 4 months ago

**Selected Answer: D**

I go with D

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-permission-classifications?pivot=portal>

upvoted 4 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

**HOTSPOT**

You have a Microsoft 365 E5 subscription that contains a user named User1.

You configure app governance integration.

User1 needs to view the App governance dashboard. The solution must use the principle of the least privilege.

Which role should you assign to User1, and which portal should User1 use to view the dashboard? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area****Role:**

- Application Administrator
- Application Developer
- Cloud Application Administrator

**Portal:**

- The Microsoft 365 admin center
- The Microsoft 365 Defender portal
- The Microsoft Defender for Cloud Apps portal
- The Microsoft Purview compliance portal

**Answer Area****Role:**

- Application Administrator
- Application Developer
- Cloud Application Administrator

**Correct Answer:****Portal:**

- The Microsoft 365 admin center
- The Microsoft 365 Defender portal
- The Microsoft Defender for Cloud Apps portal
- The Microsoft Purview compliance portal

 **haazybanj** 2 weeks, 3 days ago

Cloud Application Administrator

Microsoft 365 Defender Portal

upvoted 1 times

 **haazybanj** 3 weeks, 6 days ago

Roles

You must have one of these roles to turn on app governance:

Global Admin

Company Admin  
Security Admin  
Compliance Admin  
Compliance Data Admin  
Cloud App Security admin

One of the following administrator roles is required to see app governance pages or manage policies and settings:

Application Administrator  
Cloud Application Administrator  
Company or Global Administrator  
Compliance Administrator  
Compliance Data Administrator  
Global Reader  
Security Administrator  
Security Operator  
Security Reader (read-only)

<https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started#roles>  
upvoted 1 times

曰 **N05H3LL** 1 month ago

The "Application Administrator" role indeed has the necessary permissions to view and manage enterprise applications within the Azure and Microsoft 365 ecosystems. However, if the goal is to adhere strictly to the principle of least privilege, the "Cloud Application Administrator" role is more specific and restrictive, granting only the permissions necessary to perform the task without including broader administrative capabilities that an Application Administrator would have.

As for the portal choice, the Microsoft 365 Defender portal integrates security management across Microsoft 365 services. However, for app-specific governance and monitoring, Microsoft Defender for Cloud Apps is the specialized portal that provides a dedicated environment for managing cloud app security, including the app governance features.

So, while the Application Administrator role and the Microsoft 365 Defender portal could potentially be used to view the App governance dashboard, the Cloud Application Administrator role paired with the Microsoft Defender for Cloud Apps portal is a more direct match for the task, aligning better with the principle of least privilege and the specific focus on app governance.

upvoted 2 times

曰 **haazybanj** 1 month, 1 week ago

Cloud Application Administrator  
Microsoft 365 Defender Portal  
upvoted 1 times

曰 **DasChi\_cken** 3 months, 1 week ago

Box 1: Application Administrator  
Box 2: M365 Defender Portal

User1 needs to review all Apps and Not Cloud Apps only

upvoted 4 times

曰 **EmnCours** 3 months, 3 weeks ago

Role: Cloud Application Administrator  
Portal: The Microsoft 365 Defender Portal  
upvoted 4 times

曰 **nils241** 4 months ago

Box 1: M365 Defender Portal  
Box 2: Application Administrator (Read-only)

<https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started#roles>  
upvoted 1 times

曰 **northgaterebel** 3 months, 3 weeks ago

Role: Cloud Application Administrator  
Portal: The Microsoft 365 Defender Portal

According to your link, Cloud Application Administrator has the same permissions to the M365 Defender Portal and has less total privileges than Application Administrator.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>  
upvoted 4 times

You have an Azure subscription.

You are evaluating enterprise software as a service (SaaS) apps.

You need to ensure that the apps support automatic provisioning of Azure AD users.

Which specification should the apps support?

- A. OAuth 2.0
- B. WS-Fed
- C. SCIM 2.0
- D. LDAP 3

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: C**

C. SCIM 2.0

SCIM (System for Cross-domain Identity Management) is a protocol specifically designed for automating user provisioning and deprovisioning between identity providers like Azure AD and SaaS applications. It allows for automatic synchronization of user accounts, groups, and roles between systems, making it a common choice for SaaS app integration with identity providers like Azure AD.

upvoted 1 times

 **Jzx** 2 months, 3 weeks ago

**Selected Answer: C**

C. SCIM 2.0 (System for Cross-domain Identity Management):

SCIM is a standard protocol for automating the exchange of user identity information between identity domains, including cloud-based SaaS applications and identity providers like Azure AD. SCIM 2.0 is specifically designed for this purpose and provides a standardized way to create, read, update, and delete user accounts in a SaaS app from the identity provider. Azure AD uses SCIM for provisioning users to applications that support it.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: C**

C.SCIM

<https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/user-provisioning>

upvoted 1 times

 **nils241** 4 months ago

**Selected Answer: C**

C

<https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/user-provisioning>

or

<https://techcommunity.microsoft.com/t5/security-compliance-and-identity/provisioning-with-scim-getting-started/ba-p/880010>

upvoted 1 times

You have an Azure AD tenant and a .NET web app named App1.

You need to register App1 for Azure AD authentication.

What should you configure for App1?

- A. the executable name
- B. the bundle ID
- C. the package name
- D. the redirect URI

**Correct Answer: D**

*Community vote distribution*

D (100%)

✉ **haazybanj** 4 weeks, 1 day ago

**Selected Answer: D**

The redirect URI is the endpoint where Azure AD will send the authentication response after a user successfully authenticates with Azure AD. It is an essential configuration for enabling the authentication flow between Azure AD and the .NET web app.

upvoted 2 times

✉ **penatuna** 1 month ago

**Selected Answer: D**

Settings for each application type, including redirect URIs, are configured in Platform configurations in the Azure portal. Some platforms, like Web and Single-page applications, require you to manually specify a redirect URI. For other platforms, like mobile and desktop, you can select from redirect URIs generated for you when you configure their other settings.

- A. Executable name is a program binary name, i.e. Cool Program.app/CoolProgram
- B. Bundle ID is for iOS / macOS platform.
- C. Package name is for Android platform.
- D. Redirect URI's are used for Web applications, single-page applications and Mobile and desktop applications platforms.

<https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app#add-a-redirect-uri>

<https://learn.microsoft.com/en-us/entra/identity-platform/reply-url>

upvoted 2 times

✉ **JCkD4Ni3L** 1 month, 1 week ago

**Selected Answer: D**

The correct answer is D. the redirect URI. When registering a .NET web app named App1 for Azure AD authentication, you need to configure the redirect URI. This is the location where the authorization server sends the user once the app has been successfully authorized and granted an authorization code or access token. The redirect URI must match one of the URIs registered for the app in Azure AD. The other options (A. the executable name, B. the bundle ID, C. the package name) are typically used for native apps or mobile apps, not web apps.

upvoted 1 times

✉ **ACSC** 2 months ago

**Selected Answer: D**

correct answer

upvoted 1 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a notification through the Microsoft Authenticator app
- B. security questions
- C. voice
- D. Windows Hello for Business

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **haazybanj** 4 weeks, 1 day ago

**Selected Answer: D**

The redirect URI is the endpoint where Azure AD will send the authentication response after a user successfully authenticates with Azure AD. It is an essential configuration for enabling the authentication flow between Azure AD and the .NET web app.

upvoted 1 times

 **Pixan** 1 month ago

Hi Everyone!!

Join ET and get actual and valid study material: <https://examtopics.quora.com/> and pass your exam in first attempt. Study Smart Not Hard

upvoted 1 times

 **penatuna** 1 month ago

**Selected Answer: D**

A. A notification through the Microsoft Authenticator app requires connectivity to send the verification code to the device requesting the logon. You can use authenticators OTP but you won't receive a notification.

B. Security questions are not used as an authentication method but can be used during the self-service password reset (SSPR) process.

C. Voice. Cannot be voice as users have a mobile phone but no connectivity from this remote location.

D. Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a type of user credential that is tied to a device and uses a biometric or PIN. The user in this case have their laptops and Internet access.

Plan your multi-factor authentication deployment - Training | Microsoft Learn

upvoted 2 times

 **penatuna** 1 month ago

<https://learn.microsoft.com/en-us/training/modules/secure-aad-users-with-mfa/3-planning-mfa>

upvoted 1 times

 **JCkD4Ni3L** 1 month, 1 week ago

**Selected Answer: D**

With no Cellular network or data coverage, the only solution is a local MFA method, Windows Hello for Business is the only solution that doesn't require a mobile device.

upvoted 1 times

 **ACSC** 2 months ago

**Selected Answer: D**

correct answer

upvoted 1 times

You have an Azure AD tenant.

You discover that a large number of new apps were added to the tenant.

You need to implement an approval process for new enterprise applications.

What should you do?

- A. From the Microsoft Defender for Cloud Apps portal, create a Cloud Discovery anomaly detection policy.
- B. From the Microsoft Entra admin center, configure the Admin consent settings.
- C. From the Microsoft Defender for Cloud Apps portal, configure an app connector.
- D. From the Microsoft Entra admin center, configure an access review.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **haazybanj** 4 weeks, 1 day ago

**Selected Answer: B**

To implement an approval process for new enterprise applications in your Azure AD tenant, you should configure the Admin consent settings from the Microsoft Azure admin center.

upvoted 1 times

 **ACSC** 2 months ago

**Selected Answer: B**

correct. <https://practical365.com/use-azure-ad-admin-consent-requests-to-help-avoid-attacks-against-your-users/>

upvoted 1 times

You have a Microsoft 365 E5 subscription.

You purchase the app governance add-on license.

You need to enable app governance integration.

Which portal should you use?

- A. the Microsoft Defender for Cloud Apps portal
- B. the Microsoft 365 admin center
- C. Microsoft 365 Defender
- D. the Azure Active Directory admin center
- E. the Microsoft Purview compliance portal

**Correct Answer: C**

*Community vote distribution*

C (86%)

14%

 **haazybanj** 3 weeks ago

**Selected Answer: C**

Answer is C

<https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started#turn-on-app-governance>

upvoted 1 times

 **haazybanj** 4 weeks, 1 day ago

**Selected Answer: A**

To enable app governance integration for your Microsoft 365 E5 subscription, you should use the Microsoft Defender for Cloud Apps portal.

The Microsoft Defender for Cloud Apps portal provides comprehensive app governance capabilities, allowing you to monitor and control the usage of cloud apps within your organization. It helps you discover and assess the risk associated with different apps, enforce policies, and gain insights into app usage and permissions.

upvoted 1 times

 **haazybanj** 3 weeks ago

Answer is C:

<https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started#turn-on-app-governance>

upvoted 1 times

 **re\_zen** 3 weeks, 5 days ago

Turn on app governance

If your organization satisfies the prerequisites, go to Microsoft 365 Defender > Settings > Cloud Apps > App governance and select Use app governance

<https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started#turn-on-app-governance>

upvoted 1 times

 **JcKD4Ni3L** 1 month, 1 week ago

**Selected Answer: C**

The correct answer is C. Microsoft 365 Defender. To enable app governance integration, you should use the Microsoft 365 Defender portal. After satisfying all the prerequisites, you can navigate to Microsoft 365 Defender settings page and turn on app governance. The other options (A. the Microsoft Defender for Cloud Apps portal, B. the Microsoft 365 admin center, D. the Azure Active Directory admin center, E. the Microsoft Purview compliance portal) are not used for this specific task.

upvoted 1 times

 **ACSC** 2 months ago

**Selected Answer: C**

correct. <https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started#turn-on-app-governance>

upvoted 4 times

Your company purchases a new Microsoft 365 E5 subscription and an app named App1.

You need to create a Microsoft Defender for Cloud Apps access policy for App1.

What should you do first?

- A. Configure a Conditional Access policy to use app-enforced restrictions.
- B. Configure a Token configuration for App1.
- C. Add an API permission for App1.
- D. Configure a Conditional Access policy to use Conditional Access App Control.

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **haazybanj** 3 weeks ago

**Selected Answer: D**

The correct answer is D. Configure a Conditional Access policy to use Conditional Access App Control.

Before creating a Microsoft Defender for Cloud Apps access policy for App1, you need to configure a Conditional Access policy to use Conditional Access App Control (CAAC). CAAC is a feature of Microsoft Defender for Cloud Apps that allows you to control how users access cloud apps.

upvoted 1 times

 **JCKD4Ni3L** 1 month, 1 week ago

**Selected Answer: D**

The correct answer is D. Configure a Conditional Access policy to use Conditional Access App Control. Before creating a Microsoft Defender for Cloud Apps access policy for App1, you need to configure a Conditional Access policy to use Conditional Access App Control. This is because Microsoft Defender for Cloud Apps access policies enable real-time monitoring and control over access to cloud apps based on user, location, device, and app1. You can create access policies for any device, including devices that aren't Hybrid Azure AD Join and not managed by Microsoft Intune. The other options (A. Configure a Conditional Access policy to use app-enforced restrictions, B. Configure a Token configuration for App1, C. Add an API permission for App1) are not the first steps in this process.

upvoted 1 times

 **ACSC** 2 months ago

**Selected Answer: D**

correct answer. <https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad#how-it-works>

upvoted 1 times

**Case Study -****Overview -**

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure AD tenant named fabrikam.com.

**Existing Environment. Existing Environment**

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso\_Resources. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

**Existing Environment. Microsoft 365/Azure Environment**

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security E5
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

**Existing Environment. Problem Statements**

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named A. Datum Corporation. One hundred new A. Datum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirements. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

You need to meet the planned changes and technical requirements for App1.

What should you implement?

- A. a policy set in Microsoft Intune
- B. Azure AD Application Proxy
- C. an app configuration policy in Microsoft Intune
- D. an app registration in Azure AD

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **ACSC** 2 months ago

**Selected Answer: D**

correct answer  
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 an Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.

You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the Google Workspace app connector.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

*Community vote distribution*

A (100%)

✉  JimboJones99 1 month, 2 weeks ago

**Selected Answer: A**

I think A:Yes

OAuth app management is available only after connecting one or more of the supported platforms - Microsoft 365, Google Workspace, or Salesforce. Once connected, the OAuth apps menu option will appear under Investigate.

<https://learn.microsoft.com/en-us/defender-cloud-apps/manage-app-permissions>

upvoted 3 times

✉  cgonIT 1 month, 3 weeks ago

**Selected Answer: A**

Correct Answer: A, Yes.

Tested in lab. There is no way to detect signals from Google Workspace, for example, if you do not add first an app connector. So this answer is YES.

upvoted 2 times

✉  cgonIT 1 month, 3 weeks ago

I'm re-thinking the answer. In the official doc says:

"OAuth app management is available only after connecting one or more of the supported platforms - Microsoft 365, Google Workspace, or Salesforce."

So connector is mandatory (but for Google Workspace Subscription). What about the others?

If Microsoft specifies that only connecting Google Workspace it solves the other 2 apps monitorings... the answer would be "NO".

If states only for Google Workspace... the answer would be "YES".

What to choose?

upvoted 2 times

✉  rikicm 1 month, 3 weeks ago

**Selected Answer: A**

Microsoft Defender for Cloud Apps is now part of Microsoft 365 Defender, which correlates signals from across the Microsoft Defender suite and provides incident-level detection, investigation, and powerful response capabilities. For more information, see Microsoft Defender for Cloud Apps in Microsoft 365 Defender.

upvoted 2 times

 **ACSC** 2 months ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/defender-cloud-apps/manage-app-permissions>

upvoted 2 times

Question #38

Topic 3

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 an Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.

You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the Microsoft Azure app connector.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

*Community vote distribution*

B (67%)

A (33%)

 **cgonIT** 1 month, 3 weeks ago

**Selected Answer: B**

Correct Answer. B, No.

The way to manage those third party apps is through the Microsoft Defender for Cloud Apps -> App Connector. If not, there is no way to detect and investigate them.

<https://learn.microsoft.com/en-us/defender-cloud-apps/manage-app-permissions>

upvoted 1 times

 **rikicm** 1 month, 3 weeks ago

**Selected Answer: A**

Microsoft Entra admin center

upvoted 1 times

 **ACSC** 2 months ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/defender-cloud-apps/manage-app-permissions>

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 an Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.

You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the Amazon Web Services app connector.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: A**

*Community vote distribution*

A (57%)

B (43%)

 **Sorrynotsorry** 2 weeks, 3 days ago

**Selected Answer: B**

AWS is not an option to add in MDCA  
upvoted 1 times

 **OrangeSG** 3 weeks, 1 day ago

**Selected Answer: B**

Solution: From the Microsoft 365 Defender portal, you add the Google Workspace app connector.  
upvoted 1 times

 **JimboJones99** 1 month, 2 weeks ago

**Selected Answer: A**

A: Yes

<https://learn.microsoft.com/en-us/defender-cloud-apps/connect-aws>  
upvoted 4 times

 **ACSC** 2 months ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/defender-cloud-apps/manage-app-permissions>  
upvoted 1 times

 **syougun200x** 1 month, 2 weeks ago

Thanks, found the below on the linked page.

OAuth app management is available only after connecting one or more of the supported platforms - Microsoft 365, Google Workspace, or Salesforce. Once connected, the OAuth apps menu option will appear under Investigate.  
upvoted 2 times

Your company purchases a Microsoft 365 E5 subscription.

A user named User1 is assigned the Security Administrator role.

You need to ensure that User1 can create Microsoft Defender for Cloud Apps session policies.

What should you do first?

- A. Create a Conditional Access policy and select Require app protection policy.
- B. Create a Conditional Access policy and select Use Conditional Access App Control.
- C. Assign the Cloud Application Administrator role to User1.
- D. Assign the Cloud App Security Administrator role to User1.

**Correct Answer: B**

*Community vote distribution*

B (86%)

14%

 **MacDanorld** 1 week, 1 day ago

Personally, don't think the options make sense especially A and B, if B turn out to be the answer they want. Yes the Security Admin role is able to create the policy in question, but option B does not make sense as the correct answer to the question. How does "Create a Conditional Access policy and select Use Conditional Access App Control". sound like a likely answer to this question? to me, the question does not have an answer.  
upvoted 1 times

 **vaaws** 1 month ago

The Security Administrator role does not have the permissions to create Microsoft Defender for Cloud Apps session policies. You must assign the Cloud App Security Administrator role to User1.

Once you have assigned the Cloud App Security Administrator role to User1, you can create a Conditional Access policy that requires users to use Conditional Access App Control. This will ensure that User1 can create Microsoft Defender for Cloud Apps session policies.

D

upvoted 1 times

 **re\_zen** 3 weeks, 4 days ago

Security Administrator does have the permissions to create Microsoft Defender for Cloud Apps session policies.

<https://learn.microsoft.com/en-us/defender-cloud-apps/manage-admins#roles-and-permissions>

upvoted 1 times

 **JimboJones99** 1 month, 1 week ago

**Selected Answer: B**

B. Security Admin already has permission to create policies

Global administrator and Security administrator: Administrators with Full access have full permissions in Defender for Cloud Apps. They can add admins, add policies and settings, upload logs and perform governance actions, access and manage SIEM agents.

<https://learn.microsoft.com/en-us/defender-cloud-apps/manage-admins#microsoft-365-and-azure-ad-roles-with-access-to-defender-for-cloud-apps>

upvoted 2 times

 **itismadu** 1 month, 1 week ago

**Selected Answer: D**

D. Assign the Cloud App Security Administrator role to User1.

The Cloud App Security Administrator role provides the necessary permissions to create and manage session policies within Microsoft Defender for Cloud Apps (formerly known as Microsoft Cloud App Security). By assigning this role to User1, they will have the appropriate privileges to create and configure session policies for securing cloud applications and services.

Option C is not the correct choice as the Cloud Application Administrator role is not specifically related to Microsoft Defender for Cloud Apps session policies.

Options A and B are not directly related to assigning the necessary permissions for creating session policies within Microsoft Defender for Cloud Apps. These options pertain to setting up Conditional Access policies and Conditional Access App Control, which are different from configuring session policies in Microsoft Defender for Cloud Apps.

upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

The correct answer is D. Assign the Cloud App Security Administrator role to User1.

According to the Microsoft Entra built-in roles article<sup>1</sup>, the Cloud App Security Administrator role grants full permissions in Defender for Cloud Apps. Users with this role can create and manage all aspects of Defender for Cloud Apps session policies, which are used to monitor and control user sessions in cloud apps.

upvoted 4 times

 **cgonIT** 1 month, 3 weeks ago

**Selected Answer: B**

Answer . B. Create a Conditional Access policy and select Use Conditional Access App Control.

References:

<https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad#prerequisites-to-using-session-policies>

"The relevant apps should be deployed with Conditional Access App Control"

"Make sure you've configured your IdP solution to work with Defender for Cloud Apps, as follows:

- For Azure AD Conditional Access, see Configure integration with Azure AD
- For other IdP solutions, see Configure integration with other IdP solutions"

upvoted 2 times

 **rikicm** 1 month, 3 weeks ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad>

upvoted 2 times

You have an Azure subscription that contains a user named User1.

The App registration settings for the Azure AD tenant are configured as shown in the following exhibit.

## Enterprise applications

Manage how end users launch and view their applications

### App registrations

Users can register applications ⓘ

Yes

No

User1 builds an ASP.NET web app named App1.

You need to ensure that User1 can register App1. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Application Developer
- B. Cloud App Security Administrator
- C. Cloud Application Administrator
- D. Application Administrator

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **OrangeSG** 3 weeks, 1 day ago

**Selected Answer: A**

"Assign the Application Developer role to grant the ability to create application registrations when the Users can register applications setting is set to No. This role also grants permission to consent on one's own behalf when the Users can consent to apps accessing company data on their behalf setting is set to No."

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-app-roles#grant-individual-permissions-to-create-and-consent-to-applications-when-the-default-ability-is-disabled>

upvoted 1 times

## HOTSPOT

You have an Azure subscription that contains the resources shown in the following table.

| Name     | Type             | Location |
|----------|------------------|----------|
| RG1      | Resource group   | East US  |
| Managed1 | Managed identity | East US  |
| Managed2 | Managed identity | West US  |

The subscription contains the virtual machines shown in the following table.

| Name | Location | Identity        |
|------|----------|-----------------|
| VM1  | East US  | System-assigned |
| VM2  | West US  | System-assigned |
| VM3  | East US  | Managed1        |
| VM4  | West US  | None            |

Which identities can be assigned the Owner role for RG1, and to which virtual machines can you assign Managed2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Identities with Owner role:

- Managed1 only
- Managed1, VM1, and VM3 only
- Managed1, Managed2, and VM1 only
- Managed1, Managed2, VM1, and VM2 only
- Managed1, Managed2, VM1, VM2, and VM3 only

Virtual machines assigned to Managed2:

- VM4 only
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM1, VM2, VM3, and VM4

### Answer Area

Identities with Owner role:

- Managed1 only
- Managed1, VM1, and VM3 only
- Managed1, Managed2, and VM1 only
- Managed1, Managed2, VM1, and VM2 only
- Managed1, Managed2, VM1, VM2, and VM3 only

Correct Answer:

Virtual machines assigned to Managed2:

- VM4 only
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM1, VM2, VM3, and VM4

cloutchase1337 2 weeks, 2 days ago

Tested in lab.

Box1 Managed1,Managed2,VM1,VM2 and VM3 only

System-assigned identity is not region restricted,

User-assigned is not as well.

When you add the VM1 with a system assigned identity as an owner on the RG.

You can see in the RG RBAC permissions that the VM is added and it is created like an enterprise application.

Box2 All VMs.

Since user/system isn't restricted.

upvoted 1 times

vawws 3 weeks, 1 day ago

Box 1 Managed1,Managed2,VM1,VM2 and VM3 only

Box 2 VM1,VM2,VM3 and VM4

upvoted 3 times

haazybanj 3 weeks ago

Can you explain how you arrived at this?

upvoted 1 times

curtmcgirt 2 weeks, 5 days ago

guessing vawws logic is:

Box 1: any identity (not vm4)

Box 2: any VM in any region

while the answer given by ET seems to be:

Box 1: only identities in eastUS, where the RG lives

Box 2: only VMs in westus where Managed2 lives

upvoted 1 times

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

You plan to increase app security for the subscription.

You need to identify which apps do NOT require user authentication.

What should you do in the Microsoft 365 Defender portal?

- A. Review the cloud app catalog.
- B. Create an OAuth policy and review alerts.
- C. Create a snapshot Cloud Discovery report.
- D. Create a discovered app query.

**Correct Answer: D**

*Community vote distribution*

A (100%)

 **haazybanj** Highly Voted 3 weeks, 6 days ago

**Selected Answer: A**

A is the right answer>

Tested and confirmed you can filter to see apps that require user authentication from both cloud app catalog and Cloud discovery  
upvoted 5 times

 **haazybanj** Most Recent 4 weeks, 1 day ago

**Selected Answer: A**

To identify which apps do NOT require user authentication in the Microsoft 365 Defender portal, you should review the cloud app catalog.

Reviewing the cloud app catalog in the Microsoft 365 Defender portal provides you with a comprehensive list of all the apps connected to your Microsoft 365 environment. It allows you to see which apps require user authentication and which ones do not.

upvoted 4 times

#### Topic 4 - Question Set 4

You have a Microsoft 365 tenant.

In Azure Active Directory (Azure AD), you configure the terms of use.

You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.

What should you configure?

- A. an access policy in Microsoft Cloud App Security.
- B. Terms and conditions in Microsoft Endpoint Manager.
- C. a conditional access policy in Azure AD
- D. a compliance policy in Microsoft Endpoint Manager

**Correct Answer: C**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

Community vote distribution

C (86%) 14%

✉ **zed01** Highly Voted 2 years, 6 months ago

correct

upvoted 9 times

✉ **haazybanj** Most Recent 4 weeks, 1 day ago

**Selected Answer: C**

To ensure that only users who accept the terms of use can access the resources in your Microsoft 365 tenant, you should configure a conditional access policy in Azure AD.

A conditional access policy allows you to define specific conditions and requirements for user access to resources based on various factors such as user location, device, and user actions. By configuring a conditional access policy, you can enforce the acceptance of terms of use as a prerequisite for accessing resources in your Microsoft 365 tenant.

upvoted 1 times

✉ **cgonIT** 1 month, 3 weeks ago

**Selected Answer: C**

Tested in lab. IMHO answer should be "C".

The correct steps to accomplish this actions are:

- Create a Terms of Use from: Conditional Access -> Terms of Use. At the end, select "Custom Policy" under "Conditional Access -> Enforce with conditional access policy templates".
- Finish the Conditional Access policy with granular configurations.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

upvoted 1 times

✉ **EmnCours** 4 months, 1 week ago

**Selected Answer: C**

Correct Answer: C

upvoted 1 times

✉ **EmnCours** 3 months, 3 weeks ago

C. a conditional access policy in Azure AD

upvoted 1 times

✉ **dule27** 5 months, 2 weeks ago

**Selected Answer: C**

C. a conditional access policy in Azure AD

upvoted 1 times

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

**Selected Answer: C**

correct

upvoted 1 times

✉ **ra1paul** 9 months, 2 weeks ago

"only users who accept the terms of use can access the resources in the tenant. Other users must be denied access."  
So it's "C" because it's a condition.  
upvoted 2 times

□ **Imee** 1 year, 2 months ago  
on the exam 09222022, i answered the same. Passed the exam, btw.  
upvoted 1 times

□ **Xyz\_40** 1 year, 5 months ago  
absolutely correct to the best of my knowledge  
upvoted 2 times

□ **RandomNickname** 1 year, 6 months ago

**Selected Answer: C**

Conditional access is correct.  
See the link "How to deploy terms of use policy in AZAD" referenced in the MS article;  
<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>  
upvoted 2 times

□ **wooyourdaddy** 1 year, 6 months ago

**Selected Answer: B**

'Terms of Use' is one of the parts that can be configured in a conditional access policy.  
upvoted 2 times

□ **curtmcgirt** 2 weeks, 4 days ago

and 'conditional access policy' is C, not B.  
upvoted 1 times

□ **stromnessian** 1 year, 9 months ago

**Selected Answer: C**

Yes, it's Conditional Access.  
upvoted 2 times

□ **zmlapq99** 1 year, 10 months ago

On exam few days ago.  
upvoted 1 times

□ **Pravda** 1 year, 10 months ago

On the exam 1/20/2022  
upvoted 1 times

□ **Hooters** 1 year, 10 months ago

**Selected Answer: C**  
terms of use is part of conditional access  
upvoted 3 times

□ **007Ali** 1 year, 10 months ago

Correct configure Condition Access Terms of Use, at: Azure AD Conditional Access - Policies - Policy Name - Grant - myToUname - Terms Of Use Policy (Create the ToU settings first)  
upvoted 3 times

□ **Discuss4certi** 2 years, 2 months ago

correct the terms of use can be set in the conditional access tab.  
upvoted 4 times

You have an Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

| Name   | Type          | Membership type |
|--------|---------------|-----------------|
| Group1 | Security      | Assigned        |
| Group2 | Security      | Dynamic User    |
| Group3 | Security      | Dynamic Device  |
| Group4 | Microsoft 365 | Assigned        |
| Group5 | Microsoft 365 | Dynamic User    |

For which groups can you create an access review?

- A. Group1 only
- B. Group1 and Group4 only
- C. Group1 and Group2 only
- D. Group1, Group2, Group4, and Group5 only
- E. Group1, Group2, Group3, Group4 and Group5

**Correct Answer: D**

You cannot create access reviews for device groups.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

*Community vote distribution*

E (50%)      D (31%)      B (19%)

 **zmlapq99** Highly Voted 1 year, 10 months ago

Tested: Technically you can create access review for Dynamic Device group (no errors/warnings during the creation), however it doesn't work and you will see a hitch "Warning - No access to review" for that access review in the list.

upvoted 36 times

 **sapien45** 1 year, 5 months ago

Most useful response here,  
upvoted 3 times

 **MajorUrs** Highly Voted 2 years, 6 months ago

Correct. Dynamic user groups are also supported for Access Reviews

upvoted 11 times

 **Nyamnyam** Most Recent 2 weeks ago

**Selected Answer: B**

The question is imbecile.

The only meaningful answer is B: the assigned groups.

Dynamic groups cannot be "auto-remediated" through access reviews.

upvoted 1 times

 **Sorrynotsorry** 2 weeks, 3 days ago

**Selected Answer: B**

Group 1 and 4

Dynamic groups will get assigned by will not work

upvoted 1 times

 **AK\_1234** 1 month, 3 weeks ago

D is correct

For the Group 3 - You cannot create access reviews for device groups.

upvoted 1 times

 **ACSC** 2 months ago

**Selected Answer: D**

Even you can create access review for device groups, it doesn't work at all.

upvoted 1 times

 **Logitech** 2 months, 1 week ago

i hate this sort of questions, nobody knows what is the correct answer, because you can create the review for all of this groups. But it does not make sense because only users can be reviewed in the actual review.

upvoted 1 times

 **Vince\_MCT** 3 months, 2 weeks ago

**Selected Answer: E**

We can create access review to all.

Note: we can also create access review to dynamic devices. though no access review can be seen , question is only asking for access review creation not for the actual review.

upvoted 2 times

 **EmnCours** 4 months, 1 week ago

**Selected Answer: E**

Selected Answer E

upvoted 2 times

 **OK2020** 5 months ago

**Selected Answer: B**

Reading through the below documentations I think suggested answers are wrong.

Right answer should be : B: Group 1 & 4 only (which are assigned roles)

Global administrators and Privileged Role administrators can create reviews on role-assignable groups. For more information, see Use Azure AD groups to manage role assignments.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

The membership type for role-assignable groups must be Assigned and can't be an Azure AD dynamic group. Automated population of dynamic groups could lead to an unwanted account being added to the group and thus assigned to the role.

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

upvoted 3 times

 **dule27** 5 months ago

**Selected Answer: D**

D. Group1, Group2, Group4, and Group5 only

upvoted 2 times

 **chikorita** 8 months, 2 weeks ago

i dont get the point of creating access review for DYNAMIC group since members or devices are added based on condition.....whats the point or use case here

upvoted 3 times

 **kmk\_01** 7 months, 4 weeks ago

For dynamic users groups, access reviews are useful to make sure that the logic in the membership rules are capturing the correct accounts.

upvoted 1 times

 **divyakanth** 9 months, 4 weeks ago

**Selected Answer: D**

it doesnt make any sense creating access review for dynamica devoices if the revioew cannot be performed or completded

upvoted 2 times

 **Nazir97** 11 months ago

If you can create an access review for Dynamic Device groups, but can't actually perform a review, then that's a uncomplete, useless access review configuration in my book, therfore i think D is the correct answer

upvoted 2 times

 **NAMP** 11 months, 2 weeks ago

**Selected Answer: D**

I think MSFT assumes that you know what you are doing so if you add access reviews to dynamic devices but won't do anything, why would you do it?

upvoted 2 times

 **AMDF** 11 months, 3 weeks ago

**Selected Answer: D**

I think despite the fact that you can create for all Groups, MSFT here mentioned D answer.

upvoted 1 times

 **Jhill777** 1 year ago

**Selected Answer: E**

While you CAN create an access review for all of those groups, the scope is for "Guest users only" and "All Users" of the group. Devices do not show up as "Users" so there's a warning that states "No access to review". Yet another stupid question only MSFT would ask.

upvoted 2 times

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name  | Type   | Member of |
|-------|--------|-----------|
| User1 | Member | Group1    |
| User2 | Member | Group1    |
| User3 | Guest  | Group1    |

User1 is the owner of Group1.

You create an access review that has the following settings:

- Users to review: Members of a group
- Scope: Everyone
- Group: Group1
- Reviewers: Members (self)

Which users can perform access reviews for User3?

A. User1, User2, and User3

B. User3 only

C. User1 only

D. User1 and User2 only

#### Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review>

Community vote distribution

B (83%)

C (17%)

 **MajorUrs** Highly Voted 2 years, 6 months ago

Correct (B - User3 only)

upvoted 10 times

 **its\_tima** 10 months, 3 weeks ago

User 3 it is because the Reviewers are obviously 'self', meaning that the users can review their own role based assignments

upvoted 3 times

 **MacDanorld** Most Recent 3 days, 1 hour ago

**Selected Answer: C**

If you set Select reviewers to Users review their own access or Managers of users, B2B direct connect users and Teams won't be able to review their own access in your tenant. The owner of the Team under review will get an email that asks the owner to review the B2B direct connect user and Teams.

<https://learn.microsoft.com/en-us/entra/id-governance/create-access-review>

upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

The correct answer is B. User3 only.

According to the Microsoft Entra article on creating an access review of groups and applications<sup>1</sup>, when you select Members (self) as the reviewers, each user reviews their own access to the group or application. Therefore, in this scenario, only User3 can perform the access review for their own access to Group1. User1 and User2 cannot perform the access review for User3, even though User1 is the owner of Group1.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: B**

B. User3 only

upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: B**

B. User3 only

upvoted 1 times

 **kmk\_01** 7 months, 4 weeks ago

Self Access reviews are like marking your own homework.

upvoted 1 times

 **ThotSlayer69** 10 months, 1 week ago

**Selected Answer: B**

- When Reviewers is set to Members (Self), then only each individual member can review their own access, and if they do not then it is reported as no response
- [https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review](https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review)
- [https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review](https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review)

upvoted 2 times

 **Jhill777** 1 year ago

**Selected Answer: B**

When members are required to perform a self-review, there will only be one user showing in the "Overview" to review so only User3 will be able to review himself.

upvoted 1 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 2 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

 **airairo** 2 years, 2 months ago

why User1 can't perform access reviews??

upvoted 2 times

 **airairo** 2 years, 2 months ago

Members (self) got it.

upvoted 4 times

 **melatocaroca** 2 years, 4 months ago

Azure AD Premium P2

- Guest users who are assigned as reviewers.
- Guest users who perform a self-review
- Guest users as group owners who perform an access review.
- Guest users as application owners who perform an access review.
- Member users who are assigned as reviewers
- Member users who perform a self-review
- Member users as group owners who perform an access review
- Member users as application owners who perform an access review

upvoted 2 times

 **Eltooth** 2 years, 6 months ago

Correct - B

upvoted 1 times

 **Stormania** 2 years, 1 month ago

Why? Can you explain please?

upvoted 1 times

 **JaspaJami** 1 year, 8 months ago

Settings were self-reviewed so everyone will review themselves. So User3 is reviewed by User3

upvoted 6 times

**HOTSPOT -**

You have an Azure Active Directory (Azure AD) tenant that contains Azure AD Privileged Identity Management (PIM) role settings for the User administrator role as shown in the following exhibit.

... ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD > User Administrator >

**Role setting details - User Administrator**

Privileged Identity Management | Azure AD roles

 Edit

**Activation**

| SETTING                                  | STATE     |
|------------------------------------------|-----------|
| Activation maximum duration (hours)      | 8 hour(s) |
| Require justification on activation      | Yes       |
| Require ticket information on activation | No        |
| On activation, require Azure MFA         | Yes       |
| Require approval to activate             | Yes       |
| Approvers                                | None      |

**Assignment**

| SETTING                                                        | STATE      |
|----------------------------------------------------------------|------------|
| Allow permanent eligible assignment                            | No         |
| Expire eligible assignments after                              | 15 day(s)  |
| Allow permanent active assignment                              | No         |
| Expire active assignments after                                | 1 month(s) |
| Require Azure Multi-Factor Authentication on active assignment | No         |
| Require justification on active assignment                     | No         |

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.

Hot Area:

**Answer Area**

A user who requires access to the User administration role must perform multi-factor authentication (MFA) every [answer choice].

8 hours  
15 days  
1 month

Before an eligible user can perform a task that requires the User administrator role, the activation must be approved by a [answer choice].

global administrator only  
global administrator or privileged role administrator  
permanently assigned user administrator  
privileged role administrator only

Correct Answer:

**Answer Area**

A user who requires access to the User administration role must perform multi-factor authentication (MFA) every [answer choice].

|         |
|---------|
| 8 hours |
| 15 days |
| 1 month |

Before an eligible user can perform a task that requires the User administrator role, the activation must be approved by a [answer choice].

|                                                       |
|-------------------------------------------------------|
| global administrator only                             |
| global administrator or privileged role administrator |
| permanently assigned user administrator               |
| privileged role administrator only                    |

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure> <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan>

□ **MajorUrs** Highly Voted 2 years, 6 months ago

So correct answers are:

8 hours

Global administrators and privileged role administrators

upvoted 101 times

□ **Krille** Highly Voted 2 years, 7 months ago

"If no specific approvers are selected, privileged role administrators/global administrators will become the default approvers."

upvoted 36 times

□ **sezza\_blunt** 2 years, 5 months ago

This is exactly what it says in the PIM settings when editing a role.

upvoted 5 times

□ **Beitran** 2 years, 6 months ago

<https://janbakker.tech/active-directory-identity-governance-privileged-identity-management/>

upvoted 2 times

□ **Foggy31** Most Recent 1 month, 2 weeks ago

build in my lab, 8 hours and when not assigning approvers: "If no specific approvers are selected, privileged role administrators/global administrators will become the default approvers"

upvoted 1 times

□ **EmnCours** 4 months, 1 week ago

8 hours

Global administrators and privileged role administrators

upvoted 2 times

□ **dule27** 5 months ago

8 hours

Global administrators and privileged role administrators

upvoted 1 times

□ **OK2020** 5 months ago

I stand corrected. The time limit under "activation" is the one in effect here which is 8 Hours.

upvoted 1 times

□ **OK2020** 5 months, 3 weeks ago

My answer would be "1 Month" as it's teh time when an active assignment expire and the role would require another activation. The 8 hours is the time period before an activation request expire, different from the role lifetime which is the assignment

upvoted 1 times

□ **OK2020** 5 months ago

I stand corrected. The time limit under "activation" is the one in effect here which is 8 Hours.

upvoted 1 times

□ **OK2020** 5 months ago

I'm changing my suggested answer again: Actually it should be 1 month:

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan>

Type of assignments

There are two types of assignment – eligible and active. If a user has been made eligible for a role, that means they can activate the role

when they need to perform privileged tasks.

You can also set a start and end time for each type of assignment. This addition gives you four possible types of assignments:

Permanent eligible

Permanent active

Time-bound eligible, with specified start and end dates for assignment

Time-bound active, with specified start and end dates for assignment

In case the role expires, you can extend or renew these assignments.

We recommend you keep zero permanently active assignments for roles other than the recommended two break-glass emergency access accounts, which should have the permanent Global Administrator role.

upvoted 1 times

□ **f2bf85a** 7 months, 3 weeks ago

Note:

User may not be prompted for multi-factor authentication if they authenticated with strong credentials, or provided multi-factor authentication earlier in this session.

If there is no information about strong credentials in the question, it should be assumed that the user will be prompted for MFA every 8 hours regardless of their previous authentication status. The activation maximum duration for Azure AD PIM sets a time limit for the user's access to the privileged role, and once that time limit has been reached, the user will need to re-authenticate with multi-factor authentication to continue using the role.

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings#on-activation-require-multi-factor-authentication>

upvoted 1 times

□ **Taigr** 9 months, 2 weeks ago

on the exam 24.02.2022. I answered:

8 hours

Global administrators and Privileged role administrators

upvoted 4 times

□ **LeTrinh** 9 months, 2 weeks ago

Wrong. The correct answers are 15 days and global administrator or privileged role administrator. Because no delegation here.

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings>

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 one to 24 hours.

upvoted 1 times

□ **BTL\_Happy** 1 year ago

this question came out in my test today.

upvoted 2 times

□ **estyj** 1 year, 1 month ago

Correct. Have it setup and tested.

upvoted 1 times

□ **BB6919** 1 year, 2 months ago

Is there anything that the Global Admin can't do?

upvoted 1 times

□ **purek77** 11 months, 1 week ago

Work with Custom Security Attributes - you need a dedicated Azure AAD RBAC role.

upvoted 2 times

□ **lmeem** 1 year, 2 months ago

on the exam 09222022, i answered the same. Passed the exam, btw.

upvoted 2 times

□ **subhuman** 1 year, 5 months ago

Given answer for the second selection is wrong,

If no approvers are selected automatically by default the Global administrator or Privileged Role Administrators become the approvers.

upvoted 2 times

□ **Xyz\_40** 1 year, 5 months ago

I just did this in my Lab:

Global Admin & Privileged role Admin will become the approvers if no approver was selected.

upvoted 3 times

□ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 1 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

**HOTSPOT -**

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.

User1 has the devices shown in the following table.

| Name    | Platform   | Registered in contoso.com |
|---------|------------|---------------------------|
| Device1 | Windows 10 | Yes                       |
| Device2 | Windows 10 | No                        |
| Device3 | iOS        | Yes                       |

On November 5, 2020, you create and enforce terms of use in contoso.com that has the following settings:

- Name: Terms1
- Display name: Contoso terms of use
- Require users to expand the terms of use: On
- Require users to consent on every device: On
- Expire consents: On
- Expire starting on: December 10, 2020
- Frequency: Monthly

On November 15, 2020, User1 accepts Terms1 on Device3.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

| Statements                                                | Yes                   | No                    |
|-----------------------------------------------------------|-----------------------|-----------------------|
| On November 20, 2020, User1 can accept Terms1 on Device1. | <input type="radio"/> | <input type="radio"/> |
| On December 11, 2020, User1 can accept Terms1 on Device2. | <input type="radio"/> | <input type="radio"/> |
| On December 7, 2020, User1 can accept Terms1 on Device3.  | <input type="radio"/> | <input type="radio"/> |

**Answer Area**

| Statements                                                | Yes                              | No                               |
|-----------------------------------------------------------|----------------------------------|----------------------------------|
| On November 20, 2020, User1 can accept Terms1 on Device1. | <input checked="" type="radio"/> | <input type="radio"/>            |
| On December 11, 2020, User1 can accept Terms1 on Device2. | <input checked="" type="radio"/> | <input type="radio"/>            |
| On December 7, 2020, User1 can accept Terms1 on Device3.  | <input type="radio"/>            | <input checked="" type="radio"/> |

Box 1: Yes because User1 has not yet accepted the terms on Device1.

Box 2: Yes because User1 has not yet accepted the terms on Device2. User1 will be prompted to register the device before the terms can be accepted.

Box 3: No because User1 has already accepted the terms on Device3. The terms do not expire until December 10 and then monthly after that. th

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

 **Borbz** Highly Voted 2 years, 4 months ago

The current answer Y, Y, N is correct.

Box 1: Yes, because User1 has not yet accepted the terms on Device1.

Box 2: Yes, because User1 has not yet accepted the terms on Device2. User1 will be prompted to register the device before the terms can be accepted.

Box 3: No, because User1 has already accepted the terms on Device3. The terms do not expire until December 10 and then monthly after that upvoted 45 times

 **J4U** 2 years, 1 month ago

Yes, The given answer is correct. Don't go with with the vote. Review this article.

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

upvoted 4 times

□ **RandomNickname** 1 year, 5 months ago

Agree, reading the information provide in the Microsoft article given answer is correct.

Y,Y,N

upvoted 1 times

□ **BobHoudini** 2 years, 1 month ago

That's correct, I think many is staring at the "Expire on" but if we check what that means "The terms of use will be enforced immediately and users will be required to re-consent on this date"

Device2 hasn't registered the terms yet and will be asked to do it at 11th of December.

upvoted 3 times

□ **melatocaroca** Highly Voted 2 years, 4 months ago

Y, N,N

Start November 5, 2020

End December 10, 2020

- Box 1: Yes,
- o November 5, 2020 User1 has not yet accepted the terms on Device1 Registered in contoso.com
- Box 2: No, Answer date is December 11, 2020 expire starting on: December 10, 2020 answer date is December 11, 2020
- Box 3: No December 7, 2020 No On November 15, 2020, User1 accepts Terms1 on Device3.

upvoted 18 times

□ **Jun\_AZ500** 8 months ago

I believe the 2) is Yes, the expire starting on is meaning the Term of Use expire, and after the date user requires to accept again as "Frequency" is monthly

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

upvoted 4 times

□ **vaaws** Most Recent 1 month ago

Device 2 is not registered so YNN

upvoted 1 times

□ **EmnCours** 4 months, 1 week ago

YES

YES

NO

upvoted 2 times

□ **dule27** 5 months, 2 weeks ago

YES

YES

NO

upvoted 1 times

□ **ThotSlayer69** 10 months, 1 week ago

For Device2, when they try to access, they'll be forced to register the device on Azure AD, and their Device ID is used to enforce the Terms of use policy (meaning they will have to accept)

When it says "Expire starting on:" it means that the initial acceptance expires on that date for users, and they must reaccept the terms of use. It doesn't mean Terms1 overall expires

So:

- Yes

- Yes

- No (Accepted November 15, and December 7 < 10th where it expires for the first time, so they won't be prompted and have the ability to reaccept then)

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use#per-device-terms-of-use>

upvoted 3 times

□ **Jhill777** 1 year ago

Answer is YNN. Box 2 will get a message that states: "You can't get there from here." User will have to go to Access Work or School and register the device first.

upvoted 4 times

□ **BTL\_Happy** 1 year ago

this question came out in my test today.

upvoted 2 times

□ **WMG** 1 year, 4 months ago

Should be Y/N/N, device 2 needs to be registered first. Yes, you get asked to do it when accepting the terms, but AAD registration of devices can be blocked in various ways. So the exact answer is "No", because you cannot accept the terms without registering.

Most answers can be answered "yes, if you do X or Y or Z" so gets confusing, and the lack of info in the questions if course deliberate by MS..

upvoted 3 times

 **Xyz\_40** 1 year, 5 months ago

i performed this question on y lab. The given answers are right

upvoted 1 times

 **examamos** 1 year, 7 months ago

Regarding box 2, what expires is the "consent", not the terms-of-use requirement. So the given answer is correct: YYN

upvoted 2 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

 **SnottyPudding** 1 year, 8 months ago

Answers are Y, N, N. The second one is No because it is not registered: "Per-device terms of use...require users to consent on every device setting enables you to require end users to accept your terms of use policy on every device they're accessing from. \*\*\*\*The end user will be required to register their device in Azure AD.\*\*\*\* When the device is registered, the device ID is used to enforce the terms of use policy on each device."

The device will need to be registered before the terms of use can be accepted, and in its current unregistered state, User1 will not be able to accept Terms1.

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

upvoted 7 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 2 times

 **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022

upvoted 1 times

 **007Ali** 1 year, 10 months ago

The "can accept" makes these questions slightly vague in my mind, but I'm assuming it means "must accept", so I'd go with the following:

1 Yes - Assuming this is the first time that this device has been used since November 5th. Policy set on the 5th, so will required Terms to be accepted at next use after that date and then Monthly starting 10th December.

2 No - Device 2 is not registered and "Consent on every device will require users to register each device with Azure AD prior to getting access.". That the device could be enrolled I think is missing the point of the question.

3 No - The terms were accepted on Device 3 on 15th November, so would only be needed next on the 10th December.

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

upvoted 6 times

 **Hacker00** 1 year, 11 months ago

I think Y, N and N correct answer.

upvoted 3 times

Your company recently implemented Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

While you review the roles in PIM, you discover that all 15 users in the IT department at the company have permanent security administrator rights.

You need to ensure that the IT department users only have access to the Security administrator role when required.

What should you configure for the Security administrator role assignment?

- A. Expire eligible assignments after from the Role settings details
- B. Expire active assignments after from the Role settings details
- C. Assignment type to Active
- D. Assignment type to Eligible

**Correct Answer: D**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

*Community vote distribution*

D (80%)      B (20%)

 **Beitran** Highly Voted 2 years, 6 months ago

Correct

upvoted 14 times

 **007Ali** Highly Voted 1 year, 10 months ago

I think the best way to read this question is "What should you configure FIRST for the Security administrator role assignment?"

You would setup "D. Assignment type to Eligible" so the admins can request the role in future, for a limited time based on the Role Setting of "Activation maximum duration (hours): 8 (by default)"

Only then would you set "B. Expire active assignments after from the Role settings details"

So D is the correct answer.

upvoted 12 times

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

**Selected Answer: D**

D. Assignment type to Eligible:

When you set the assignment type to "Eligible," it means that users will not have permanent access to the role but will be eligible for it. They will need to activate the role when required, and it won't be active by default. This approach allows you to enforce just-in-time access, meaning that users will only have access to the Security administrator role when they request and activate it through PIM. Once their role activation period ends, they will lose access to the role automatically.

upvoted 1 times

 **EmnCours** 4 months, 1 week ago

**Selected Answer: D**

Correct Answer: D

upvoted 1 times

 **OK2020** 5 months ago

**Selected Answer: B**

I would say B for teh below reason

Eligible means teh user needs to take action to activate the role but it may then be permanent and won't expire. This doesn't comply with the ask "when required". Hence time bound should be applied on "Active" roles to disable access after completing the task and right until it's required again for the user to request another activation

upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: D**

D. Assignment type to Eligible

upvoted 1 times

 **IS\_PT\_ISO** 5 months, 1 week ago

**Selected Answer: D**

D is the correct answer  
upvoted 1 times

 **existingname** 1 year, 3 months ago

D is correct. in the exam today  
upvoted 3 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022  
upvoted 1 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.  
upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

On the exam ~~今天~~ - March 4, 2022  
upvoted 2 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022  
upvoted 1 times

 **Hacker00** 1 year, 11 months ago

Correct  
upvoted 2 times

 **BaderJ** 2 years, 2 months ago

Passed the exam today 23/09/2021  
This question came in the exam.  
upvoted 3 times

 **melatocaroca** 2 years, 4 months ago

eligible A role assignment that requires a user to perform one or more actions to use the role.

If a user has been made eligible for a role, that means they can activate the role when they need to perform privileged tasks.

There is no difference in the access given to someone with a permanent versus an eligible role assignment.

The only difference is that some people do not need that access all the time.

Eligible role user permissions

- Request activation of a role that requires approval
  - View the status of your request to activate
  - Complete your task in Azure AD if activation was approved
- upvoted 3 times

 **Eltooth** 2 years, 6 months ago

Eligible yes however you also need to remove perm assignment of security admin role from users.  
upvoted 4 times

You have a Microsoft 365 tenant.

The Sign-ins activity report shows that an external contractor signed in to the Exchange admin center.

You need to review access to the Exchange admin center at the end of each month and block sign-ins if required.

What should you create?

- A. an access package that targets users outside your directory
- B. an access package that targets users in your directory
- C. a group-based access review that targets guest users
- D. an application-based access review that targets guest users

**Correct Answer: C**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

Community vote distribution

C (100%)

✉ **melatocaroca** Highly Voted 2 years, 4 months ago

Answer: C

You can target a group with a conditional policy to detect and remediate the login at the end of each month

Not valid, A, B, D

D admin is not using an app is using a privileged role to use Exchange admin center

A and B No

An access package.

A bundle of resources that a team or project needs and is governed with policies. Access packages are defined in containers called catalogs. To reduce the risk of stale access, you should enable periodic reviews of users who have active assignments to an access package in Azure AD entitlement management

upvoted 16 times

✉ **hhaywood** Highly Voted 2 years, 6 months ago

Should be D - Application Based review with Guest users - <https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review#create-one-or-more-access-reviews>

upvoted 6 times

✉ **hhaywood** 2 years, 5 months ago

Ok after some testing I was wrong! Although app base review sounds right its for registered apps not MS EOL - I assume you would have to create a group specifically for EOL management and assign the review to that - poorly worded question

upvoted 5 times

✉ **sezza\_blunt** 2 years, 5 months ago

Yes, you're right. You'd need to create a group first and apply the access review to the group. You can't do an app-based review on Exchange Online.

upvoted 5 times

✉ **sapien45** 1 year, 5 months ago

Thank you so much, I was having headaches trying to figure out why not D

upvoted 2 times

✉ **haazybanj** Most Recent 4 weeks, 1 day ago

**Selected Answer: C**

To review access to the Exchange admin center at the end of each month and block sign-ins if required, you should create a group-based access review that targets guest users.

By creating a group-based access review, you can specifically target the guest users in your Microsoft 365 tenant, which includes external contractors. This allows you to regularly review their access to the Exchange admin center and make necessary adjustments or block their sign-ins if required.

upvoted 1 times

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

The correct answer is D. an application-based access review that targets guest users.

According to the Microsoft Entra article on creating an access review of groups and applications<sup>1</sup>, you can create an access review for any group

or application that is connected to Microsoft Entra ID. This includes security groups, Microsoft 365 groups, distribution lists, and Azure AD enterprise applications. You can also create an access review for multiple resources in access packages by using Microsoft Entra entitlement management

upvoted 2 times

□ **EmnCours** 3 months, 3 weeks ago

**Selected Answer: C**

Answer: C

upvoted 1 times

□ **dule27** 5 months, 1 week ago

**Selected Answer: C**

C. a group-based access review that targets guest users

upvoted 1 times

□ **LeTrinh** 9 months, 3 weeks ago

D can be right to:

See the link: <https://www.rebeladmin.com/2019/03/step-step-guide-azure-ad-access-reviews-applications/>

upvoted 1 times

□ **LeTrinh** 9 months, 2 weeks ago

My bad, answer is C

-> ONLY choosing group-based access review can target guest users.

upvoted 1 times

□ **AWS56** 9 months, 3 weeks ago

**Selected Answer: C**

C is the right answer

upvoted 1 times

□ **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

□ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 1 times

□ **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022

upvoted 2 times

□ **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 1 times

□ **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

□ **007Ali** 1 year, 10 months ago

After looking in a lab at each of the options, I believe this is getting at the following settings:

Identity Governance -> New Access Review -> Review Type -> "Select Review Scope" and "Scope".

Therefore C is the correct answer.

upvoted 5 times

□ **Cloudcrawler** 2 years, 2 months ago

It seems both C and D is correct. Guest user access review can be both group and application based :

<https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-guest-access-with-access-reviews#create-and-perform-an-access-review-for-guests>

upvoted 3 times

□ **Domza** 2 years, 5 months ago

Looks like its asking about external users/guest in this case. Not so much about app review.

Also, when MS asked about "App" review, they mean app you create/develop.

upvoted 2 times

□ **ndhanaraj** 2 years, 6 months ago

How about the following MS Content?:

Ask group owners to confirm they still need guests in their groups: Employee access might be automated with some on premises Identity and Access Management (IAM), but not invited guests. If a group gives guests access to business sensitive content, then it's the group owner's responsibility to confirm the guests still have a legitimate business need for access.

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 tenant.

You have 100 IT administrators who are organized into 10 departments.

You create the access review shown in the exhibit. (Click the Exhibit tab.)

### Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

|                                                   |                                                                                                       |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Review name *                                     | <input type="text" value="Admin review"/>                                                             |
| Description                                       | <input type="text" value=""/>                                                                         |
| Start date *                                      | <input type="text" value="12/18/2020"/>                                                               |
| Frequency                                         | <input type="text" value="Monthly"/>                                                                  |
| Duration (in days) *                              | <input type="text" value="14"/>                                                                       |
| End                                               | <input checked="" type="radio"/> Never <input type="radio"/> End by <input type="radio"/> Occurrences |
| Number of times                                   | <input type="text" value="0"/>                                                                        |
| End date                                          | <input type="text" value="01/17/2021"/>                                                               |
| Users                                             |                                                                                                       |
| Scope                                             | <input checked="" type="radio"/> Everyone <input type="radio"/> Specific users                        |
| Review role membership (permanent and eligible) * | <input type="text" value="Application Administrator and 72 others"/>                                  |
| Reviewers                                         | <input type="text" value="(Preview) Manager"/>                                                        |
| (Preview) Fallback reviewers                      | <input type="text" value="Megan Bowen"/>                                                              |
| <input type="checkbox"/> Upon completion settings |                                                                                                       |

**Start**

You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You create a separate access review for each role.

Does this meet the goal?

A. Yes

B. No

### Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

Community vote distribution

B (100%)

 **Eltooth**  2 years, 6 months ago

No - each access review would still send review approval to Megan as no manager has been set for the user accounts under review.

upvoted 11 times

 **dule27** Most Recent ⓘ 5 months, 1 week ago

**Selected Answer: B**

B. No is correct answer

upvoted 1 times

 **estyj** 1 year, 1 month ago

No, no admin reviewer set and Megan is the fallback reviewer. She will still receive reviews.

upvoted 2 times

 **sapien45** 1 year, 5 months ago

No

If you choose either Managers or users or Group owner(s), you can also specify a fallback reviewer. Fallback reviewers are asked to do a review when the user has no manager specified in the directory or if the group doesn't have an owner.

upvoted 1 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 3 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

 **melatocaroca** 2 years, 4 months ago

Answer NO

Why reason

Because admin review is not modified, Megan Brow as Fallback Reviewer will still receiving reviews, no manager has been assigned to admin review.

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 tenant.

You have 100 IT administrators who are organized into 10 departments.

You create the access review shown in the exhibit. (Click the Exhibit tab.)

### Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

**Review name \*** Admin review

**Description** ①

店铺：专业认证88

**Start date \*** 12/18/2020

**Frequency** Monthly

**Duration (in days) ①**

14

**End ①**

Never End by Occurrences

**Number of times** 0

**End date** 01/17/2021

**Users**

**Scope** Everyone

Review role membership (permanent and eligible) \*

Application Administrator and 72 others

**Reviewers**

**Reviewers**

(Preview) Manager

(Preview) Fallback reviewers ①

Megan Bowen

Upon completion settings

**Start**

You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You modify the properties of the IT administrator user accounts.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: A**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

Community vote distribution

A (67%)

B (33%)

 **MajorUrs** Highly Voted 2 years, 6 months ago

The answer assumes you set manager for every account.

Seems correct, but feels stupid and misleading

upvoted 27 times

✉  **letsgobraves** 2 years, 6 months ago

your typical MS exam question. Sometimes they expect you to assume, other times they want you to answer with the given information....SMDH

upvoted 3 times

✉  **JerryGolais**  2 years, 6 months ago

A - Yes. Megan Bowen is receiving the access reviews because no Managers are set for those users under Job Info, she is the fallback reviewer. If you set the Manager value to a user, this user will receive the review instead of Megan Bowen.

upvoted 13 times

✉  **EmnCours**  4 months, 1 week ago

**Selected Answer: A**

Correct Answer: A

upvoted 2 times

✉  **dule27** 5 months ago

**Selected Answer: A**

A. YES is the correct answer

upvoted 2 times

✉  **OK2020** 5 months ago

**Selected Answer: B**

NO

IT Administraor is not the users "Manager" in AAAD.

<https://learn.microsoft.com/en-us/powershell/module/azuread/set-azureadusermanager?view=azureadps-2.0>

upvoted 1 times

✉  **santalazza** 11 months, 2 weeks ago

**Selected Answer: A**

MajorUrs is right.

upvoted 2 times

✉  **estyj** 12 months ago

No, you have to set the Access Reviewer, otherwise it will still default to the Fallback reviewer. Modifying properties of the IT admin account is not going to set the manager of each department.

upvoted 1 times

✉  **DeepMoon** 1 year, 2 months ago

Correct Answer: NO

Review is set for Everyone.

'Everyone' is universal catch-all group for all AAD users.

Modify the properties of the IT administrator user accounts is not like to assign a manager for all groups inside Everyone.

Because admin review is not modified: no manager has been assigned to each group inside Everyone.

Megan Brow as Fallback Reviewer will still be receiving reviews.

upvoted 1 times

✉  **jvallespin** 1 year, 4 months ago

**Selected Answer: B**

Manager is not an specific property of an AAD User. You won't see manager when retrieve \*(All) properties for a particular user so i wouls say B.

upvoted 2 times

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

who's willing to bet jvallespin is a short indian :')

upvoted 1 times

✉  **WMG** 1 year, 4 months ago

This answer should serve as a caution for users with low experience reading here. Instead of believing someone like the above who are completely wrong, google "set manager for azure ad user". (Hint: Set-AzureADUserManager).

upvoted 7 times

✉  **kmk\_01** 7 months, 4 weeks ago

Harsh but true.

upvoted 1 times

✉  **Faheem2020** 1 year, 2 months ago

You could indeed go the AAD portal, edit a users properties and assign a Manager from "Job Information" tab

upvoted 1 times

✉  **sapien45** 1 year, 5 months ago

Megan Bowen just had a depression because of the unidentified managers

upvoted 7 times

 **zts** 1 year, 5 months ago

probably on the road to counseling  
upvoted 1 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.  
upvoted 1 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022  
upvoted 1 times

 **melatocaroca** 2 years, 4 months ago

Answer: NO

Modify the properties of the IT administrator user accounts is not like to modify admin review to assign a manager, so, Because admin review is not modified, Megan Brow as Fallback Reviewer will still receiving reviews, no manager has been assigned to admin review.

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 tenant.

You have 100 IT administrators who are organized into 10 departments.

You create the access review shown in the exhibit. (Click the Exhibit tab.)

### Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name \* Admin review ✓

Description ⓘ 店铺：专业认证88

Start date \* 12/18/2020

Frequency Monthly

Duration (in days) ⓘ 14

End ⓘ Never End by Occurrences

Number of times 0

End date 01/17/2021

Users

Scope Everyone

Review role membership (permanent and eligible) \*

Application Administrator and 72 others

Reviewers

Reviewers (Preview) Manager

(Preview) Fallback reviewers ⓘ Megan Bowen

Upon completion settings

**Start**

You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You set Reviewers to Member (self).

Does this meet the goal? 店铺：专业认证88

A. Yes

B. No

#### Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

Community vote distribution

B (100%)

Correct: "Fallback reviewers are asked to do a review when the user has no manager specified in the directory or the group does not have an owner."

upvoted 8 times

 **EmnCours** Most Recent ⓘ 3 months, 3 weeks ago

**Selected Answer: B**

B. No is the correct answer

upvoted 1 times

 **dule27** 5 months, 1 week ago

**Selected Answer: B**

B. No is the correct answer

upvoted 1 times

 **DeepMoon** 1 year, 2 months ago

Given Answer is Correct.

Requirement "You need to ensure that the manager of each department receives the access reviews of their respective department."  
Setting to Self-Review won't accomplish that.

upvoted 4 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 1 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

 **Eltooth** 2 years, 6 months ago

Correct - No.

upvoted 3 times

 **zed01** 2 years, 6 months ago

Self review will generate an access review for all admins. So the answer is correct.

upvoted 4 times

 **melatocaroca** 2 years, 5 months ago

Select reviewers section, select either one or more people to perform the access reviews.

Group owner(s) (Only available when performing a review on a Team or group)

Selected user(s) or groups(s)

Users review own access

Managers of users. If you choose either Managers of users or Group owners you also have the option to specify a fallback reviewer. Fallback reviewers are asked to do a review when the user has no manager specified in the directory or the group does not have an owner.

upvoted 2 times

 **melatocaroca** 2 years, 4 months ago

Answer NO

Members (self) - Use this option to have the users review their own role assignments. Groups assigned to the role will not be a part of the review when this option is selected. This option is only available if the review is scoped to Users and Groups.

Also Megan Brow still there as Fallback Reviewer so will still receiving reviews

upvoted 2 times

 **wombat09** 2 years, 5 months ago

"You need to ensure that the manager of each department receives the access reviews of their respective department." in 10 departments each with its manager you would not assign all the users to the correct manager (at most 10 if all managers were also admins)

No is the correct

upvoted 2 times

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.

You plan to create an emergency-access administrative account named Emergency1. Emergency1 will be assigned the Global administrator role in Azure AD.

Emergency1 will be used in the event of Azure AD functionality failures and on-premises infrastructure failures.

You need to reduce the likelihood that Emergency1 will be prevented from signing in during an emergency.

What should you do?

- A. Configure Azure Monitor to generate an alert if Emergency1 is modified or signs in.
- B. Require Azure AD Privileged Identity Management (PIM) activation of the Global administrator role for Emergency1.
- C. Configure a conditional access policy to restrict sign-in locations for Emergency1 to only the corporate network.
- D. Configure a conditional access policy to require multi-factor authentication (MFA) for Emergency1.

#### Correct Answer: A

##### Community vote distribution

|         |     |
|---------|-----|
| A (88%) | 13% |
|---------|-----|

 **MajorUrs** Highly Voted 2 years, 6 months ago

The answer is stupid, because creating alert does not help with reducing the likelihood.  
But it is correct, because all other answers will create additional blockers to connect  
upvoted 51 times

 **Eltooth** 2 years, 6 months ago

Agreed - all other answers would prevent emergency (breakglass) account from working. Answer is A - always log changes to break glass account.  
upvoted 6 times

 **lime568** 1 year, 8 months ago

Actually the answer it is ok. If someone will change the password for this user and ony one person know the new password ?  
upvoted 5 times

 **JerryGolais** 2 years, 6 months ago

A by elimination. You are right that is pretty dumb.  
upvoted 4 times

 **YetiSpaghetti** 1 year, 5 months ago

Preach. I laughed at how dumb this answer was.  
upvoted 3 times

 **MarioMK** Highly Voted 2 years, 5 months ago

Woow. I guess there is a competition at Microsoft as to who can formulate a question in the most stupid way possible. I have read 5 times in order to understand what are they trying to say. I think this is done on purpose to make things look harder than they really are  
upvoted 14 times

 **haazybanj** Most Recent 4 weeks, 1 day ago

**Selected Answer: A**

The correct answer is A. Configure Azure Monitor to generate an alert if Emergency1 is modified or signs in.

All of the other options would add additional barriers to signing in with the emergency-access administrative account, which could prevent it from being used in an emergency.

upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

The correct answer is C. Configure a conditional access policy to restrict sign-in locations for Emergency1 to only the corporate network.  
upvoted 1 times

 **Jzx** 2 months, 3 weeks ago

**Selected Answer: D**

D. Configure a conditional access policy to require multi-factor authentication (MFA) for Emergency1:

Enforcing MFA for Emergency1 adds an extra layer of security and ensures that even if a password is compromised or other issues arise, Emergency1 will still need to provide a second form of authentication to access Azure AD resources. This is a crucial security measure, especially

for accounts with high privileges like Global administrators. MFA enhances security and helps protect against unauthorized access, even in emergency situations.

upvoted 1 times

**DasChi\_cken** 3 months, 1 week ago

**Selected Answer: A**

You need to protect this Account AS IT IS the highest privileged Admin, but you can't use protection methods mentioned in answer B, C and D because that could block Access.

The only way to "protect" is to Monitor.

Answer A is a good answer only the word "likelihood" is a bit misleading

upvoted 2 times

**EmnCours** 4 months, 1 week ago

**Selected Answer: A**

A. Configure Azure Monitor to generate an alert if Emergency1 is modified or signs in.

upvoted 2 times

**dule27** 5 months, 1 week ago

**Selected Answer: A**

A. Configure Azure Monitor to generate an alert if Emergency1 is modified or signs in.

upvoted 2 times

**estyj** 1 year, 1 month ago

A. Yes need to monitor that break glass account so that you are aware of any changes to account in case of a real emergency.

upvoted 1 times

**DeepMoon** 1 year, 2 months ago

Perfect question. Perfect Answer.

This is an account used in 'break the glass' scenarios. It only has a very long password, that is kept under lock and key. User ID and password are not connected to any user or device for authentication. No MFA can block its access. Even with cell or network/email/phone down situations you can login with this account. You can login from anywhere. So it needs to be monitored to prevent tampering and account usage.

upvoted 3 times

**Faheem2020** 1 year, 3 months ago

Makes perfect sense to put your emergency account on monitor.

<https://docs.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access>

upvoted 3 times

**subhuman** 1 year, 5 months ago

Answer provided is correct always log activities from the Emergency "Break Glass" Account to monitor for any changes. All other choices will definitely prevent the account from being accessible

upvoted 1 times

**Xyz\_40** 1 year, 5 months ago

The question needs to be modified as it not correctly fits to the answer. Though only answer "A" fits it.

upvoted 1 times

**TP447** 1 year, 7 months ago

Was expecting the answer to be excluding the account from CA so that it can sign in always when needed but there was no option. Option A is most logical...ish

upvoted 1 times

**Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 3 times

**RVR** 1 year, 11 months ago

Think they went for D and messed up! "require" instead of exclude and boom!

upvoted 1 times

**Anker** 2 years, 4 months ago

Pretty poor question haha. I was thinking there would be an answer like adding them as an exemption in a conditional access policy so they wouldn't be subject to MFA or something but I guess just Alerting works...

upvoted 2 times

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You implement entitlement management to provide resource access to users at a company named Fabrikam, Inc. Fabrikam uses a domain named fabrikam.com.

Fabrikam users must be removed automatically from the tenant when access is no longer required.

You need to configure the following settings:

- Block external user from signing in to this directory: No
- Remove external user: Yes
- Number of days before removing external user from this directory: 90

What should you configure on the Identity Governance blade?

- A. Access packages
- B. Entitlement management settings
- C. Terms of use
- D. Access reviews settings

**Correct Answer: B**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users>

*Community vote distribution*

B (100%)

 **haazybanj** 4 weeks, 1 day ago

**Selected Answer: B**

The correct answer is B. Entitlement management settings.

The entitlement management settings page is where you configure the settings for managing access to resources in your Azure AD tenant. This includes settings for external users, such as whether to allow them to sign in and how long to keep their accounts active after their access is no longer required.

upvoted 1 times

 **DasChi\_cken** 3 months, 1 week ago

**Selected Answer: B**

Question already Providers the answer

You implement ---entitlement management--- to provide resource access to users at a company named Fabrikam, Inc.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: B**

B. Entitlement management settings

upvoted 1 times

 **kalisprod** 3 months, 3 weeks ago

**Selected Answer: B**

Tested in lab - Answer is correct

upvoted 1 times

 **dule27** 5 months, 1 week ago

**Selected Answer: B**

B. Entitlement management settings

upvoted 1 times

 **AArif098** 9 months, 3 weeks ago

**Selected Answer: B**

Tested in la and this is correct

Azure AD > Identity Governance > >Entitle Management > Settings. This is where you will see requirements.

upvoted 2 times

 **ANDRESCB1988** 1 year ago

**Selected Answer: B**

Correct

upvoted 1 times

 **Xyz\_40** 1 year, 5 months ago

No stress. the answer is correct

upvoted 2 times

 **wooyourdaddy** 1 year, 6 months ago

**Selected Answer: B**

B 100%. The provided link has the answer to the requirements at this part of the page:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users#manage-the-lifecycle-of-external-users>

upvoted 4 times

 **Davidf** 1 year, 6 months ago

**Selected Answer: B**

Correct

upvoted 1 times

You have an Azure Active Directory (Azure AD) P1 tenant.

You need to review the Azure AD sign-in logs to investigate sign-ins that occurred in the past.

For how long does Azure AD store events in the sign-in logs?

- A. 14 days
- B. 30 days
- C. 90 days
- D. 365 days

**Correct Answer: B**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention#how-long-does-azure-ad-store-the-data>

*Community vote distribution*

B (100%)

✉ **Eltooth** Highly Voted 2 years, 6 months ago

Correct - 30 days however this requires AADP1 or P2 licence as AD free only keeps 7 days of sign in logs. Wording should be clearer on question.  
upvoted 7 times

✉ **its\_tima** 10 months ago

Words were clear as the question mentions P1 tenant, meaning premium 1.  
upvoted 4 times

✉ **haazybanj** Most Recent 4 weeks, 1 day ago

**Selected Answer: B**

The correct answer is B. 30 days.

Azure AD P1 tenants store sign-in logs for 30 days. After 30 days, the logs are deleted.

If you need to store sign-in logs for longer than 30 days, you can export them to an Azure Storage account or use Azure Monitor to archive them.  
upvoted 1 times

✉ **dbmc** 2 months ago

On exam today - October 5th 2023  
upvoted 1 times

✉ **EmnCours** 3 months, 3 weeks ago

**Selected Answer: B**

B. 30 days  
upvoted 1 times

✉ **dule27** 5 months, 1 week ago

**Selected Answer: B**

B. 30 days  
upvoted 1 times

✉ **estyj** 1 year, 1 month ago

correct sign in logs only go back 1 month = 30 days, audit logs as well.  
upvoted 1 times

✉ **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022  
upvoted 1 times

✉ **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022  
upvoted 2 times

✉ **stromnessian** 1 year, 9 months ago

**Selected Answer: B**

Yes, it's 30 days.  
upvoted 3 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 3 times

 **Hacker00** 1 year, 11 months ago

Correct

upvoted 3 times

 **melatocaroca** 2 years, 5 months ago

To be selected in the exam, to add, free, No, because no 7 days, but to choose 30 or 90 they need to add P1 or P2, but assume P2 is more expensive so thought only just P1, so 30 is correct

upvoted 3 times

 **Jhill777** 1 year ago

Makes perfect sense.

upvoted 1 times

 **Domza** 2 years, 5 months ago

Plus there are Security report and Activity Report.

Security - 90 days with P2

Activity - 30 days with P2

upvoted 3 times

You have an Azure subscription that contains the resources shown in the following table.

| Name        | Type                                                        |
|-------------|-------------------------------------------------------------|
| Group1      | Group that has the Assigned membership type                 |
| App1        | Enterprise application in Azure Active Directory (Azure AD) |
| Contributor | Azure subscription role                                     |
| Role1       | Azure Active Directory (Azure AD) role                      |

For which resources can you create an access review?

- A. Group1, Role1, and Contributor only
- B. Group1 only
- C. Group1, App1, Contributor, and Role1
- D. Role1 and Contributor only

**Correct Answer: C**

Access reviews require an Azure AD Premium P2 license.

Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.

Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium P2.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review?toc=/azure/active-directory/governance/toc.json>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

*Community vote distribution*

C (100%)

 **researched\_answer\_boi** Highly Voted 2 years, 2 months ago

Yeah, it is possible to create access reviews for both Azure AND Azure AD roles.

Tested in Azure portal.

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review>  
upvoted 12 times

 **researched\_answer\_boi** 2 years, 2 months ago

...and also for enterprise apps:

[https://portal.azure.com/#blade/Microsoft\\_AAD\\_IAM/StartboardApplicationsMenuBlade/AccessReviews](https://portal.azure.com/#blade/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/AccessReviews)

upvoted 6 times

 **melatocaroca** Highly Voted 2 years, 4 months ago

Access reviews require an Azure AD Premium P2 license.

Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.

Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium P2., not by default

So correct answer based on that C

You need a P2 to create access review for Privileged role, normal in any enterprise to have P2

upvoted 8 times

 **AK\_1234** Most Recent 1 month, 3 weeks ago

C . Access reviews require an Azure AD Premium P2 license.

Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.

- Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium P2.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: C**

C. Group1, App1, Contributor, and Role1

upvoted 1 times

 **dule27** 5 months, 1 week ago

**Selected Answer: C**

C. Group1, App1, Contributor, and Role1

upvoted 1 times

 **JN\_311** 5 months, 3 weeks ago

This is question I have doubts on the answer, not sure if the answer is 100% correct: It says 'For which resources can you create an access review? I would pick B Group1, reason for this, if you create an Access Review, these are the options.

- Applications
- Teams and groups

You can select Security Groups.

upvoted 1 times

 **BTL\_Happy** 1 year ago

this question came out in my test today.

upvoted 4 times

 **ANDRESCB1988** 1 year ago

**Selected Answer: C**

correct

upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 2 times

 **stromnessian** 1 year, 9 months ago

**Selected Answer: C**

All of them, so C.

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022

upvoted 2 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 2 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 2 times

 **BaderJ** 2 years, 2 months ago

Passed the exam today 23/09/2021

This question came in the exam.

upvoted 3 times

 **airairo** 2 years, 2 months ago

the answer is incorrect.

you can assign access review to :

- Applications
- Teams and groups : All Microsoft 365 groups with guest users = (Guest users only )

or : Select Teams + groups

upvoted 3 times

 **Eltooth** 2 years, 5 months ago

Answer is correct - C.

upvoted 2 times

You have an Azure Active Directory (Azure AD) tenant that uses conditional access policies.

You plan to use third-party security information and event management (SIEM) to analyze conditional access usage.

You need to download the Azure AD log by using the administrative portal. The log file must contain changes to conditional access policies.

What should you export from Azure AD?

- A. audit logs in CSV format
- B. sign-ins in CSV format
- C. audit logs in JSON format
- D. sign-ins in JSON format

**Correct Answer: C**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs>

*Community vote distribution*

C (100%)

 **melatocaroca** Highly Voted 2 years, 5 months ago

You can also choose to download the filtered data, up to 250,000 records, by selecting the Download button. You can download the logs in either CSV or JSON format

So this question, can be one of those that you will got Corect if you choose any of both csv or JSON,

You can use the JSON transform feature in the Power Query Editor in Excel to split each property in the JSON object in the AuditData column into multiple columns so that each property has its own column.

So my vote goes to C, JSON

<https://docs.microsoft.com/en-us/microsoft-365/compliance/export-view-audit-log-records?view=o365-worldwide>

upvoted 11 times

 **hhaywood** Highly Voted 2 years, 5 months ago

C - Answer is correct - Audit Logs show the fact policies were changed (tested in tenant), Sign-ins only show access was granted/denied  
upvoted 6 times

 **sezza\_blunt** 2 years, 5 months ago

Agree - I confirmed in my tenant too. BUT - why json over csv? Both appear to provide the same information.

upvoted 3 times

 **xm3000** 2 years, 5 months ago

json tend to be the implicit std for sharing files between different sys

upvoted 2 times

 **TooManyExams** 2 years, 2 months ago

when I click on download it states I can download up to 250000 records. but csv only takes 50000 records. good reason for json  
<https://docs.microsoft.com/en-us/microsoft-365/compliance/export-view-audit-log-records?view=o365-worldwide>

upvoted 2 times

 **melatocaroca** 2 years, 4 months ago

You can use the JSON transform feature in the Power Query Editor in Excel to split each property in the JSON object in the AuditData column into multiple columns so that each property has its own column.

upvoted 2 times

 **haazybanj** Most Recent 4 weeks, 1 day ago

**Selected Answer: C**

The correct answer is C. audit logs in JSON format.

Audit logs contain a record of all administrative actions and changes made within Azure AD, such as user and group management, application assignments, and policy modifications.

upvoted 1 times

 **haazybanj** 4 weeks, 1 day ago

**Selected Answer: C**

The correct answer is C. audit logs in JSON format.

Audit logs contain a record of all administrative actions and changes made within Azure AD, such as user and group management, application assignments, and policy modifications.

upvoted 1 times

□ **Jzx** 2 months, 3 weeks ago

**Selected Answer: C**

C. Audit logs in JSON format:

Audit logs in JSON format contain detailed information about various activities in Azure AD, including changes to conditional access policies. These logs provide comprehensive data that can be ingested by third-party security information and event management (SIEM) systems for analysis. They are typically the preferred format for auditing and monitoring purposes because they contain structured data that is easier to parse and analyze.

upvoted 1 times

□ **ServerBrain** 3 months ago

**Selected Answer: C**

We don't know what 3rd part SIEM the logs will be imported to. JSON is more universal than csv..

upvoted 1 times

□ **EmnCours** 3 months, 3 weeks ago

**Selected Answer: C**

Correct Answer: C

upvoted 1 times

□ **dule27** 5 months, 1 week ago

**Selected Answer: C**

C. audit logs in JSON format

upvoted 1 times

□ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 2 times

□ **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 1 times

□ **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

□ **zizoutn** 2 years, 6 months ago

it's "D" and not "C" because in Sign-ins you can see the conditional access usage .

upvoted 3 times

□ **sezza\_blunt** 2 years, 5 months ago

But the question says: "The log file must contain changes to conditional access policies"

That information is only in the audit logs.

upvoted 6 times

□ **Eltooth** 2 years, 6 months ago

Looks 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.

You have a Microsoft 365 tenant.

You have 100 IT administrators who are organized into 10 departments.

You create the access review shown in the exhibit. (Click the Exhibit tab.)

### Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

**Review name \*** Admin review

**Description** (i)  

**Start date \*** 12/18/2020  

**Frequency** Monthly ▼

**Duration (in days)** (i) 14

**End** (i) Never End by Occurrences

**Number of times** 0

**End date** 01/17/2021  

**Users**

**Scope** Everyone

**Review role membership (permanent and eligible) \***  
Application Administrator and 72 others

**Reviewers**

**Reviewers** (Preview) Manager ▼

(Preview) Fallback reviewers (i)  
Megan Bowen

Upon completion settings

Start

You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You add each manager as a fallback reviewer.

Does this meet the goal?

- A. Yes
- B. No

#### Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

Community vote distribution

 **hhaywood** Highly Voted  2 years, 5 months ago

No - Correct - each manager would receive all reviews if all are fallbacks.  
upvoted 9 times

 **EmnCours** Most Recent  3 months, 3 weeks ago

**Selected Answer: B**

No is the correct answer  
upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: B**

No is the correct answer  
upvoted 1 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.  
upvoted 1 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022  
upvoted 1 times

 **melatocaroca** 2 years, 4 months ago

You need to also modify the admin review to remove to Megan Bowen as fallback reviewer, and assign one user as reviewer, without that, Megan will still receiving the review as fallback reviewer, of admin review, you need to add each manager as reviewer not as fallback reviewer  
upvoted 3 times

 **julioglez88** 2 years, 5 months ago

The correct answer should be B: NO  
The option of Fallback reviewer is when you set as reviewer to the manager or group owner and somehow that user is not having a manager in the directory. In those case, the fallback reviewer, which could be a department head would be the reviewer.  
"Fallback reviewers are asked to do a review when the user has no manager specified in the directory or the group does not have an owner."  
upvoted 3 times

You have an Azure Active Directory (Azure AD) tenant that contains the objects shown in the following table.

| Name      | Type             |
|-----------|------------------|
| User1     | User             |
| Guest1    | Guest            |
| Identity1 | Managed identity |

Which objects can you add as eligible in Azure AD Privileged Identity Management (PIM) for an Azure AD role?

- A. User1, Guest1, and Identity1
- B. User1 and Guest1 only
- C. User1 only
- D. User1 and Identity1 only

**Correct Answer: B**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan>

Community vote distribution

B (100%)

 **Opemi** Highly Voted 2 years, 2 months ago

Correct, you cannot add a non-interactive account as eligible use.

upvoted 10 times

 **stromnessian** Highly Voted 1 year, 9 months ago

B.

Note: You cannot assign service principals as eligible to Azure AD roles, Azure roles, and Privileged Access groups but you can grant a time limited active assignment to all three.

upvoted 7 times

 **EmnCours** Most Recent 3 months, 3 weeks ago

Selected Answer: B

Correct, you cannot add a non-interactive account as eligible use.

upvoted 1 times

 **dule27** 5 months, 1 week ago

Selected Answer: B

B. User1 and Guest1 only

upvoted 1 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 1 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

**HOTSPOT -**

You have an Azure Active Directory (Azure AD) tenant that contains the following group:

- Name: Group1
- Members: User1, User2
- Owner: User3

On January 15, 2021, you create an access review as shown in the exhibit. (Click the Exhibit tab.)

**Create an access review**

**Review name \*** Review1

**Description** 店铺: 专业认证88

**Start date \*** 01/15/2021

**Frequency** Monthly

**Duration (in days)** 14

**End** Never

**Number of times** 0

**End date \*** 02/15/2021

**Users**

**Users to review** Members of a group

**Scope** Everyone

**Group \*** Group1

**Reviewers**

**Reviewers** Members (self)

**Programs**

Link to program >  
Default Business Flow

Upon completion settings

Advanced settings

**Start** 店铺: 专业认证88

Users answer the Review1 question as shown in the following table.

| User  | Date             | Do you still need access to Group1? |
|-------|------------------|-------------------------------------|
| User1 | January 17, 2021 | Yes                                 |
| User2 | January 20, 2021 | No                                  |

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

| Statements                                                        | Yes                              | No                    |
|-------------------------------------------------------------------|----------------------------------|-----------------------|
| On February 5, 2021, User1 can answer the Review1 question again. | <input type="radio"/>            | <input type="radio"/> |
| On January 25, 2021, User2 can answer the Review1 question again. | <input type="radio"/>            | <input type="radio"/> |
| On January 22, 2021, User3 can answer the Review1 question.       | <input checked="" type="radio"/> | <input type="radio"/> |

Correct Answer:

### Answer Area

| Statements                                                        | Yes                              | No                               |
|-------------------------------------------------------------------|----------------------------------|----------------------------------|
| On February 5, 2021, User1 can answer the Review1 question again. | <input checked="" type="radio"/> | <input type="radio"/>            |
| On January 25, 2021, User2 can answer the Review1 question again. | <input checked="" type="radio"/> | <input type="radio"/>            |
| On January 22, 2021, User3 can answer the Review1 question.       | <input type="radio"/>            | <input checked="" type="radio"/> |

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/review-your-access>

Elpida Highly Voted 2 years, 2 months ago

I would say NO, YES, NO. According to the doc, "You can change your response at any time until the access review has ended" which refers to the duration of the review (15 days). Therefore, the user can change her response until January 29th, and will then be able to answer again on February 25th.

upvoted 57 times

mcas 1 year ago

I think that changing the response is what is meant in #1 by "answer the question again", so should be YES  
upvoted 1 times

RVR 1 year, 11 months ago

Why should the first one be No ?

upvoted 1 times

summut 1 year, 10 months ago

Because the review end date is 14 days after the start (on 15th Jan) so end of review cycle for the month is 29th Jan. After that date the Review cycle will not start again until 15th Feb.  
upvoted 11 times

Lozo2020 1 year, 6 months ago

I don't think there will be a review cycle given the fact that there is an end date. That would be the case for never ending  
upvoted 1 times

Jaspajami 1 year, 8 months ago

So the first should be yes because user1 can answer again during review period  
upvoted 1 times

RandomNickname Highly Voted 1 year, 5 months ago

#1 No, because as it's rolling "monthly" review cycle with an end date, the review period which is eligible for input or change is a 14 day period, since User 1 responded in the first period which started 15th Jan and ended 29th Jan, to respond 5th Feb would be outside of this scope.

#2 Yes, Similar to #1 for User1, this is within the 14 day period of User2.

#3 No, Reviews are for Group1, which User3 is not a member of.

upvoted 13 times

□ **Jhill777** 1 year ago

If you want to change your response, reopen the access reviews page and update your response. You can change your response at any time until the access review has ended.

upvoted 1 times

□ **Sorrynotsorry** Most Recent 2 weeks, 3 days ago

No. Yes. No

upvoted 1 times

□ **dule27** 5 months ago

NO

YES

NO

upvoted 1 times

□ **ThotSlayer69** 10 months, 1 week ago

- On February 5, User1 can answer the Review1 question again: No
- Review1 is closed for new answers, and the monthly frequency means it has not been enough time to launch a new one yet
- On January 25, User2 can answer the Review1 question again: Yes
- If by again they mean change their answer, then YES, BUT if by again they mean a new one, then NO
- Stupid question design
- On January 22, User3 can answer the Review1 question: No
- Not subject of review, not a member of the group

No

Yes (...Probably)

No

upvoted 2 times

□ **jack987** 11 months, 2 weeks ago

The correct answer is No - Yes - No

upvoted 2 times

□ **Jhill777** 1 year ago

If you want to change your response, reopen the access reviews page and update your response. You can change your response at any time until the access review has ended.

upvoted 1 times

□ **Jhill777** 1 year ago

Then MSFT says, "Duration (in days): How long a review is open for input from reviewers."

upvoted 2 times

□ **Xpb** 1 year, 3 months ago

No, Yes, No

upvoted 3 times

□ **rachee** 1 year, 4 months ago

Per the link, If you want to change your response, reopen the access reviews page and update your response. You can change your response at any time until the access review has ended.

Yes/Yes/No

upvoted 5 times

□ **InformationOverload** 1 year, 6 months ago

NO, YES, NO for me

upvoted 4 times

□ **clem24** 1 year, 6 months ago

No/Yes/No for me

User1 cant access the same review on 5th Feb as it falls outside of the 14 day window for that review. - No

User 2 can still access the review (within 14 days of current review). - Yes

User 3 isnt in scope of the review - No

upvoted 4 times

□ **TP447** 1 year, 7 months ago

No/Yes/No for me

User1 cant access the same review on 5th Feb as it falls outside of the 14 day window for that review. - No

User 2 can still access the review (within 14 days of current review). - Yes

User 3 isnt in scope of the review - No

upvoted 4 times

□ **SnottyPudding** 1 year, 8 months ago

1. NO. The review window is 1/15-1/29 and then starts again on 2/15. Between 1/30 and 2/14, responses cannot be submitted because this is outside of the 14-day response window. The access review is not every 14 days--it's monthly, with a 14-day response window.

2. YES. The user is changing her mind within the 14-day review response window.

3. YES. The response window is 1/15-1/29. User3 has until 1/29 to respond.

upvoted 3 times

✉ **Bulldozer** 1 year, 8 months ago

The correct answer is NO, YES, YES.

1 - NO: Because the review end date is 14 days after the start (January 15), the end of the review cycle for the month is January 29. After that date, the review cycle will not start again until February 15.

2 - YES: Because the user will not be removed from the group until the end of the access review period.

3 - YES: Because access review can be performed until January 29.

upvoted 3 times

✉ **JaspaJami** 1 year, 8 months ago

3: but User3 is not member of the group

upvoted 5 times

✉ **mcas** 1 year ago

owners are also members of a group in AAD, you can see it in the Groups blade when you select a group

upvoted 1 times

✉ **ZauberSRS** 12 months ago

I created a group in Azure AD, I made myself owner. I do not appear as member.

upvoted 1 times

✉ **NawafAli** 1 year, 11 months ago

YES, YES, NO

upvoted 8 times

✉ **BaderJ** 2 years, 2 months ago

Passed the exam today 23/09/2021

This question came in the exam.

upvoted 5 times

✉ **serggioff** 1 year, 8 months ago

callese inutil

upvoted 7 times

**HOTSPOT -**

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. The company has a business partner named Fabrikam, Inc.

Fabrikam uses Azure AD and has two verified domain names of fabrikam.com and litwareinc.com. Both domain names are used for Fabrikam email addresses.

You plan to create an access package named package1 that will be accessible only to the users at Fabrikam.

You create a connected organization for Fabrikam.

You need to ensure that the package1 will be accessible only to users who have fabrikam.com email addresses.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

To allow access for users who have fabrikam.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

Correct Answer:

**Answer Area**

To allow access for users who have fabrikam.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance**
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD**
- The External collaboration settings in Azure AD**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-request-policy>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create>

 **syougun200x** 2 months, 2 weeks ago

For those who are confused with policy and assignment, you can see policy is configured on this MS tutorial below. But I dont see "policy" when I create a new package in my test tenant. Maybe there was a layout change?

<https://www.youtube.com/watch?v=zaaKvaAYwI4&t=74s>

upvoted 1 times

 **marsof** 4 months, 2 weeks ago

Correct.

Box1: An access package POLICY in Identity Governance

Access Package Policy specifies the policy by which subjects may request or be assigned an access package via an access package assignment. While Access PackageAssignment is an assignment of an access package to a particular subject for a period of time.

Box2: The external Collaboration settings in Azure AD

Portal > Azure AD > External Identities > External collaboration Settings > Collaboration restrictions > Deny invitation to specified domains

Source: <https://learn.microsoft.com/en-us/graph/api/resources/entitlementmanagement-overview?view=graph-rest-1.0>

upvoted 3 times

□ **TafMuko** 5 months, 3 weeks ago

I don't see how External Collaboration settings would play a part in this if they are both internal verified domains...

upvoted 3 times

□ **JckD4Ni3L** 1 month, 1 week ago

This access package is created on contoso.com tenant FOR Fabrikam and litwareinc... collaboration will block litwareinc domain if configured so allowing only Fabrikam to access the package.

upvoted 1 times

□ **rajbne** 7 months, 1 week ago

just confused on the wording access package "assignment" or "policy" ?

upvoted 2 times

□ **northgaterebel** 3 months, 1 week ago

i am too. when creating a new access package, at the top of the Requests section it reads: "Create a policy to specify who can request an access package, who can approve requests, and when access expires." so i guess that means it's a policy although it's called Requests? so cryptic :-(

upvoted 1 times

□ **Jhill777** 1 year ago

Add an external Azure AD directory by typing one of its domain names. Note that users with any of the directory's domains in their UPN will be able to request, unless those domains are blocked by the B2B allow or deny list

upvoted 2 times

□ **lmeem** 1 year, 2 months ago

on the exam 09222022, i answered the same. Passed the exam, btw.

upvoted 4 times

□ **sapien45** 1 year, 5 months ago

It is called Collaboration Restrictions

upvoted 4 times

□ **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

□ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 2 times

□ **stromnessian** 1 year, 9 months ago

Given answer is correct.

upvoted 1 times

□ **phony** 1 year, 9 months ago

Block : <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/allow-deny-list>

upvoted 2 times

□ **phony** 1 year, 9 months ago

Add a deny list

This is the most typical scenario, where your organization wants to work with almost any organization, but wants to prevent users from specific domains to be invited as B2B users.

To add a deny list:

Sign in to the Azure portal.

Select Azure Active Directory > Users > User settings.

Under External users, select Manage external collaboration settings.

upvoted 1 times

□ **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 1 times

□ **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 2 times

 NawafAli 1 year, 11 months ago

correct answer.

upvoted 3 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection policies enforced.

You create an Azure Sentinel instance and configure the Azure Active Directory connector.

You need to ensure that Azure Sentinel can generate incidents based on the risk alerts raised by Azure AD Identity Protection.

What should you do first?

- A. Add a Microsoft Sentinel data connector.
- B. Configure the Notify settings in Azure AD Identity Protection.
- C. Create a Microsoft Sentinel playbook.
- D. Modify the Diagnostics settings in Azure AD.

**Correct Answer: A**

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-ad-identity-protection>

Community vote distribution

|         |         |
|---------|---------|
| C (77%) | A (23%) |
|---------|---------|

DeepMoon Highly Voted 1 year ago

Add a Microsoft Sentinel Data connector is the wrong answer. Meant to mislead.

Because question itself mentions that AAD connector was added. Which seem to cover all AAD functionality including Identity Protection feature.

What you are asked to do is generate incidents based on the risk alerts.

For that you use playbooks in Sentinel. Which automates tasks that SOC engineers need to such as generte risk alerts. So answer is C.  
upvoted 12 times

Ed2learn 1 month ago

This is not the same connector. There is AAD connector AND a AAD Identity Protection connector.

upvoted 2 times

ServerBrain 3 months ago

some people pay for this

upvoted 3 times

nils241 4 months ago

I agree with you

AAD Connector Description (from Sentinel Connectors)

The Azure Active Directory solution for Microsoft Sentinel enables you to ingest Azure Active Directory Audit, Sign-in, Provisioning, Risk Events and Risky User/Service Principal logs using Diagnostic Settings into Microsoft Sentinel.

upvoted 1 times

w00t Highly Voted 1 year, 2 months ago

Wording is kind of weird.

The data connector you're adding in Sentinel is called "Azure Active Directory Identity Protection".

So yes, you're adding a data connector within Sentinel.

upvoted 7 times

wooyourdaddy 10 months, 1 week ago

I agree with this answer. There are distinct Azure Active Directory and Azure Active Directory Identity Protection data connectors.

<https://learn.microsoft.com/en-us/azure/sentinel/data-connectors-reference#azure-active-directory>

<https://learn.microsoft.com/en-us/azure/sentinel/data-connectors-reference#azure-active-directory-identity-protection>

upvoted 3 times

AMZ 7 months ago

A. Add a Microsoft Sentinel data connector. - Reason, the connector that has been mentioned in the question is not the correct one for the use case. Logic app is not necessary to create an incident. incidents will show on the Sentinel page as log as the analytical rule is in place. Shitty question and MS is trying to catch us out. - answer A

upvoted 2 times

Sorrynotsorry Most Recent 2 weeks, 3 days ago

Selected Answer: A

AAD Identity Connector is a separate Connector, plus it has been changed now and added into the Defender 365 Data Connector

upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

The correct answer is D. Modify the Diagnostics settings in Azure AD.

According to the Microsoft Entra article on Connect Azure Active Directory data to Microsoft Sentinel1, you need to enable the Diagnostics settings in Azure AD to stream the sign-in logs, audit logs, and provisioning logs to a Log Analytics workspace. This is a prerequisite for connecting the Azure Active Directory data connector to Microsoft Sentinel.

upvoted 2 times

 **ACSC** 2 months ago

**Selected Answer: C**

Use playbook to generate incidents in Sentinel

upvoted 1 times

 **ServerBrain** 3 months ago

**Selected Answer: C**

The only way to generate incidents is by playbook

upvoted 1 times

 **prabhjot** 3 months, 2 weeks ago

Playbook comes Post Incident ( it job is SOAR and not incident management). I feel A and if you feel Data conenctor are already in place then the Ans Could be D ( that is config the Sign in log or user logs ) configuration part

upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: C**

C. Create a Microsoft Sentinel playbook.

upvoted 1 times

 **JN\_311** 5 months, 3 weeks ago

**Selected Answer: C**

I will go with Answer C, Sentinel Playbook. As the question mentions the AAD connector is created You create an 'Azure Sentinel instance' and configure the 'Azure Active Directory connector'.

upvoted 1 times

 **Bjarki2330** 6 months ago

**Selected Answer: A**

A is the right answer. There is a separate connector for AAD identity protection.

upvoted 2 times

 **ThotSlayer69** 10 months, 1 week ago

**Selected Answer: C**

Creating a Sentinel instance and configuring the Azure AD Connector = configuring the Azure AD connector within Sentinel settings, as detailed here: <https://learn.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts>

When configuring the connection, the option for Sentinel to generate incidents based on risk alerts for Azure AD Identity Protection is enabled, so it should already be connected and configured.

This is all done before we are asked what is the first thing we should do, and I'm honestly confused as to what they want. I guess playbooks are the next step?

So C?

upvoted 4 times

 **Techfall** 10 months, 1 week ago

No, wooyourdaddy has the answer below. The question specifically says that the \_Azure Active Directory\_ connector is installed - this does not have the logs needed for these alerts. The \_Azure Active Directory Identity Protection\_ connector needs to be installed. There is a more detailed description of this connector here: <https://learn.microsoft.com/en-us/azure/sentinel/media/incidents-from-alerts/generate-security-incidents.png> "Integrate... Identity Protection alerts with Microsoft Sentinel to... create custom alerts".

upvoted 2 times

 **ennak** 11 months, 1 week ago

playbook is the way to proceed if you want to have incident created

<https://learn.microsoft.com/en-us/azure/sentinel/overview>

upvoted 1 times

 **nhmh90** 11 months, 1 week ago

**Selected Answer: C**

I think the answer is C

<https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC>

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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure AD, you create an assignment for the Insights administrator role.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉  **nshg** 1 month, 1 week ago

To redirect the alerts, the action email settings need to be updated in the specific Azure Monitor alert rules to send to the new security admin's email address.

selected B

upvoted 1 times

✉  **dule27** 5 months, 1 week ago

**Selected Answer: B**

B. No is the correct answer

upvoted 1 times

✉  **DeepMoon** 1 year, 2 months ago

Correct Answer.

Permissions should be given to a Security Administrator or

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

Insights Administrator is an administrator Ofc365 Viva app. (Employee Experience Platform).

upvoted 2 times

✉  **Rucasll** 1 year, 2 months ago

create a data collection rule

upvoted 3 times

✉  **hb0011** 1 year, 3 months ago

So what is the right answer?

upvoted 1 times

✉  **TheMCT** 1 year, 1 month ago

The answer given is correct which is NO

upvoted 1 times

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

yea it is but what she meant was....Whats the correct way of doing so?

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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure AD, you modify the Diagnostics settings.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **dule27** 5 months, 1 week ago

**Selected Answer: B**

B. No is the correct answer  
upvoted 1 times

 **Nazir97** 11 months ago

Modifying the Diagnostics settings in Azure AD is one way to ensure that a new security administrator receives the alerts instead of you for failed Azure AD user sign-in attempts.

To do this, follow these steps:

Sign in to the Azure portal as a global administrator or security reader.

Navigate to Azure Active Directory > Diagnostic settings.

Select the diagnostic setting that you want to modify.

In the email notification section, add the email address of the new security administrator.

Click Save to apply the changes.

This will ensure that the new security administrator receives email alerts for failed Azure AD user sign-in attempts, instead of you.  
upvoted 2 times

 **haskelatchi** 6 months, 2 weeks ago

nice try microsoft employee or 5ft1 indian man with no hairline  
upvoted 5 times

 **wsrudmen** 10 months, 1 week ago

Where do you get that?  
This is wrong. There's no email notification for diagnostic setting.

You can only send to:

Send to Log Analytics workspace  
Archive to a storage account  
Stream to an event hub  
Send to partner solution

Correct answer is B -> NO

upvoted 3 times

 **jack987** 11 months, 2 weeks ago

**Selected Answer: B**

The correct answer is B -> NO

upvoted 1 times

 **estyj** 12 months ago

Ans B. No, Need to go to Azure monitor to modify action group not diagnostic settings.

upvoted 1 times

 **Jhill777** 1 year ago

**Selected Answer: B**

SigninLogs within "Diagnostic Setting" options are:

- Send to LAW
- Archive to a storage account
- Stream to an event hub
- Send to a partner solution.

upvoted 3 times

 **DeepMoon** 1 year ago

Answer is B.

Diagnostic settings are in Azure Monitor. Not in AAD.

Nothing here that say's about using Defender for Cloud. Defender for cloud is a separate service. And monitoring logs would be premium paid feature. Nothing here mentions Defender for Cloud.

upvoted 1 times

 **Jhill777** 1 year ago

I'm looking at them in AAD right now. Answer is still B though.

upvoted 2 times

 **Hot\_156** 1 year, 2 months ago

**Selected Answer: B**

Action group change is needed.

upvoted 2 times

 **Dragi** 1 year, 3 months ago

Action group change is needed.

upvoted 4 times

 **CDR** 1 year, 5 months ago

Customize the security alerts email notifications via the portal

You can send email notifications to individuals or to all users with specific Azure roles.

From Defender for Cloud's Environment settings area, select the relevant subscription, and open Email notifications.

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/configure-email-notifications>

upvoted 1 times

 **sapien45** 1 year, 5 months ago

Settings is done in alert group in LAW

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-install-use-log-analytics-views>

upvoted 1 times

 **RandomNickname** 1 year, 5 months ago

**Selected Answer: B**

B, nothing to see here....

upvoted 1 times

 **RandomNickname** 1 year, 5 months ago

It's likely you'll actually need Defender for Cloud apps activity policy, see below for reference;

<https://docs.microsoft.com/en-gb/defender-cloud-apps/user-activity-policies>.

upvoted 1 times

 **jasonga** 1 year, 5 months ago

**Selected Answer: B**

Should be B nothing in diagnostic settings allows configuration of a recipient for alerts

upvoted 2 times

 **jasonga** 1 year, 5 months ago

Should be B nothing in diagnostic settings allows configuration of a recipient for alerts

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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure Monitor, you create a data collection rule.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **dule27** 5 months, 1 week ago

**Selected Answer: B**

B. No is the correct answer  
upvoted 1 times

 **Xive** 1 year ago

**Selected Answer: B**

Action group is where you can update email recipients  
upvoted 1 times

 **DeepMoon** 1 year, 2 months ago

Given Answer is Correct. Data Collection Rules is not the way to go here.

Data Collection Rules (DCRs) define the data collection process in Azure Monitor. DCRs specify what data should be collected, how to transform that data, and where to send that data. Some DCRs will be created and managed by Azure Monitor to collect a specific set of data to enable insights and visualizations.

From <<https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-rule-overview>>

upvoted 1 times

 **Rucasll** 1 year, 2 months ago

Should be A  
upvoted 2 times

 **haskelatchi** 6 months, 2 weeks ago

I can see the 5ft1 little indian man with no hairline has made multiple accounts  
upvoted 1 times

You have an Azure Active Directory Premium P2 tenant.

You create a Log Analytics workspace.

You need to ensure that you can view Azure Active Directory (Azure AD) audit log information by using Azure Monitor.

What should you do first?

- A. Run the Set-AzureADTenantDetail cmdlet.
- B. Create an Azure AD workbook.
- C. Modify the Diagnostics settings for Azure AD.
- D. Run the Get-AzureADAuditDirectoryLogs cmdlet.

**Correct Answer: C**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics>

*Community vote distribution*

C (100%)

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: C**

C. Modify the Diagnostics settings for Azure AD.  
upvoted 1 times

 **dule27** 5 months, 1 week ago

**Selected Answer: C**

C. Modify the Diagnostics settings for Azure AD.  
upvoted 1 times

 **Jhill777** 1 year ago

**Selected Answer: C**

Send logs to Azure Monitor  
Sign in to the Azure portal.

Select Azure Active Directory > Diagnostic settings -> Add diagnostic setting. You can also select Export Settings from the Audit Logs or Sign-ins page to get to the diagnostic settings configuration page.

upvoted 3 times

 **DeepMoon** 1 year, 2 months ago

Given Answer is Correct.

AAD/Diagnostic Settings/Add Diagnostic Settings/Export Settings/Send to Log Analytic Workspace

<https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics#send-logs-to-azure-monitor>

Hybrid identity and access management best practices - BRK3243

upvoted 2 times

 **wooyourdaddy** 1 year, 6 months ago

**Selected Answer: C**

Based on the link provided below, this portion of page validates the answer:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics#send-logs-to-azure-monitor>

upvoted 1 times

 **kakakayayaya** 1 year, 6 months ago

Correct!

upvoted 1 times

## HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant contains the users shown in the following table.

| Name  | Role                                           |
|-------|------------------------------------------------|
| User1 | <b>None</b>                                    |
| User2 | <b>Privileged authentication administrator</b> |
| User3 | <b>Global administrator</b>                    |

In Azure AD Privileged Identity Management (PIM), you configure the Global administrator role as shown in the following exhibit.

| <b>Edit</b>                                                    |              |
|----------------------------------------------------------------|--------------|
| <b>Setting</b>                                                 | <b>State</b> |
| Activation maximum duration (hours)                            | 1 hour(s)    |
| Require justification on activation                            | Yes          |
| Require ticket information on activation                       | No           |
| On activation, require Azure MFA                               | Yes          |
| Require approval to activate                                   | No           |
| Approvers                                                      | None         |
| <b>Assignment</b>                                              |              |
| <b>Setting</b>                                                 | <b>State</b> |
| Allow permanent eligible assignment                            | Yes          |
| Expire eligible assignments after                              | -            |
| Allow permanent active assignment                              | Yes          |
| Expire active assignments after                                | -            |
| Require Azure Multi-Factor Authentication on active assignment | No           |
| Require justification on active assignment                     | Yes          |

User1 is eligible for the Global administrator role.

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

| Statements                                                                                        | Yes                              | No                               |
|---------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 requires Azure Multi-Factor Authentication (MFA) to activate the Global administrator role. | <input type="radio"/>            | <input type="radio"/>            |
| User2 must approve all activation requests for the Global administrator role.                     | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 and User3 can edit the Global administrator role assignment.                                | <input type="radio"/>            | <input checked="" type="radio"/> |

Correct Answer:

## Answer Area

| Statements                                                                                        | Yes                              | No                               |
|---------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 requires Azure Multi-Factor Authentication (MFA) to activate the Global administrator role. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 must approve all activation requests for the Global administrator role.                     | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 and User3 can edit the Global administrator role assignment.                                | <input type="radio"/>            | <input checked="" type="radio"/> |

Box 1: Yes -

MFA is required on activation -

Box 2: No -

The Privileged Authentication Administrator can set or reset any authentication method for any user, including Global Administrators.

The Privileged Role Administrator can manage role assignments, including the Global Administrator role, in Azure Active Directory, as well as within Azure AD

Privileged Identity Management. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units.

Box 3: No -

The Privileged Authentication Administrator can set or reset any authentication method for any user, including Global Administrators.

The Privileged Role Administrator can manage role assignments, including the Global Administrator role, in Azure Active Directory, as well as within Azure AD

Privileged Identity Management. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units.

 **dejo** Highly Voted  1 year, 2 months ago

Yes - "On activation, require Azure MFA" is set to Yes

No - "Require approval to activate" is set to No

No - Privileged Authentication Administrator can't assign roles (Privileged ROLE Administrator can!)

upvoted 23 times

 **viveet** Highly Voted 1 year, 2 months ago

Privileged Authentication Administrator Can access to view, set and reset authentication method information for any user (admin or non-admin).

Privileged Role Administrator Can manage role assignments in Azure AD, and all aspects of Privileged Identity Management.

upvoted 5 times

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

YES

NO

YES

upvoted 1 times

 **dule27** 5 months, 1 week ago

YES

NO

NO

upvoted 1 times

 **LeTrinh** 9 months ago

YES - The MFA is required for users who are eligible for a role

NO - Require approval set to NO

NO - because the Approval set to NONE -> User2 (Privileged Authentication administrator) cannot approve the active request -> ONLY Global Administrator or Privileged Role Administrator role can approve or manage PIM role settings (see picture)

upvoted 1 times

 **doch** 10 months, 2 weeks ago

YNY

#2 If no specific approvers are selected, Privileged Role Administrators and Global Administrators become the default approvers. But the role given to User2 here is Privileged Role Administrator.

#3 Privileged Authentication Administrator can manage Global Admin so this should be yes. <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-authentication-administrator>

upvoted 2 times

 **doch** 10 months, 1 week ago

Typo. But the role given to User2 here is Privileged \*\*Authen\*\* Administrator.

upvoted 2 times

 **Faheem2020** 1 year, 2 months ago

For the 2 and 3 to be YES, User 2 should be a privileged role administrator

upvoted 1 times

You have a Microsoft 365 subscription that contains the following:

- An Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium P2 license
- A Microsoft SharePoint Online site named Site1
- A Microsoft Teams team named Team1

You need to create an entitlement management workflow to manage Site1 and Team1.

What should you do first?

- A. Configure an app registration.
- B. Create an Administrative unit.
- C. Create an access package.
- D. Create a catalog.

**Correct Answer: C**

*Community vote distribution*

D (58%)      C (43%)

**Zak366** Highly Voted 9 months, 2 weeks ago

**Selected Answer: D**

Went to my tenant, tried creating access package under resource Roles with teams and sharepoint site and it is saying No groups in Default catalog, however, there is a checkbox which allows all groups and teams NOT in default catalog to show up, so technically I CAN create access package without creating a catalog first, but this is MS and question says "First" so I pick D, Create a catalog  
upvoted 6 times

**Nivos300** Most Recent 3 weeks, 4 days ago

**Selected Answer: C**

To initiate an entitlement management workflow for managing Site1 and Team1 in Microsoft 365, the first step is to create an access package. Access packages are fundamental to defining and managing access to resources, facilitating a streamlined entitlement management process. Therefore, the correct option is:  
C. Create an access package.  
upvoted 1 times

**JckD4Ni3L** 1 month, 1 week ago

**Selected Answer: C**

C. create an catalog, assign the ressources you need. then create a access package... I do this regularly with partner companies.  
upvoted 1 times

**Intrudire** 1 month, 2 weeks ago

**Selected Answer: D**

From the SC-300 book by Dwayne Natwick, 1st Edition, 2022, page 293:  
"The first step in entitlement management is to create catalogs. If you do not create a catalog for your access packages, users will have access to the general catalog. If you want to clearly define the catalog, then one should be created because you cannot move an access package to another catalog once it is created."  
upvoted 4 times

**ACSC** 2 months ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create#overview>  
upvoted 2 times

**sherifhamed** 2 months, 1 week ago

**Selected Answer: C**

C. Create an access package.

To create an entitlement management workflow to manage Site1 and Team1, you should start by creating an access package.  
upvoted 2 times

**zz64** 3 months, 2 weeks ago

I think the C will work. But the best way to do it is D...  
Create a new catalog, group resources inside and create an access package.  
upvoted 1 times

**nils241** 4 months ago

**Selected Answer: C**

I would say C.

Reason:

There is a Built-in catalog called "General". Therefore I can directly create an Access Package.

Checked this in my tenant under: Azure AD-> Identity Governance | Catalogs

Also from MS:

"If you don't specify a catalog, your access package goes in the general catalog"

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create#overview>

Therefore, it seems that it is not necessary to first create a catalog.

upvoted 3 times

✉ **dule27** 5 months, 1 week ago

**Selected Answer: D**

D. Create a catalog.

upvoted 3 times

✉ **Nazir97** 11 months ago

**Selected Answer: C**

it is C, watch this

<https://youtu.be/LGpgqRVG65g?t=8115>

upvoted 4 times

✉ **ikidreamz** 5 months, 3 weeks ago

Hi, the video shows an existing access package. When you create a new access package, you see a compulsory field called Catalog selection, so you need to have a catalog to add your package, so answer is D

upvoted 1 times

✉ **its\_tima** 9 months, 3 weeks ago

creating an access package is first, next comes the catalog

upvoted 1 times

✉ **jack987** 11 months, 1 week ago

**Selected Answer: D**

The correct answer is D - Create a catalog

Access packages for governed applications should be in a designated catalog. If you don't already have a catalog for your application governance scenario, create a catalog in Microsoft Entra entitlement management.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/identity-governance-applications-deploy#deploy-entitlement-management-policies-for-automating-access-assignment>

upvoted 3 times

✉ **Logitech** 2 months, 1 week ago

Why not use General Catalog? It is possible to create the access package right there.

upvoted 1 times

✉ **Logitech** 2 months, 1 week ago

Ok I tested it :). D - Create a catalog have to be done, or modify the general Catalog and the Groups and SharePoint Sites.

upvoted 1 times

✉ **AMDF** 11 months, 4 weeks ago

**Selected Answer: D**

Voting for D, Catalog

upvoted 4 times

✉ **mcas** 1 year ago

**Selected Answer: C**

as mentioned by others this MS article states you need to first create a Catalog, so should be C

<https://learn.microsoft.com/en-us/azure/active-directory/governance/identity-governance-applications-deploy#deploy-entitlement-management-policies-for-automating-access-assignment>

upvoted 4 times

✉ **SvenHorsheim** 1 year ago

**Selected Answer: D**

So sure. You could create an access package under the general catalog, but afaik you wouldn't be able to select either the SharePoint site or Teams site within the access package unless they were included in the Catalog, so before you did that you would have to add them to the catalog, so why not create a new catalog since you are messing with catalogs anyway?

upvoted 3 times

✉ **SvenHorsheim** 1 year ago

See this article. Clearly states all access packages should be in their own Catalog and the first step according to MSFT is to create a catalog and populate with your resources--in this case SPO and Teams sites.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/identity-governance-applications-deploy#deploy-entitlement-management-policies-for-automating-access-assignment>

upvoted 4 times

□ **lme** 1 year, 2 months ago

on the exam 09222022, i answered the same. Passed the exam, btw.

upvoted 1 times

□ **Faheem2020** 1 year, 2 months ago

"All access packages must be put in a container called a catalog. A catalog defines what resources you can add to your access package. If you don't specify a catalog, your access package will be put into the general catalog."

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create>

You don't need to create a catalog unless for delegation access. Access package is all that is needed

upvoted 4 times

□ **existingname** 1 year, 3 months ago

IMHO D. To create a access package, need to create a catalog first

upvoted 2 times

□ **vijeet** 1 year, 2 months ago

If you're an administrator or catalog owner, you can add resources to the catalog while creating an access package. If you're an access package manager, you can't add resources you own to a catalog. You're restricted to using the resources available in the catalog. If you need to add resources to a catalog, you can ask the catalog owner.

upvoted 1 times

□ **GryffindorOG** 1 year, 2 months ago

When you create and access package you have the option to create a catalog after you give the AP a name and description

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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure Monitor, you modify the action group.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

*Community vote distribution*

A (100%)

 **zed026** Highly Voted 1 year, 3 months ago

Answer should be Yes. <https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups#configure-notifications>  
upvoted 18 times

 **its\_tima** 10 months, 3 weeks ago

This exam question fails to clarify if its with least administrative support. There are 2 ways of doing this I assume, I guess the shortcut is to configure the diagnostic settings in Azure AD. The second option would be groups and configuring notifications  
upvoted 1 times

 **ServerBrain** 3 months ago

Why go to China via South Africa?? This is about Azure Monitor, best you edit Azure Monitor settings than Azure AD settings..  
upvoted 1 times

 **w00t** Highly Voted 1 year, 2 months ago

Should be YES - Action Group  
upvoted 10 times

 **haazybanj** Most Recent 4 weeks, 1 day ago

**Selected Answer: A**

Yes, modifying the action group in Azure Monitor will allow you to change the recipient of the email alerts for failed Azure AD user sign-in attempts.  
upvoted 1 times

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: A**

A. Yes

You can configure alert notifications in Azure Monitor by modifying the action group associated with the alert rule. In the action group settings, you can specify who should receive the notifications when the alert is triggered.  
upvoted 1 times

 **dule27** 5 months, 1 week ago

**Selected Answer: A**

A. Yes is the correct answer  
upvoted 1 times

 **SteveRivera** 5 months, 1 week ago

This question is part of a series of questions, configure the diagnostic settings and the action group are both correct. If you get this question in the test remember that one or more can be choose or none of them, in this case if you see these ones you know.  
upvoted 2 times

 **Arold75** 6 months, 2 weeks ago

**Selected Answer: A**

@Admin it is possible for you to update this response  
upvoted 2 times

 **topzz** 7 months, 4 weeks ago

SI SI SI!!!!

upvoted 2 times

 **MohamedBebars** 11 months, 1 week ago

**Selected Answer: A**

Yes it right one

upvoted 1 times

 **jack987** 11 months, 1 week ago

**Selected Answer: A**

The correct answer is A - Yes, you modify the action group from Azure Monitor.

<https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups#configure-notifications>

upvoted 1 times

 **kk1** 11 months, 2 weeks ago

**Selected Answer: A**

Should be YES - Action Group

upvoted 2 times

 **ccaitlab** 1 year ago

Wrong answer. Should be yes.

upvoted 3 times

 **Jawad1462** 1 year, 1 month ago

**Selected Answer: A**

Is the correct answer

upvoted 5 times

 **Hot\_156** 1 year, 2 months ago

**Selected Answer: A**

Should be Yes

upvoted 3 times

 **pikapin** 1 year, 2 months ago

**Selected Answer: A**

I agree, Yes

upvoted 4 times

 **niroha8910** 1 year, 2 months ago

Should be yes

upvoted 3 times

**HOTSPOT -**

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant.

The tenant contains the groups shown in the following table.

| Name   | Source                  | Member of   |
|--------|-------------------------|-------------|
| Group1 | Cloud                   | Group3      |
| Group2 | Active Directory domain | <b>None</b> |
| Group3 | Cloud                   | <b>None</b> |

The tenant contains the users shown in the following table.

| Name  | Directory-synced | Member of |
|-------|------------------|-----------|
| User1 | No               | Group1    |
| User2 | No               | Group2    |
| User3 | Yes              | Group3    |

You create an access review as shown in the following table.

| Setting                    | Value                   |
|----------------------------|-------------------------|
| Review type                | Teams + Groups          |
| Review scope               | All users               |
| Group                      | Group2, Group3          |
| Reviewers                  | Users review own access |
| If reviewers don't respond | Remove access           |

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

| Statements                                                                                            | Yes                              | No                    |
|-------------------------------------------------------------------------------------------------------|----------------------------------|-----------------------|
| User1 will be removed automatically from Group 1 if the user does not respond to the review request.  | <input type="radio"/>            | <input type="radio"/> |
| User 2 will be removed automatically from Group 3 if the user does not respond to the review request. | <input type="radio"/>            | <input type="radio"/> |
| User 3 will be removed automatically from Group 2 if the user does not respond to the review          | <input checked="" type="radio"/> | <input type="radio"/> |

Correct Answer:

## Answer Area

### Statements

Yes

No

User1 will be removed automatically from Group 1 if the user does not respond to the review request.

User 2 will be removed automatically from Group 3 if the user does not respond to the review request.

User 3 will be removed automatically from Group 2 if the user does not respond to the review

Box 1: No -

User1 is member of Group1. Group1 is in the cloud. Group1 is member of Group3. Group3 is in the cloud.

The access review applies to Group3, but not to Group1. The access review is setup to remove access if reviewers don't respond.

Box 2: Yes -

User2 is member of Group2. Group1 is in an Active Directory domain.

The access review applies to Group2.

Box 3: No -

User3 is member of Group3, not of Group2.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

✉ f3dj4 Highly Voted 1 year, 2 months ago

This should be N N N. User1's membership cannot be managed since he is a member of a nested group. User2's membership cannot be managed since he is a part of Group2 which is an AD group (not AAD). User3 is not the member of Group2.

upvoted 20 times

✉ jack987 11 months, 1 week ago

I agree with f3dj4. The answer is N N N.

upvoted 1 times

✉ mcas 1 year ago

User1's membership cannot be managed because he is not synced, he is only on-prem, not because he is a member of a nested group

upvoted 2 times

✉ Tanidanindo 4 months, 1 week ago

The fact that he is not directory synced means it's a cloud account.

upvoted 3 times

✉ geobarou Highly Voted 1 year, 2 months ago

Please some help with question2. Why is Yes? User2 is not a member of Group3.

upvoted 7 times

✉ purek77 11 months, 1 week ago

It should be No due to below. Especially 2nd paragraph:

Access Reviews can't change the group membership of groups that you synchronize from on-premises with Azure AD Connect. This is because the source of authority is on-premises.

You can still use Access Reviews to schedule and maintain regular reviews of on-premises groups. Reviewers will then take action in the on-premises group.

upvoted 4 times

✉ OK2020 Most Recent 4 months, 3 weeks ago

Given the question correction :

User2- Group3 & User3-Group2

The answer is: NYN

upvoted 4 times

✉ lahl 1 month, 1 week ago

I confirm that comes in the exam as :  
User2- Group3 & User3-Group2  
So the answer is : NYN  
upvoted 1 times

✉ **Hull** 3 months, 1 week ago

I do believe this is the case, User2, which is a cloud user, cannot be a member of AD synced group in the first place.  
upvoted 2 times

✉ **dule27** 5 months, 1 week ago

No  
No  
No  
upvoted 1 times

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

Answer is N, N, N on folks nem  
upvoted 1 times

✉ **splearner** 8 months, 1 week ago

On exam 2023-03-28, but they corrected it: the second table now says User2 belongs to Group3 and User3 belongs to Group2. Makes more sense now.  
upvoted 2 times

✉ **haovo** 11 months, 1 week ago

This question is on the exam today Dec 28th 2022. But the user group table is difference. User2 is a member of Group3 and User3 is a member of Group2.  
upvoted 6 times

✉ **Santeria** 11 months, 1 week ago

So it's NNY?  
upvoted 2 times

✉ **BB6919** 10 months, 4 weeks ago

So, it should be NNY as given in the answer. Because user2 which is a cloud account will be part of a cloud group and will get affected by access review.  
upvoted 5 times

✉ **Ikeinater** 12 months ago

NNN  
User 1 is in group 1 outside the scope of the review  
User 2 is not in group 3 so can't be removed from a group not a member of  
User 3 not in group 2 so can't be removed from a group not a member of  
upvoted 5 times

✉ **Cloud\_apps** 1 year ago

Dose any one know the proper answer for this. its messing with my progress  
upvoted 1 times

✉ **Jhill777** 1 year ago

Access reviews can't change the group membership of groups that you synchronize from on-premises with Azure AD Connect. This restriction is because the source of authority is on-premises.  
<https://learn.microsoft.com/en-us/azure/active-directory/governance/deploy-access-reviews>  
upvoted 3 times

✉ **Elpresidento27** 1 year, 1 month ago

<https://learn.microsoft.com/en-us/azure/active-directory/governance/complete-access-review#apply-the-changes>

- "Manually or automatically applying results doesn't have an effect on a group that originates in an on-premises directory."

- "For users who have membership through a nested group, we will not remove their membership to the nested group and therefore they will retain access to the resource being reviewed."

upvoted 3 times

✉ **chikorita** 8 months, 2 weeks ago

very informative  
upvoted 1 times

✉ **Hot\_156** 1 year, 2 months ago

\*\*\*Group 3 is a cloud group\*\*\* user2 is a cloud user\*\*\*\* They can be managed by Azure AD access review  
upvoted 1 times

✉ **Hot\_156** 1 year, 2 months ago

User2 is not a member of the group3 so that doesn't apply. Also, a cloud account cannot be a member of a synced group, so how is that user2 a member of Group2????  
upvoted 2 times

You have a Microsoft 365 E5 subscription that contains a web app named App1.

Guest users are regularly granted access to App1.

You need to ensure that the guest users that have NOT accessed App1 during the past 30 days have their access removed. The solution must minimize administrative effort.

What should you configure?

- A. a Conditional Access policy
- B. a compliance policy
- C. a guest access review
- D. an access review for application access

**Correct Answer: D**

Access to groups and applications for employees and guests changes over time. To reduce the risk associated with stale access assignments, administrators can use Azure Active Directory (Azure AD) to create access reviews for group members or application access.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

*Community vote distribution*

D (100%)

 **pikapin** Highly Voted 1 year, 2 months ago

**Selected Answer: D**

Correct

upvoted 8 times

 **haazybanj** Most Recent 4 weeks, 1 day ago

**Selected Answer: D**

The best answer is D. an access review for application access.

Access reviews for application access allow you to review and approve or deny user access to specific applications. This is the most specific and targeted solution to the problem, as it allows you to focus on the guest users that have not accessed App1 in the past 30 days.

Conditional access policies, compliance policies, and guest access reviews are all more general solutions that could be used to address the problem, but they would require more administrative effort to configure and manage.

upvoted 1 times

 **nshg** 1 month, 1 week ago

The correct answer is C) a guest access review.

A guest access review allows you to review and remove guest user access that is no longer needed. You can configure the policy to automatically remove access for guest users that have not accessed the application in a specified period of time, such as 30 days.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: D**

D. an access review for application access

upvoted 2 times

 **mali1969** 3 months, 3 weeks ago

C. a guest access review

You can create a recurring access review of guest users across all Microsoft 365 groups and applications, and specify the inactivity period as 30 days

upvoted 1 times

 **mali1969** 3 months, 3 weeks ago

the answer is C. a guest access review. A guest access review allows you to review and remove guest users who have not accessed a web app during a specified period of time. You can also enable automatic, recurring access reviews for guest users across all Microsoft 365 groups and Teams.

Some additional information:

- A Conditional Access policy is used to enforce security requirements for accessing resources, such as multi-factor authentication or device compliance.
- A compliance policy is used to define rules and actions to protect data on devices that are enrolled in Intune.
- An access review for application access is used to review and revoke user access to applications that are assigned through Azure AD.

upvoted 1 times

 **dule27** 5 months, 1 week ago

**Selected Answer: D**

D. an access review for application access

upvoted 1 times

 **reastman66** 11 months, 3 weeks ago

They have updated the name of the access review to Guests assigned to an application. Correct Answer is D

upvoted 4 times

## HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

| Name   | Owner | Number of internal users | Number of guest users |
|--------|-------|--------------------------|-----------------------|
| Group1 | User1 | 500                      | 25                    |
| Group2 | User2 | 295                      | 100                   |

You create an access review for Group1 as shown in the following table.

| Setting      | Value                   |
|--------------|-------------------------|
| Review type  | Teams + Groups          |
| Review scope | All users               |
| Reviewers    | Users review own access |

You create an access review for Group2 as shown in the following table.

| Setting      | Value            |
|--------------|------------------|
| Review type  | Teams + Groups   |
| Review scope | Guest users only |
| Reviewers    | Group owner      |

What is the minimum number of Azure Active Directory Premium P2 licenses required for each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Group1:


Group2:


Group1:


Correct Answer: Group2:


Box 1: 525 -

For Group1:

Review scope: All users, Reviewers: Users review own access

Note: How many licenses must you have?

Your directory needs at least as many Azure AD Premium P2 licenses as the number of employees who will be performing the following

tasks:

Member users who are assigned as reviewers

Member users who perform a self-review

Member users as group owners who perform an access review

Member users as application owners who perform an access review

For guest users, licensing needs will depend on the licensing model you're using. However, the below guest users' activities are considered

Azure AD Premium

P2 usage:

Guest users who are assigned as reviewers

Guest users who perform a self-review

Guest users as group owners who perform an access review

Guest users as application owners who perform an access review

Box 2: 1 -

For Group2:

Review scope: Guest users only. Reviewers: Group Owner.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#license-requirements>

ACSC Highly Voted 1 year ago

Answer is:

Group 1: 500 - Guest users (4th example in the link)

Group 2: 1

<https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#example-license-scenarios>

upvoted 20 times

jack987 Highly Voted 11 months, 1 week ago

The correct answer is:

Group 1: 500

Group 2: 1

Scenario = An administrator creates an access review of Group C with 50 member users and 25 guest users. Makes it a self-review.

Calculation = 50 licenses for each user as self-reviewers.\*

Number of licenses = 50

\* Azure AD External Identities (guest user) pricing is based on monthly active users (MAU), which is the count of unique users with authentication activity within a calendar month. This model replaces the 1:5 ratio billing model, which allowed up to five guest users for each Azure AD Premium license in your tenant.

Refer to: <https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#license-requirements>

upvoted 7 times

mayleni 9 months, 3 weeks ago

totally, also is the example in doc!!!!

upvoted 2 times

c2thelint Most Recent 3 months, 1 week ago

Licences are not required for the guest users as they use the AD External Identities (guest user) licencing model where the first 50,000 monthly guest user activities are free.

upvoted 2 times

marsot 4 months, 2 weeks ago

Box 1: 500, because guest users may not count, depending on the agreement.

Box2: 1, only the owner needs a license

upvoted 1 times

dule27 5 months ago

Group 1: 525 ?

Group 2: 1

upvoted 1 times

dule27 5 months ago

Correction:

Group 1: 500

Group 2: 1

upvoted 1 times

sbettani 6 months, 1 week ago

525 - 1 <https://learn.microsoft.com/en-us/azure/active-directory/governance/manage-guest-access-with-access-reviews>

upvoted 1 times

□  **Jhill777** 1 year ago

Going with 500 for the first one.

In your Azure AD tenant, guest user collaboration usage is billed based on the count of unique guest users with authentication activity within a calendar month. This model replaces the 1:5 ratio billing model, which allowed up to five guest users for each Azure AD Premium license in your tenant. When your tenant is linked to a subscription and you use External Identities features to collaborate with guest users, you'll be automatically billed using the MAU-based billing model.

Your first 50,000 MAUs per month are free for both Premium P1 and Premium P2 features. To determine the total number of MAUs, we combine MAUs from all your tenants (both Azure AD and Azure AD B2C) that are linked to the same subscription.

upvoted 3 times

□  **TheMCT** 1 year, 1 month ago

The given answer is correct.

Your directory needs at least as many Azure AD Premium P2 licenses as the number of employees who will be performing the following tasks:

Member users who are assigned as reviewers

Member users who perform a self-review

Member users as group owners who perform an access review

Member users as application owners who perform an access review

upvoted 6 times

□  **Koekjesdoos** 11 months, 3 weeks ago

See ACSC answers. Guest users don't need the license

upvoted 1 times

**HOTSPOT -**

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a group named All Company and has the following Identity Governance settings:

- Block external users from signing in to this directory: Yes
- Remove external user: Yes
- Number of days before removing external user from this directory: 30

On March 11, 2022, you create an access package named Package1 that has the following settings:

- Resource roles
- 1. Name: All Company
- 2. Type: Group and Team
- 3. Role: Member
- Lifecycle
- 1. Access package assignment expire: On date
- 2. Assignment expiration date: April 1, 2022

On March 1, 2022, you assign Package1 to the guest users shown in the following table.

| Name   | Email address      |
|--------|--------------------|
| Guest1 | guest1@outlook.com |
| Guest2 | guest2@outlook.com |

On March 2, 2022, you assign the Reports reader role to Guest1.

On April 1, 2022, you invite a guest user named Guest3 to contoso.com.

On April 4, 2022, you add Guest3 to the All Company group.

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

NOTE: Each correct selection is worth one point.

Hot Area:

| <b>Statements</b>                                     | <b>Yes</b>            | <b>No</b>             |
|-------------------------------------------------------|-----------------------|-----------------------|
| On May 5, 2022, the Guest1 account is in contoso.com. | <input type="radio"/> | <input type="radio"/> |
| On May 5, 2022, the Guest2 account is in contoso.com. | <input type="radio"/> | <input type="radio"/> |
| On May 5, 2022, the Guest3 account is in contoso.com. | <input type="radio"/> | <input type="radio"/> |

Correct Answer:

| <b>Statements</b>                                     | <b>Yes</b>                       | <b>No</b>                        |
|-------------------------------------------------------|----------------------------------|----------------------------------|
| On May 5, 2022, the Guest1 account is in contoso.com. | <input type="radio"/>            | <input checked="" type="radio"/> |
| On May 5, 2022, the Guest2 account is in contoso.com. | <input type="radio"/>            | <input checked="" type="radio"/> |
| On May 5, 2022, the Guest3 account is in contoso.com. | <input checked="" type="radio"/> | <input type="radio"/>            |

Box 1: No -

On March 2, 2022, you assign the Reports reader role to Guest1.

On April 1 the access package assignment expires. After another 30 days, well before May 5, the guest user account is removed.

Box 2: No -

On April 1 the access package assignment expires. After another 30 days, well before May 5, the guest user account is removed.

Box 3: Yes -

Note: Lifecycle -

On the Lifecycle tab, you specify when a user's assignment to the access package expires. You can also specify whether users can extend their assignments.

In the Expiration section, set Access package assignments expires to On date, Number of days, Number of hours, or Never.

For On date, select an expiration date in the future.

For Number of days, specify a number between 0 and 3660 days.

For Number of hours, specify a number of hours.

Based on your selection, a user's assignment to the access package expires on a certain date, a certain number of days after they are approved, or never.

Note 2: By default, when an external user no longer has any access package assignments, they are blocked from signing in to your directory. After 30 days, their guest user account is removed from your directory.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-lifecycle-policy>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users>

□ **Learner2022** Highly Voted 1 year ago

How can you assign package 1 on 1st March 2022 before package 1 was created (on 11th March 2022)?

upvoted 16 times

□ **mcas** Highly Voted 1 year ago

The Identity Governance settings state:

Select what happens when an external user, who was added to your directory through an access package request, loses their last assignment to any access package.

Number of days before removing external user from this directory: 30

the Assignment (assigned to Guest1 and Guest2) expires on April 1, 2022 so by May 1 the 30 days have passed and therefore Guest 1 and Guest 2 are removed, so Q1 and Q2 should be NO

Q3 is YES because Guest 3 is not affected by the access package

upvoted 6 times

□ **VeIN** 11 months, 1 week ago

There is lack of info in this question & date mix for me. From the description it looks like at least guest 1 & 2 already existed before package was assigned so they will be NOT removed. (box 1 & 2 : YES)

"Entitlement management ONLY removes accounts that were invited through entitlement management. Also, note that a user will be blocked from signing in and removed from this directory even if that user was added to resources in this directory that were not access package assignments. If the guest WAS PRESENT in this directory prior to receiving access package assignments, they will remain. However, if the guest was invited through an access package assignment, and after being invited was also assigned to a OneDrive for Business or SharePoint Online site, they will still be removed."

upvoted 1 times

□ **rajbne** 7 months, 1 week ago

agreed , based on that it should YYY

upvoted 1 times

□ **dule27** Most Recent 5 months ago

NO

NO

YES

upvoted 2 times

□ **dobriv** 6 months, 3 weeks ago

It should be NO, NO, NO

"Entitlement management only removes accounts that were invited through entitlement management. Also, note that a user will be blocked from signing in and removed from this directory even if that user was added to resources in this directory that were not access package assignments. If the guest was present in this directory prior to receiving access package assignments, they will remain. However, if the guest was invited through an access package assignment, and after being invited was also assigned to a OneDrive for Business or SharePoint Online site, they will still be removed."

you can find this at the end of the link :

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users>

upvoted 5 times

□ **mayleni** 9 months, 3 weeks ago

I will say NO, NO, NO.

Guest 3 is affected by global guest user policy, no by package

upvoted 3 times

□ **its\_tima** 9 months, 3 weeks ago

you're right, Guest3 has no link to the access package, therefore, no timed assignment policy will be applied. So they still exist

upvoted 1 times

 **Taigr** 9 months, 3 weeks ago

Well, but Guest3 was added in group named All Company and has the following Identity Governance settings:  
① Block external users from signing in to this directory: Yes  
② Remove external user: Yes  
③ Number of days before removing external user from this directory: 30

So should not be based on this membership deleted as external user after 30 days?  
He was added 4.April, so 5th May can be deleted already.  
upvoted 1 times

 **hyc1983** 1 year ago

I think the answer is correct. For guest1 and guest2, they were added through an access package. Even though guest1 was assigned a role later, the settings for the lifecycle of external users will have impacts.  
For guest3, it's not added through access packages, so it's not affected.  
upvoted 1 times

 **Hot\_156** 1 year, 2 months ago

User3 was invited to the tenant the day the access package expired, so if I am not wrong, it didn't affect User3, as the access package already expired, it won't remove the guests later on  
upvoted 2 times

 **apokavk** 1 year, 2 months ago

on second thought user 3 is not in the assignment of the package and is added manually, so it could be yes indeed  
upvoted 1 times

 **apokavk** 1 year, 2 months ago

this is wrong...got confused, identity governance will remove it...

upvoted 3 times

 **apokavk** 1 year, 2 months ago

IMHO the third answer is no because on the 5th of May the access package has already expired and user 3 is not able to gain access  
upvoted 2 times

 **Hot\_156** 1 year, 1 month ago

This makes me think the account is still in the company on May 5th because in April it was added to a role. The account won't be removed from the company if there is any access assigned to it.

On April 4, 2022, you add Guest3 to the All Company group.

Or am I wrong?

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant named Contoso that contains a terms of use (Toll) named Terms1 and an access package. Contoso users collaborate with an external organization named Fabrikam. Fabrikam users must accept Terms1 before being allowed to use the access package.

You need to identify which users accepted or declined Terms1.

What should you use?

- A. sign-in logs
- B. the Usage and Insights report
- C. provisioning logs
- D. audit logs

**Correct Answer: D**

View Azure AD audit logs -

If you want to view more activity, Azure AD terms of use policies include audit logs. Each user consent triggers an event in the audit logs that is stored for 30 days.

You can view these logs in the portal or download as a .csv file.

To get started with Azure AD audit logs, use the following procedure:

1. Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator.
2. Browse to Azure Active Directory > Security > Conditional Access > Terms of use.
3. Select a terms of use policy.
4. Select View audit logs.
5. On the Azure AD audit logs screen, you can filter the information using the provided lists to target specific audit log information.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

*Community vote distribution*

D (92%) 8%

✉ **palito1980** Highly Voted 1 year, 2 months ago

**Selected Answer: D**

This link supports the answer

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use#view-azure-ad-audit-logs>

upvoted 8 times

✉ **haazybanj** Most Recent 4 weeks, 1 day ago

**Selected Answer: D**

The correct answer is D. audit logs.

Audit logs contain a record of all administrative actions and changes made within Azure AD, such as user and group management, application assignments, and policy modifications.

upvoted 1 times

✉ **Leacco99** 2 months, 1 week ago

Audit logs

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

upvoted 1 times

✉ **Jzx** 2 months, 3 weeks ago

**Selected Answer: B**

B. The Usage and Insights report:

This report provides information about how users are using various features and services in Azure AD. It can track whether users have accepted or declined terms of use, making it a suitable choice for your scenario.

upvoted 1 times

✉ **EmnCours** 4 months, 1 week ago

**Selected Answer: D**

Selected Answer: D

upvoted 1 times

 **dule27** 5 months, 1 week ago

**Selected Answer: D**

D. audit logs

upvoted 1 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name  | User type | Member of |
|-------|-----------|-----------|
| User1 | Member    | Group1    |
| User2 | Member    | Group1    |
| User3 | Guest     | Group1    |

User1 is the owner of Group1.

You create an access review that has the following settings:

- What to review: Teams + Groups
- Scope: All users
- Group: Group1
- Reviewers: Users review their own access

Which users can perform access reviews for User3?

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

#### Correct Answer: A

Note:

If you set Select reviewers to Users review their own access or Managers of users, B2B direct connect users and Teams won't be able to review their own access in your tenant. The owner of the Team under review will get an email that asks the owner to review the B2B direct connect user and Teams.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

Community vote distribution

|         |    |
|---------|----|
| B (95%) | 5% |
|---------|----|

□  **JakeLi** Highly Voted 1 year, 1 month ago

Correct answer is B: User3

You can ask the guests themselves or a decision maker to participate in an access review and recertify (or attest) to the guests' access.

Refer to the below article:

<https://learn.microsoft.com/en-us/azure/active-directory/governance/manage-guest-access-with-access-reviews>  
upvoted 7 times

□  **ACSC** Most Recent 2 months ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/active-directory/governance/manage-guest-access-with-access-reviews>  
upvoted 2 times

□  **c2thelint** 3 months, 1 week ago

A seems right. In a team or group access review, only the group owners (at the time the review starts) are considered as reviewers.  
upvoted 1 times

□  **EmnCours** 4 months, 1 week ago

Selected Answer: B

Correct answer is B  
upvoted 2 times

□  **Sango** 5 months ago

A (User 1 = Owner). A. If you set Select reviewers to Users review their own access or Managers of users, B2B direct connect users and Teams won't be able to review their own access in your tenant. The owner of the Team under review (User 1) will get an email that asks the owner to review the B2B direct connect user and Teams. Source: <https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review>  
upvoted 2 times

□  **dule27** 5 months, 1 week ago

Selected Answer: B

B. User3 only  
upvoted 3 times

 **Taigr** 9 months, 3 weeks ago

**Selected Answer: A**  
Based on Microsoft description is answer A correct I think.

If you set Select reviewers to Users review their own access or Managers of users, B2B direct connect users and Teams won't be able to review their own access in your tenant. The owner of the Team under review will get an email that asks the owner to review the B2B direct connect user and Teams.

If you select Managers of users, a selected fallback reviewer will review any user without a manager in the home tenant. This includes B2B direct connect users and Teams without a manager.

upvoted 1 times

 **kmk\_01** 7 months, 3 weeks ago

There is no indication in the question that User 3 is a B2B Direct Connect User. So answer A doesn't apply.  
upvoted 1 times

 **AlanWake69** 11 months, 1 week ago

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

 **jack987** 11 months, 1 week ago

**Selected Answer: B**  
I agree with JakeLi. The correct answer is B - User3 only.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/manage-guest-access-with-access-reviews>  
upvoted 2 times

 **ACSC** 1 year ago

**Selected Answer: B**  
Users make their own review  
upvoted 1 times

 **libran** 1 year, 1 month ago

**Selected Answer: B**  
Correct answer is B: User3  
upvoted 1 times

 **Hot\_156** 1 year, 2 months ago

**Selected Answer: B**  
This is the same question as "Question #3 - Topic 4" and the answer is B  
upvoted 2 times

 **geobarou** 1 year, 2 months ago

**Selected Answer: B**  
Correct answer is B: User2.  
The access review is one-stage access review. Because of the value 'Users review their own access', every member will review his access. The owner will perform the access review with the value 'Users review their own access' ONLY if it is a multi-stage access. That's what the link says.  
upvoted 2 times

 **Hot\_156** 1 year, 2 months ago

**Selected Answer: B**  
The link makes reference to this  
"If you set Select reviewers to Users review their own access or Managers of users, B2B direct connect users and Teams won't be able to review their own access in your tenant. The owner of the Team under review will get an email that asks the owner to review the B2B direct connect user and Teams."  
However, there is no information saying anything about this being a B2B direct connect organization... If I am not wrong, when there is a B2B direct org connected, the user type is not Guest... not sure but I would say B is the correct answer here  
upvoted 3 times

 **pikapin** 1 year, 2 months ago

**Selected Answer: B**  
I would say B too  
upvoted 1 times

 **Imee** 1 year, 2 months ago

on the exam 09222022, i answered the same. Passed the exam, btw.  
upvoted 2 times

 **w00t** 1 year, 2 months ago

USER 3 -- B

upvoted 3 times

店铺：专业认证88

店铺：专业认证88

**HOTSPOT -**

You have an Azure Active Directory (Azure AD) tenant that contains three users named User1, User2, and User3.

You create a group named Group1. You add User2 and User3 to Group1.

You configure a role in Azure AD Privileged Identity Management (PIM) as shown in the Application Administrator exhibit. (Click the Application Administrator tab.)

## Role setting details - Application Administrator

Privileged Identity Management | Azure AD roles



Edit

### Activation

| Setting                                  | State                 |
|------------------------------------------|-----------------------|
| Activation maximum duration (hours)      | 5 hour(s)             |
| Require justification on activation      | Yes                   |
| Require ticket information on activation | No                    |
| Require approval to activate             | Yes                   |
| Approvers                                | 0 Member(s), 1 Group( |

### Assignment

| Setting                                              | State      |
|------------------------------------------------------|------------|
| Allow permanent eligible assignment                  | No         |
| Expire eligible assignments after                    | 3 month(s) |
| Allow permanent active assignment                    | No         |
| Expire active assignments after                      | 1 month(s) |
| Require Azure Multi-Factor Authentication on acti... | No         |
| Require justification on active assignment           | Yes        |

Group1 is configured as the approver for the Application administrator role.

You configure User2 to be eligible for the Application administrator role.

For User1 you add an assignment to the Application administrator role as shown in the Assignment exhibit. (Click the Assignment tab.)

# Add assignments

Privileged Identity Management | Azure AD roles

Membership    Setting

Assignment type ⓘ

Eligible

Active

Maximum allowed eligible duration is 3 month(s).

Assignment starts \*

01/01/2021



12:00:00 AM

Assignment ends \*

01/31/2021



11:59:00 PM

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

NOTE: Each correct selection is worth one point.

Hot Area:

| Statements                                                                                                                                                                  | Yes                   | No                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| User1 is assigned the Application administrator role automatically.                                                                                                         | <input type="radio"/> | <input type="radio"/> |
| When User2 requests to be assigned the Application administrator role, only User3 can approve the request.                                                                  | <input type="radio"/> | <input type="radio"/> |
| If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00. | <input type="radio"/> | <input type="radio"/> |

Correct Answer:

| Statements                                                                                                                                                                  | Yes                              | No                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 is assigned the Application administrator role automatically.                                                                                                         | <input type="radio"/>            | <input checked="" type="radio"/> |
| When User2 requests to be assigned the Application administrator role, only User3 can approve the request.                                                                  | <input type="radio"/>            | <input checked="" type="radio"/> |
| If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00. | <input checked="" type="radio"/> | <input type="radio"/>            |

Box 1: No -

User1 is eligible from 1/1/2021 to 1/31/2021.

However, here the Application Administrator role requires approval.

Box 2: No -

User2 is also member of Group1, and Group1 is configured as the approver for the Application administrator role.

Box 3: Yes -

User1 is eligible from 1/1/2021 to 1/31/2021.

Activation maximum duration (hours) is set to 5 hours.

existingname Highly Voted 1 year, 3 months ago

On the exam today  
I answer N, Y, Y  
I think user2 cannot approve his own request  
upvoted 18 times

Bjarki2330 1 year, 3 months ago

I agree. You can see it stated here: <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow>

"Approvers are not able to approve their own role activation requests."  
upvoted 9 times

Logitech 2 months, 1 week ago

Thank you for the link.  
The wording of the quets sucks because he has allready an eligible assingment.  
And they write: when users2 request to be assigned... instead of when user2 activates his role.  
Assignment is not activation in my opinion.  
MS quests make me angry, sometimes.  
upvoted 1 times

jack987 11 months, 1 week ago

I agree with existingname. The correct answer is N-Y-Y.  
upvoted 1 times

Hot\_156 Highly Voted 1 year, 2 months ago

It is N,Y,Y  
I tested this in my lab, so you cannot approve a request for yourself. Also, if there are guest accounts in the group, they will receive the email about approving the request but they cannot do it  
upvoted 7 times

Nyamnyam Most Recent 3 weeks, 2 days ago

N-Y-N  
1. User1 is set as eligible, not active.  
2. Approvers are not able to approve their own role activation requests.  
3. Assignment expires on 31 Jan at 23:59. Full stop.  
upvoted 2 times

Nivos300 3 weeks, 6 days ago

I think the answer is correct  
N  
N  
Y  
upvoted 1 times

cgonIT 1 month, 3 weeks ago

Correct Answer is: No, No, No.  
1. No. The User1 needs to be approved by any approver (User2 or User3, so Group1 Users).  
2. No. Approvers are not able to approve their own role activation requests, see next link:  
<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-approval-workflow#approve-requests>  
3. No. The role can't be request to be activated if end-date is after the End Time of the assigned Role. Tested in lab right now and the error message during activation says:  
"The following policy rules failes:[\"ExpirationRule\"]".  
upvoted 2 times

curtmcgirt 2 weeks, 4 days ago

doesn't your explanation of #2 mean that only user3 can approve user2's request? aka 'yes'?  
upvoted 1 times

dule27 5 months ago

NO  
YES  
YES  
upvoted 1 times

ExamStudy68 7 months, 3 weeks ago

I may be wrong, but I think the point of the last question is User1 activated on Jan 31 at 23:00 so User1 is activated when the assignment ends at 11:59pm - before the five hour time limit completes. Not sure what the answer is - still looking.  
upvoted 2 times

LeTrinh 9 months, 3 weeks ago

N, Y, N  
The Activation maximum duration (5 hours) is only for the timeline of the request to activate the role. So the answer is wrong.  
upvoted 4 times

 **34reefer** 8 months, 1 week ago

31 jan 23:00 > 1 Feb 04:00 is 5 hours, so N,Y,Y  
upvoted 2 times

 **b233f0a** 5 months, 1 week ago

N,Y,N  
Assignment expired 31 Jan @ 11:59 so cannot be used in Feb  
upvoted 3 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

**HOTSPOT -**

You have a Microsoft 365 E5 subscription.

You create an access review for Azure Active Directory (Azure AD) roles.

You need to ensure that users who do not respond to review requests are removed automatically from the roles. The solution must minimize administrative effort.

Which two settings should you modify? To answer, select the settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Reviewers**

Reviewers

店铺：专业认证88 Members (self) ▼

^ Upon completion settings

Auto apply results to resource ⓘ Enable Disable

If reviewers don't respond ⓘ No change ▼

Action to apply on denied guest users ⓘ Remove user's membership from the resource ▼

(Preview) At end of review, send + Select User(s) or Group(s)  
notification to

^ Advanced settings

Show recommendations ⓘ Enable Disable

Require reason on approval ⓘ Enable Disable

Mail notifications ⓘ Enable Disable

Reminders ⓘ Enable Disable

Additional content for reviewer email ⓘ

### Correct Answer:

Reviewers

Reviewers

Members (self)



#### Upon completion settings

Auto apply results to resource ⓘ Enable Disable

If reviewers don't respond ⓘ No change



Action to apply on denied guest users ⓘ Remove user's membership from the resource



(Preview) At end of review, send notification to + Select User(s) or Group(s)

#### Advanced settings

Show recommendations ⓘ Enable Disable

Require reason on approval ⓘ Enable Disable

Mail notifications ⓘ Enable Disable

Reminders ⓘ Enable Disable

Additional content for reviewer email ⓘ

Box 1: Reviewers, Members (self)

Reviewers for guest users can be:

Specified reviewers: Certain users within your organization

Group owners: Office 365 Group owners that also includes Teams

Self-review: Guest users can review access on their own

Box 2: If reviewers don't respond, No Change

If reviewers don't respond (within the configured review period):

No change: Leave user's access unchanged

Remove access: Remove user's access

Approve access: Approve user's access

Take recommendations: Take the system's recommendation on denying or approving the user's continued access

Reference:

<https://blog.quadrotech-it.com/blog/how-to-manage-guest-access-in-azure-active-directory-pt-1/>

ACSC Highly Voted 1 year ago

In my opinion

Box 1: Reviewers, Members (self)

Box 2: If reviewers don't respond, Remove access

This is the least administrative effort.

upvoted 9 times

existingname Highly Voted 1 year, 3 months ago

on the exam today. I chose:

- if reviewers didn't respond

- additional content for reviewer e-mail

upvoted 6 times

Nyamnyam Most Recent 3 weeks, 2 days ago

Really dumb question. Only one setting change is needed:

If reviewer don't respond = Remove access

IMO, the Members (self) should NOT be changed - this is the best possible way to reduce admin effort. And is the only possible way to remove ONLY the non-responding users.

upvoted 1 times

 **dobriv** 6 months, 3 weeks ago

For me these are correct :

- 1) If reviewers don't respond - remove access
- 2) Require reason on approval - disable

The first one is clear.

The second one is for minimum administrative effort.

upvoted 2 times

 **chikorita** 8 months, 2 weeks ago

for me;

Auto apply result to resource: this will automatically remove the access

If Reviewers don't respond: then remove access.

correct me if wrong

upvoted 1 times

 **chikorita** 8 months, 1 week ago

appearing for exam tomorrow, still positive on this answer

upvoted 1 times

 **DeepMoon** 1 year ago

Box 1: If Reviewers don't respond, remove access.

Box 2: Additional Content for Reviewer email,

Warn users due to inaction.

Since you don't users caught off guard with inaction and creating additional administrative effort;

upvoted 3 times

 **pikapin** 1 year, 2 months ago

Should not include Remove access too?

upvoted 1 times

 **geobarou** 1 year, 2 months ago

IMO the answer is:

-if reviewers didn't respond / obviously

-At the end of review, send notification to / Because it says "You need to ensure..."

upvoted 2 times

**HOTSPOT**

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.

An administrator deletes User1.

You need to identify the following:

- How many days after the account of User1 is deleted can you restore the account?
- Which is the least privileged role that can be used to restore User1?

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Number of days:

  
15  
30  
90  
180

Role:

  
User administrator  
Network administrator  
Helpdesk administrator  
Domain name administrator

Number of days: 30

**Correct Answer:**

Role: User administrator

 **BRoald** Highly Voted 10 months, 2 weeks ago

Correct, the helpdesk administrator cannot recover deleted users and the other 2 options doesn't make any sense;

1. 30 days
  2. user administrator
- upvoted 12 times

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

1. 30 days
  2. user administrator
- upvoted 2 times

 **dule27** 5 months, 1 week ago

Number of days: 30  
Role: User Administrator  
upvoted 1 times

 **penatuna** 7 months, 1 week ago

Number of days: 30

After you delete a user, the account remains in a suspended state for 30 days. During that 30-day window, the user account can be restored, along with all its properties. After that 30-day window passes, the permanent deletion process is automatically started and can't be stopped.

Role: User Administrator

You must have one of the following roles to restore and permanently delete users.

- Global administrator
- Partner Tier1 Support
- Partner Tier2 Support
- User administrator

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

upvoted 3 times

 **Taigr** 9 months, 2 weeks ago

Was on test 24.02.2022. I answered same as here is.

upvoted 1 times

## HOTSPOT

You have an Azure AD tenant that contains the groups shown in the following exhibit.

| <input type="checkbox"/> | Name ↑         | Group Type    | Membership Type | Source            | Security enabled |
|--------------------------|----------------|---------------|-----------------|-------------------|------------------|
| <input type="checkbox"/> | AC All Company | Microsoft 365 | Assigned        | Cloud             | No               |
| <input type="checkbox"/> | G Group1       | Microsoft 365 | Assigned        | Cloud             | Yes              |
| <input type="checkbox"/> | GR Group2      | Security      | Assigned        | Cloud             | Yes              |
| <input type="checkbox"/> | GR Group3      | Security      | Dynamic         | Cloud             | Yes              |
| <input type="checkbox"/> | GR Group4      | 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.

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 a managed identity to <answer choice>.

Group2 only  
All Company and Group1 only  
Group2, Group3, and Group4 only  
All Company, Group1, and Group2 only  
All Company, Group1, Group2, Group3, and Group4

You can add an Azure AD cloud user to <answer choice>.

Group2 only  
All Company and Group1 only  
Group2, Group3, and Group4 only  
All Company, Group1, and Group2 only  
All Company, Group1, Group2, Group3, and Group4

**Answer Area**

You can add a managed identity to <answer choice>.

Group2 only  
All Company and Group1 only  
Group2, Group3, and Group4 only  
All Company, Group1, and Group2 only  
All Company, Group1, Group2, Group3, and Group4

**Correct Answer:**

You can add an Azure AD cloud user to <answer choice>.

Group2 only  
All Company and Group1 only  
Group2, Group3, and Group4 only  
All Company, Group1, and Group2 only  
All Company, Group1, Group2, Group3, and Group4

It seems correct.

Here my thinking:

- Managed identity to Security group only.
- The security group can't be Dynamic or sync from OnPremise

- AD User Cloud can be added to Security and M365 groups
  - Not the dynamic (Group3) as it's using a query to get members
  - Not Group4 as it's synch from OnPrem
- upvoted 8 times

□ **EmnCours** Most Recent 4 months, 1 week ago

Group 2 only  
All company, Group 1 and Group 2 only  
upvoted 1 times

□ **dule27** 5 months ago

Group 2 only  
All company, Group 1 and Group 2 only  
upvoted 2 times

□ **dejo** 10 months ago

2) Cloud users CAN be added to the dynamic cloud security group (like Group3)! Also, I think that cloud users can be added to the security group synced from the on-prem, but only if the group writeback is enabled for that group. That user will be visible as a group member in the Azure AD, but won't be synced back to the on-prem AD group

Not tested but here is more info:

- <https://identity-man.eu/2022/07/05/using-the-new-group-writeback-functionality-in-azure-ad/>  
"Users which are 'cloud only' and are a member of the group are therefore not written back as member."

- <https://practical365.com/azure-ad-connect-group-writeback-deep-dive/>  
"If you add any Azure AD cloud-only identities, they will not show up in Active Directory and your group membership will not be consistent."  
upvoted 1 times

□ **Halwagy** 10 months, 2 weeks ago

The given answer is correct  
upvoted 2 times

□ **BRoald** 10 months, 2 weeks ago

second answer is correct, allcompany, group 1 & 2, im not sure about the first question. I looked up and i only can find something about security groups, but not about dynamic groups  
upvoted 2 times

□ **CheMetto** 4 months, 2 weeks ago

I follow this idea:

You can't add any members to any dynamic group manually! You have to change roles of the group to make it happen, so answer is no  
upvoted 1 times

You have an Azure AD tenant that contains two users named User1 and User2.

You plan to perform the following actions:

- Create a group named Group1.
- Add User1 and User2 to Group1.
- Assign Azure AD roles to Group1.

You need to create Group1.

Which two settings can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Group type: Microsoft 365 -  
Membership type: Assigned
- B. Group type: Security -  
Membership type: Assigned
- C. Group type: Security -  
Membership type: Dynamic User
- D. Group type: Microsoft 365 -  
Membership type: Dynamic User
- E. Group type: Security -  
Membership type: Dynamic Device

**Correct Answer: AB**

*Community vote distribution*

AB (100%)

 **haazybanj** 1 month, 1 week ago

**Selected Answer: AB**

- A. Group type: Microsoft 365 -  
Membership type: Assigned
  - B. Group type: Security -  
Membership type: Assigned
- upvoted 1 times

 **EmnCours** 4 months, 1 week ago

**Selected Answer: AB**

- A. Group type: Microsoft 365 -  
Membership type: Assigned
  - B. Group type: Security -  
Membership type: Assigned
- upvoted 1 times

 **dule27** 5 months, 1 week ago

**Selected Answer: AB**

- A. Group type: Microsoft 365 -  
Membership type: Assigned
  - B. Group type: Security -  
Membership type: Assigned
- upvoted 2 times

 **AArif098** 9 months, 3 weeks ago

**Selected Answer: AB**

Correct - Tested and when you select either M365 Group as Group type or Security, the default Assignment Type is "Assigned"

This can't be changed

upvoted 1 times

⊕  **BRoald** 10 months, 2 weeks ago

Correct, when you create a group you MUST enable "azure ad roles can be assigned to the group" (cannot be done afterwards). If you enable this feature when creating a group, dynamic groups are getting greyed out / disabled.

So yes, only assigned security and assigned m365 groups

upvoted 4 times

⊕  **Zak366** 9 months, 2 weeks ago

Just confirmed on my tenant

upvoted 1 times

## DRAG DROP

You have a Microsoft 365 E5 subscription.

You need to perform the following tasks:

- Identify the locations and IP addresses used by Azure AD users to sign in.
- Review the Azure AD security settings and identify improvement recommendations.
- Identify changes to Azure AD users or service principals.

What should you use for each task? To answer, drag the appropriate resources to the correct requirements. Each resource 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.

| Resources             | Answer Area                                                                     |
|-----------------------|---------------------------------------------------------------------------------|
| Audit logs            | Identify the locations and IP addresses used by Azure AD users to sign in:      |
| Identity secure score | Identify changes to Azure AD users or service principals:                       |
| Provisioning logs     | Review the Azure AD security settings and identify improvement recommendations: |
| Sign-in logs          |                                                                                 |

| Answer Area                                                                     |
|---------------------------------------------------------------------------------|
| Identify the locations and IP addresses used by Azure AD users to sign in:      |
| Identify changes to Azure AD users or service principals:                       |
| Review the Azure AD security settings and identify improvement recommendations: |

 **BRoald** Highly Voted 10 months, 2 weeks ago

Answers are correct!

upvoted 17 times

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

- Sign-in logs
- Audit logs
- Identity secure score

upvoted 1 times

 **dule27** 5 months, 1 week ago

- Sign-in logs
- Audit logs
- Identity secure score

upvoted 2 times

 **JN\_311** 5 months, 2 weeks ago

Agree with all the answers  
upvoted 1 times

 **bda92b3** 8 months, 4 weeks ago

Correct  
upvoted 1 times

## Case Study -

## Overview -

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

## Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | <i>None</i>                       |
| User2 | <i>None</i>                       |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner       | Members                        |
|-------------|----------|-----------------|-------------|--------------------------------|
| IT_Group1   | Security | Assigned        | <i>None</i> | All users in the IT department |
| AdatumUsers | Security | Assigned        | <i>None</i> | User1, User2                   |

## Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

## Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

## Requirements. Planned Changes -

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

## Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You need to implement the planned changes for Package1.

Which users can create and manage the access review?

- A. User3 only
- B. User4 only
- C. User5 only
- D. User3 and User4
- E. User3 and User5
- F. User4 and User5

**Correct Answer: E**

*Community vote distribution*

E (100%)

 **penatuna** 2 months, 3 weeks ago

**Selected Answer: E**

Requirements. Planned Changes:

Configure an access review for an access package named Package1.

Looking at the link below, only User3 & User5 can create and manage access reviews for access package named Package1.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/deploy-access-reviews#who-will-create-and-manage-access-reviews>  
upvoted 2 times

 **itismadu** 1 month, 1 week ago

Strongly agree with you.

Its User3 & User5

The administrative role required to create, manage, or read an access review depends on the type of resource being reviewed.

The type of resource is access Package. Hence user 3 and User 5 - <https://learn.microsoft.com/en-us/entra/id-governance/deploy-access-reviews#who-will-create-and-manage-access-reviews>

upvoted 1 times

⊕ **roman\_cat** 3 months, 1 week ago

Should be F. User 4 and 5. Least privilege access

upvoted 1 times

⊕ **marsot** 4 months, 2 weeks ago

**Selected Answer: E**

To create and perform an access review for users, you need to have one of the following roles:

- Global administrator
- User administrator
- Identity Governance Administrator
- Privileged Role Administrator (for reviews of role-assignable groups only)
- (Preview) Microsoft 365 or AAD Security Group owner of the group to be reviewed

<https://learn.microsoft.com/en-us/azure/active-directory/governance/manage-access-review#create-and-perform-an-access-review-for-users>

upvoted 2 times

⊕ **Ikazimirs** 4 months, 2 weeks ago

but user 4 is the user with Privileged Role Administrator role....

upvoted 4 times

⊕ **CheMetto** 4 months, 2 weeks ago

**Selected Answer: E**

First, you must be assigned one of the following roles:

- Global administrator  
User administrator  
Identity Governance Administrator  
Privileged Role Administrator (for reviews of role-assignable groups only)  
(Preview) Microsoft 365 or AAD Security Group owner of the group to be reviewed

<https://learn.microsoft.com/en-us/azure/active-directory/governance/manage-access-review>

upvoted 3 times

## Case Study -

## Overview -

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

## Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | <i>None</i>                       |
| User2 | <i>None</i>                       |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner       | Members                        |
|-------------|----------|-----------------|-------------|--------------------------------|
| IT_Group1   | Security | Assigned        | <i>None</i> | All users in the IT department |
| AdatumUsers | Security | Assigned        | <i>None</i> | User1, User2                   |

## Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

## Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

## Requirements. Planned Changes -

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

## Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You need to resolve the issue of the guest user invitations.

What should you do for the Azure AD tenant?

- A. Configure the Continuous access evaluation settings.
- B. Configure a Conditional Access policy.
- C. Modify the External collaboration settings.
- D. Configure the Access reviews settings.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: C**

C. Modify the External collaboration settings.  
upvoted 1 times

 **marsov** 4 months, 2 weeks ago

**Selected Answer: C**

Azure Portal > Azure AD > External identities > External collaboration settings > (Guest invite settings Section) check "Only users assigned to specific admin roles can invite guest users"  
upvoted 1 times

 **CheMetto** 4 months, 2 weeks ago

**Selected Answer: C**

Answer is correct. You can change the option of who can invite guest.  
upvoted 1 times



## Case Study -

## Overview -

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

## Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | <i>None</i>                       |
| User2 | <i>None</i>                       |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner       | Members                        |
|-------------|----------|-----------------|-------------|--------------------------------|
| IT_Group1   | Security | Assigned        | <i>None</i> | All users in the IT department |
| AdatumUsers | Security | Assigned        | <i>None</i> | User1, User2                   |

## Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

## Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

## Requirements. Planned Changes -

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

## Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You need to modify the settings of the User administrator role to meet the technical requirements.

Which two actions should you perform for the role? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Select Require justification on activation.
- B. Select Require ticket information on activation.
- C. Modify the Expire eligible assignments after setting.
- D. Set all assignments to Eligible.
- E. Set all assignments to Active.

**Correct Answer: CD**

Community vote distribution

CD (100%)

 **cgonIT** 1 month, 3 weeks ago

**Selected Answer: CD**

C. Modify the Expire eligible assignments after setting.

"Users assigned the User administrator role must be able to request permission to use the role when needed" It's the only way to "be able to request permission", making it Eligible. If it were "active", there won't be able to "ask for" anything.

D. Set all assignments to Eligible.

"up to one year." So there is needed to set an expiration date to be eligible and not active all time.

upvoted 1 times

 **Logitech** 2 months, 1 week ago

Where can i find the "Expire eligible assignments after setting." ?

upvoted 1 times

 **ServerBrain** 3 months ago

**Selected Answer: CD**

no debate on this answer

upvoted 1 times

 **Tanidanindo** 4 months, 1 week ago

**Selected Answer: CD**

correct

upvoted 3 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

You have a Microsoft 365 E5 subscription that contains a user named User1.

You need to ensure that User1 can create access reviews for Azure AD roles. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Privileged role administrator
- B. Identity Governance Administrator
- C. User administrator
- D. User Access Administrator

**Correct Answer: C**

*Community vote distribution*

|         |    |
|---------|----|
| A (94%) | 6% |
|---------|----|

kanag1 Highly Voted 4 months ago

**Selected Answer: A**

To create access reviews for Azure resources, you must be assigned to the Owner or the User Access Administrator role for the Azure resources. To create access reviews for Azure AD roles, you must be assigned to the Global Administrator or the Privileged Role Administrator role.

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-roles-and-resource-roles-review#prerequisites>

upvoted 7 times

haazybanj Most Recent 2 weeks, 3 days ago

**Selected Answer: A**

Access reviews: User Administrator (with the exception of access reviews of Azure or Microsoft Entra roles, which require Privileged Role Administrator). In this case, the Access review is for an Azure role which requires Privileged Role Administrator.

[https://learn.microsoft.com/en-us/entra/id-governance/identity-governance-overview?WT.mc\\_id=Portal-Microsoft\\_Azure\\_ELMAdmin#appendix-least-privileged-roles-for-managing-in-identity-governance-features](https://learn.microsoft.com/en-us/entra/id-governance/identity-governance-overview?WT.mc_id=Portal-Microsoft_Azure_ELMAdmin#appendix-least-privileged-roles-for-managing-in-identity-governance-features)

upvoted 1 times

Nyamnyam 3 weeks, 2 days ago

**Selected Answer: A**

Look at the table here <https://learn.microsoft.com/en-us/entra/id-governance/deploy-access-reviews#who-will-create-and-manage-access-reviews>

Specifically the row "Microsoft Entra roles"

upvoted 1 times

haazybanj 4 weeks, 1 day ago

**Selected Answer: B**

The correct answer is B. Identity Governance Administrator.

The Identity Governance Administrator role allows users to create and manage access reviews for Azure AD roles, as well as other identity governance features.

Privileged role administrator: This role allows users to manage all privileged roles in Azure AD. This is more permission than User1 needs, as they only need to be able to create access reviews for Azure AD roles.

upvoted 1 times

itismadu 1 month, 1 week ago

**Selected Answer: A**

In Microsoft 365 (M365), users with specific roles can create access reviews for Azure Active Directory (Azure AD) roles. Here are the roles that can perform this task:

Global Administrator: Global administrators have full access to all administrative features in Microsoft 365 and Azure AD, including the ability to create access reviews for Azure AD roles.

Security Administrator: Security administrators have permissions to manage security-related settings in Azure AD, and they can create access reviews for Azure AD roles.

Privileged Role Administrator: Privileged Role Administrators can manage assignments for privileged roles in Azure AD, including the ability to create access reviews for these roles.

upvoted 1 times

 **itismadu** 1 month, 1 week ago

Chatgpt Response  
upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

The correct answer is B. Identity Governance Administrator.

According to the web search results, the Identity Governance Administrator role can create and manage access reviews for Azure AD roles<sup>1</sup>. The Privileged role administrator role can only manage Azure AD roles, but not access reviews<sup>2</sup>. The User administrator and User Access Administrator roles do not have permissions to create or manage access reviews<sup>3</sup>.

upvoted 2 times

 **rikicm** 1 month, 3 weeks ago

**Selected Answer: A**  
Global administrators and Privileged Role administrators can create reviews on role-assignable groups  
upvoted 1 times

 **Reinhart68** 2 months ago

**Selected Answer: A**  
To create access reviews for Azure AD roles, you must be assigned to the Global Administrator or the Privileged Role Administrator role.  
upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: A**  
A. Privileged role administrator  
upvoted 2 times

 **FaizulHaque** 3 months, 4 weeks ago

Should be B - Identity Governance Administrator (principle of least privilege)  
upvoted 1 times

 **eternalenvy** 4 months ago

**Selected Answer: A**  
To create access reviews for Azure resources, you must be assigned to the Owner or the User Access Administrator role for the Azure resources.

To create access reviews for Azure AD roles, you must be assigned to the Global Administrator or the Privileged Role Administrator role.  
upvoted 2 times

 **eternalenvy** 4 months ago

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-roles-and-resource-roles-review?toc=%2Fazure%2Factive-directory%2Fgovernance%2Ftoc.json#prerequisites>  
upvoted 1 times

## HOTSPOT

You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3.

You have two Azure AD roles that have the Activation settings shown in the following table.

| Name  | Required justification on activation | Require approval to activate | Approvers |
|-------|--------------------------------------|------------------------------|-----------|
| Role1 | No                                   | Yes                          | User1     |
| Role2 | Yes                                  | No                           | None      |

The Azure AD roles have the Assignment settings shown in the following table.

| Role  | Allow permanent eligible assignment | Allow Permanent activate assignment | Require justification on active assignment |
|-------|-------------------------------------|-------------------------------------|--------------------------------------------|
| Role1 | Yes                                 | Yes                                 | Yes                                        |
| Role2 | No                                  | Yes                                 | Yes                                        |

The Azure AD roles have the eligible users shown in the following table.

| Role  | Eligible assignment |
|-------|---------------------|
| Role1 | User1, User2        |
| Role2 | User3               |

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 User1 requests Role1, the request will be approved automatically.        | <input type="radio"/> | <input type="radio"/> |
| User1 can approve the request of User3 for Role2.                           | <input type="radio"/> | <input type="radio"/> |
| User1 must provide justification to approve the request of User2 for Role1. | <input type="radio"/> | <input type="radio"/> |

### Answer Area

#### Correct Answer:

##### Statements

If User1 requests Role1, the request will be approved automatically.

Yes



No



User1 can approve the request of User3 for Role2.



User1 must provide justification to approve the request of User2 for Role1.



✉ **northgaterebel** Highly Voted 3 months, 3 weeks ago

N - Approvers cannot approve their own role activation requests (Topic 4 Question 34)

N - User1 is not an approver for Role2

N - Justification is not required for Role1

upvoted 8 times

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

N, N, Y. changed my mind. Require justification on active assignment is Yes for Role 1.

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings#require-justification-on-active-assignment>

upvoted 5 times

✉ **Logitech** 2 months, 1 week ago

1. NO - just, tested it. You cannot approve your own request, it is not even visible under "approve requests"

2. No of course.

3. Yes - can not approve without justification

upvoted 3 times

✉ **penatuna** 2 months, 2 weeks ago

I'm thinking N, N, N.

User2 is an eligible user for the Role1, and "Required justification on activation = NO".

I think that Role1 needs the justification only on active assignment.

upvoted 3 times

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

NNN.

Question 3 is "to approve the request of User2", who is in table 3 configured for "Eligible assignment". So when he triggers a request to activate the role for him, only "Require justification on activation" is evaluated. And it is set to "No" in table 1.

upvoted 1 times

✉ **SumitSahoo** 2 months ago

1. No - User 1 is not getting the request to approve. hence the request is always in a pending state. and unless approved, the role will not be added.

2. No - User1 is not an approver for Role2

3. Yes - User 1 needs to provide a justification while approving the requests.

upvoted 4 times

✉ **KrissB** 3 months, 3 weeks ago

I thought you can't self approve, so why would the User 1 request for Role one be automatically approved?

upvoted 2 times

**HOTSPOT**

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

| Name   | Role                            |
|--------|---------------------------------|
| Admin1 | Global Administrator            |
| Admin2 | Application Administrator       |
| Admin3 | Cloud Application Administrator |
| Admin4 | Application Developer           |
| User1  | None                            |

You plan to deploy an on-premises app named App1. App1 will be registered in Azure AD and will use Azure AD Application Proxy.

You need to delegate the installation of the Application Proxy connector and ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which user should perform the installation, and which role should you assign to User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User that should perform the installation:

- Admin1
- Admin2
- Admin3
- Admin4

Assign User1 the role of:

- Application Administrator
- Application Developer
- Cloud Application Administrator
- Global Administrator

**Correct Answer:****Answer Area**

User that should perform the installation:

- Admin1
- Admin2
- Admin3
- Admin4

Assign User1 the role of:

- Application Administrator
- Application Developer
- Cloud Application Administrator
- Global Administrator

 **Leacco99** Highly Voted 2 months, 1 week ago

Admin 2

Application Developer as per link below.

<https://learn.microsoft.com/en-us/azure/active-directory/develop/web-app-tutorial-01-register-application>

upvoted 7 times

 **haazybanj** Most Recent 3 weeks, 6 days ago

Admin 2

Application Dev

upvoted 1 times

 **JimboJones99** 1 month, 1 week ago

Admin 2 and Cloud Application Administrator

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-app-roles#assign-built-in-application-admin-roles>

upvoted 1 times

 **JimboJones99** 1 month, 1 week ago

I mean Application Administrator. Cloud Application Admin cannot manage application proxy.

upvoted 2 times

 **JustAGuyCramsForCerts** 1 month, 1 week ago

Guys, please stop messing up answers.

Answer ---> Admin 2 + Application Administrator <---

Application Developer has rights ONLY for registering an app;

Cloud Application Administrator has rights to register app and manage it in any ways (including removing etc.) but CAN'T set up App proxy!!!

The only answer is Application Administrator, which CAN set up App proxy and manage app in any way possible. And this is a least privilege after Global Admin.

upvoted 1 times

 **Haerenhal** 3 days, 8 hours ago

You are right. Global Admins and Application Administrators are the only two roles who can setup Application Proxy.

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

upvoted 1 times

 **JckD4Ni3L** 1 month, 1 week ago

You are wrong, Admin2 is an Application Administrator. However User1 has no roles, and the minimum role required to register an App is Application Developer.

See doc: <https://learn.microsoft.com/en-us/entra/identity-platform/web-app-tutorial-01-register-application#prerequisites>

upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

The answer is:

User who should perform the installation: User2

Role that should be assigned to User1: Application Administrator

upvoted 1 times

 **Leacco99** 2 months, 1 week ago

Admin 2

Application Dev

upvoted 4 times

 **penatuna** 2 months, 2 weeks ago

To my understanding, there are these two questions:

1) Create application proxy connectors

Global admin & Application admin can do this. Application admin is least privileged.

2) Register App1 in Azure AD.

Global admin, Application admin & Cloud application admin can do this. Cloud application admin is least privileged. It really depends if User1 needs the Application Proxy rights. I think that the question is pretty vague on that.

Please correct me, if I'm wrong.

upvoted 1 times

 **penatuna** 2 months ago

The second answer might be Application developer.

This MS Learn page says that you have to be at least a Cloud application administrator:

<https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

However, another MS Learn page says that Application developer is enough:

<https://learn.microsoft.com/en-us/azure/active-directory/develop/web-app-tutorial-01-register-application>

I think I will go with Application developer, cause it's least privileged.

upvoted 3 times

✉️ **Vince\_MCT** 3 months, 2 weeks ago

Admin 2 - App admin

Keyword is to use least of privileges. so definitely not admin1 as it was GA.

upvoted 2 times

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

Agreed. <https://learn.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application>

upvoted 1 times

✉️ **stai** 3 months, 2 weeks ago

Admin1, Application Administrator

Cloud Application Administrator can create and manage all aspects of app registrations and enterprise apps except App Proxy  
<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

upvoted 2 times

✉️ **Logitech** 2 months, 1 week ago

Application Dev can register Apps and has least privileges.

upvoted 2 times

✉️ **JustAGuyCramsForCerts** 1 month, 1 week ago

Read the question carefully, you should configure Application Proxy -> you need Application Administrator for it. App Dev has no rights to configure App Proxy

upvoted 1 times

## HOTSPOT

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

| Name  | Member of administrative unit          |
|-------|----------------------------------------|
| User1 | AU1                                    |
| User2 | AU1                                    |
| User3 | AU1                                    |
| User4 | AU2                                    |
| User5 | Not a member of an administrative unit |

The users are assigned the roles shown in the following table.

| User  | Role                   | Role scope     |
|-------|------------------------|----------------|
| User1 | Password Administrator | Organization   |
| User2 | Global Reader          | Organization   |
| User3 | None                   | Not applicable |
| User4 | Password Administrator | AU1            |
| User5 | None                   | Not applicable |

For which users can User1 and User4 reset passwords? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User 1:

- User3 only
- User2 and User5 only
- User3 and User5 only
- User2, User3, and User5 only
- User3, User4 and User5 only
- User2, User3, User4, and User5

User 4:

- User3 only
- User2 and User3 only
- User3 and User5 only
- User1, User2, and User3 only

## Answer Area

User 1:

User3 only  
User2 and User5 only  
User3 and User5 only  
User2, User3, and User5 only  
User3, User4 and User5 only  
**User2, User3, User4, and User5**

Correct Answer:

User 4:

User3 only  
User2 and User3 only  
User3 and User5 only  
**User1, User2, and User3 only**

 **haazybanj** 4 weeks, 1 day ago

Correct

upvoted 1 times

 **Leacco99** 2 months, 1 week ago

Correct.

Organization - everyone under the org  
AU1 - only those belonging to the said AU

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

Correct

User1 -> User2, User3, User4, User5

User4 -> User1, User2 & User3

upvoted 1 times

 **kanag1** 4 months ago

Correct

User1 -> User2, User3, User4, User5

User4 -> User1, User2 & User3

Can reset passwords for non-administrators and Password Administrators

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords>

upvoted 4 times

You have a Microsoft 365 E5 subscription that contains a user named User1. User is eligible for the Application administrator role.

User1 needs to configure a new connector group for an application proxy.

What should you use to activate the role for User1?

- A. the Microsoft Defender for Cloud Apps portal
- B. the Microsoft 365 admin center
- C. the Azure Active Directory admin center
- D. the Microsoft 365 Defender portal

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **Charlie33** 3 months, 3 weeks ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-activate-role>  
upvoted 2 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: C**

C. the Azure Active Directory admin center  
upvoted 2 times

You have an Azure subscription that contains a registered app named App1.

You need to review the sign-in activity for App1. The solution must meet the following requirements:

- Identify the number of failed sign-ins.
- Identify the success rate of sign-ins.
- Minimize administrative effort.

What should you use?

- A. Sign-in logs
- B. Access reviews
- C. Audit logs
- D. Usage & insights

**Correct Answer: A**

*Community vote distribution*

D (68%)      A (32%)

 **nils241** Highly Voted 4 months ago

**Selected Answer: D**

D: Usage & insights  
upvoted 6 times

 **kijken** Most Recent 5 days, 7 hours ago

D and A are solutions and D is less effort  
upvoted 1 times

 **haazybanj** 4 weeks, 1 day ago

**Selected Answer: D**

Usage & Insights is the best choice for reviewing the sign-in activity for App1 and identifying the number of failed sign-ins, the success rate of sign-ins, and minimizing administrative effort.  
upvoted 1 times

 **ACSC** 2 months ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins#microsoft-entra-usage-and-insights>  
upvoted 3 times

 **Janker** 2 months, 1 week ago

**Selected Answer: D**

D: All required info is in Usage & Insight  
upvoted 2 times

 **sherifhamed** 2 months, 1 week ago

**Selected Answer: A**

A. Sign-in logs

Azure Active Directory (Azure AD) sign-in logs provide information about user sign-ins and can be used to identify the number of failed sign-ins, the success rate of sign-ins, and other sign-in-related activities. Sign-in logs are a common source for monitoring and analyzing sign-in activity for registered apps like App1, and they provide the necessary information to meet the specified requirements while minimizing administrative effort.  
upvoted 1 times

 **Jzx** 2 months, 3 weeks ago

**Selected Answer: A**

A. Sign-in logs:

Sign-in logs in Azure Active Directory (Azure AD) provide detailed information about user sign-in activities, including successful and failed sign-ins. You can easily identify the number of failed sign-ins and calculate the success rate of sign-ins using the data in these logs. Additionally, sign-in logs are designed for this specific purpose, making them the most appropriate choice.  
upvoted 1 times

 **syougun200x** 2 months, 1 week ago

You can achieve the goal with Sign-in logs. But landing Usage and Insights, it already lists number of failure and success rate so you do not even have to set filtering.

upvoted 1 times

 **EmnCours** 3 months, 3 weeks ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-all-sign-ins>

upvoted 2 times

 **Harishvarshan** 3 months, 2 weeks ago

The article proves it's D, see the bottom of the page

upvoted 1 times

 **kalisprod** 3 months, 3 weeks ago

**Selected Answer: D**

I agree with D. Tested in own lab - Provides all the required information quickly without having to check through sign-in logs. Remember question states "minimize administrative effort".

upvoted 1 times

 **sehlohomoletsane** 3 months, 3 weeks ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-all-sign-ins>

upvoted 2 times

Your company has an Azure AD tenant that contains a user named User1.

The company has two departments named marketing and finance.

You need to grant permissions to User1 to manage only the users in the marketing department. The solution must ensure that User1 does NOT have permissions to manage the users in the finance department.

What should you create first?

- A. a management group
- B. an administrative unit
- C. a resource group
- D. a Microsoft 365 group

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉  **haazybanj** 4 weeks, 1 day ago

**Selected Answer: B**

Administrative Unit

upvoted 1 times

✉  **cgonIT** 1 month, 3 weeks ago

**Selected Answer: B**

Correct answer. B. an administrative unit.

"Administrative units restrict permissions in a role to any portion of your organization that you define. You could, for example, use administrative units to delegate the Helpdesk Administrator role to regional support specialists, so they can manage users only in the region that they support."

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

upvoted 1 times

✉  **EmnCours** 3 months, 3 weeks ago

**Selected Answer: B**

B. an administrative unit

upvoted 1 times

You have an Azure AD tenant that contains an access package named Package1 and a user named User1. Package1 is configured as shown in the following exhibit.

### Expiration

Access package assignments expire ⓘ

On date  Number of days  Number of hours (Preview)  Never

Assignments expire after (number of days)

365

[Show advanced expiration settings](#)

### Access Reviews

Require access reviews \* ⓘ

Yes  No

Starting on ⓘ

03/01/2022

Review frequency ⓘ

Annually  Bi-annually  Quarterly  Monthly  Weekly

Duration (in days) ⓘ

90

Maximum 175

Reviewers ⓘ

Self-review

Specific reviewer(s)

Manager

You need to ensure that User1 can modify the review frequency of Package1. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Security administrator
- B. Privileged role administrator
- C. External Identity Provider administrator
- D. User administrator

**Correct Answer: D**

*Community vote distribution*

D (90%) 10%

 penatuna Highly Voted 2 months, 2 weeks ago

**Selected Answer: D**

Tried this with all the suggested answer, and none of them can modify the review frequency of Package1. See explanation below.

Security Admin

- Cannot update Policy

Privileged role administrator

- Gets "No access" to Access Packages.

External Identity Provider administrator

- Gets "No access" to Access Packages.

User administrator

- Gets "No access" to Access Packages.

User administrator used to be the right choice for this question. However, things have now changed:

The User Administrator role is no longer allowed to manage catalogs and access packages in Azure AD Entitlement Management. Please transition to the Identity Governance Administrator role to continue managing access without disruption, or go to the Entitlement Management settings page if you need to temporarily opt out.

So, if there is an option in this question to choose Identity Governance Administrator, choose that.

[https://learn.microsoft.com/azure/active-directory/governance/identity-governance-overview?WT.mc\\_id=Portal-Microsoft\\_Azure\\_ELMAdmin#appendix---least-privileged-roles-for-managing-in-identity-governance-features](https://learn.microsoft.com/azure/active-directory/governance/identity-governance-overview?WT.mc_id=Portal-Microsoft_Azure_ELMAdmin#appendix---least-privileged-roles-for-managing-in-identity-governance-features)  
upvoted 6 times

 **Sorrynotsorry** Most Recent ⓘ 2 weeks, 3 days ago

**Selected Answer: B**

To create access reviews for Azure resources, you must be assigned to the Owner or the User Access Administrator role for the Azure resources. To create access reviews for Microsoft Entra roles, you must be assigned to the Global Administrator or the Privileged Role Administrator role.  
upvoted 1 times

 **Leacco99** 2 months, 1 week ago

Should be Identity Governance Admin if up to date, but if not present, choose User Administrator.

"The least privileged role for Entitlement management has changed from the User Administrator role to the Identity Governance Administrator role."

[https://learn.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview?WT.mc\\_id=Portal-Microsoft\\_Azure\\_ELMAdmin#appendix---least-privileged-roles-for-managing-in-identity-governance-features](https://learn.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview?WT.mc_id=Portal-Microsoft_Azure_ELMAdmin#appendix---least-privileged-roles-for-managing-in-identity-governance-features)  
upvoted 3 times

 **kanag1** 4 months ago

**Selected Answer: D**

o enable reviews of access packages, you must meet the prerequisites for creating an access package:

Microsoft Azure AD Premium P2 or Microsoft Entra ID Governance  
Global administrator, Identity Governance administrator, User administrator, Catalog owner, or Access package manager  
upvoted 3 times

 **JimboJones99** 1 month, 2 weeks ago

This has been superseded. See penatuna and Leacco99's comments above.

upvoted 1 times

**HOTSPOT**

You have an Azure subscription.

Azure AD logs are sent to a Log Analytics workspace.

You need to query the logs and graphically display the number of sign-ins per user.

How should you complete the query? To answer, select the appropriate options in the answer area,

NOTE: Each correct selection is worth one point.

**Answer Area**

```
SigninLogs
| where ResultType == 0
| login_count = count() by Identity
| extend
| print
| project
| render
| summarize
| columnchart
| extend
| print
| project
| render
| summarize
```

**Answer Area**

```
SigninLogs
| where ResultType == 0
| login_count = count() by Identity
| extend
| print
| project
| render
| summarize
| columnchart
| extend
| print
| project
| render
| summarize
```

Correct Answer:

AK\_1234 1 month, 3 weeks ago

- Summarize
- Render

upvoted 1 times

✉️  **nils241** 4 months ago

```
SigninLogs  
|where ResultType == 0  
|summarize login_count = count() by Identity  
|render columnchart
```

Test in my lab.

upvoted 4 times

✉️  **kanag1** 4 months ago

```
Correct  
SigninLogs  
| where ResultType == 0  
| summarize login_count = count() by Identity  
| render columnchart
```

upvoted 1 times

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

You need to identify which users access Facebook from their devices and browsers. The solution must minimize administrative effort.

What should you do first?

- A. Create a Conditional Access policy.
- B. Create a Defender for Cloud Apps access policy.
- C. Create an app configuration policy in Microsoft Endpoint Manager.
- D. From the Microsoft Defender for Cloud Apps portal, unsanction Facebook.

**Correct Answer: D**

*Community vote distribution*

D (67%)

B (33%)

MacDanorld 5 days, 16 hours ago

**Selected Answer: B**

How does unsanctioning an app which effectively block access to the app give you an insight to which users access it on their device? i dont see how D is the answer to this question. I believe creating a CLOUD APP ACCESS POLICY is what is needed.

Please correct me if i am wrong  
upvoted 2 times

Haerenhal 3 days, 7 hours ago

Yes B is the answer. Create a Defender for Cloud Apps access policy:

Creating a Defender for Cloud Apps access policy allows you to define conditions and settings to monitor and control access to specific cloud applications, such as Facebook. This approach helps you gain insights into user activities related to Facebook without immediately blocking or unsanctioning the application.

upvoted 1 times

ACSC 2 months ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/defender-cloud-apps/governance-discovery#sanctioningunsanctioning-an-app>  
upvoted 1 times

Logitech 2 months, 1 week ago

such a stupid question. First you can see it anyway dont need to unsanctioned the app. I can add a random Tag too.  
If you have MDE Integration, what you normal have if you are using CAS. Then you block unsancitoned apps automaticlly. If you enable network proteciton it will block it in all browser.

upvoted 1 times

sehlohomoletsane 3 months, 3 weeks ago

Answer is to create a conditional access policy

(You should create a Conditional Access policy. Conditional Access policies allow you to control access to cloud apps based on user, location, device, and app. You can create access policies for any device, including devices that aren't Hybrid Azure AD Join and not managed by Microsoft Intune, by rolling out client certificates to managed devices or using existing certificates, such as third-party MDM certificates. For example, you can deploy client certificates to managed devices and then block access from devices without a certificate. This solution minimizes administrative effort)

upvoted 1 times

OutLawTheBoyzz 3 months, 2 weeks ago

Read this... You can mark a specific risky app as unsanctioned by clicking the three dots at the end of the row. Then select Unsanctioned. Unsanctioning an app doesn't block use, but enables you to more easily monitor its use with the Cloud Discovery filters. You can then notify users of the unsanctioned app and suggest an alternative safe app for their use, or generate a block script using the Defender for Cloud Apps APIs to block all unsanctioned apps.

<https://learn.microsoft.com/en-us/defender-cloud-apps/governance-discovery>

upvoted 1 times

sehlohomoletsane 3 months, 3 weeks ago

apologies for the double word

upvoted 1 times

kanag1 4 months ago

**Selected Answer: D**

Unsanctioning an app doesn't block use, but enables you to more easily monitor its use with the Cloud Discovery filters. You can then notify users of the unsanctioned app and suggest an alternative safe app for their use, or generate a block script using the Defender for Cloud Apps APIs to block all unsanctioned apps.

<https://learn.microsoft.com/en-us/defender-cloud-apps/governance-discovery#sanctioningunsanctioning-an-app>

upvoted 3 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM).

You need to identify users that are eligible for the Cloud Application Administrator role.

Which blade in the Privileged Identity Management settings should you use?

- A. Azure resources
- B. Privileged access groups
- C. Review access
- D. Azure AD roles

**Correct Answer: B**

*Community vote distribution*

D (100%)

nils241 Highly Voted 4 months ago

**Selected Answer: D**

- A. Role does not fit
- B. Blade does not exist
- C. Makes sense only if an access review would exist
- D: Easiest way: Azure AD roles -> Assignments

Any other suggestions?

upvoted 7 times

haazybanj Most Recent 4 weeks, 1 day ago

**Selected Answer: D**

The Azure AD roles blade in the Privileged Identity Management settings allows you to manage Azure AD roles, including assigning roles to users and groups, and reviewing user and group eligibility for roles

upvoted 1 times

sherifhamed 2 months, 1 week ago

**Selected Answer: D**

To identify users eligible for the Cloud Application Administrator role using Azure AD Privileged Identity Management (PIM), you should use the "Azure AD roles" blade in the Privileged Identity Management settings (option D).

Here's how you can do it:

Go to the Azure portal (<https://portal.azure.com>).

In the left-hand navigation pane, navigate to "Azure Active Directory."

Under the "Security" section, select "Privileged Identity Management."

On the Privileged Identity Management dashboard, select "Azure AD roles."

In the list of roles, locate and select the "Cloud Application Administrator" role.

In the "Eligible" tab, you can view the list of users who are eligible for the Cloud Application Administrator role.

upvoted 1 times

EmnCours 3 months, 3 weeks ago

**Selected Answer: D**

- D. Azure AD roles
- upvoted 1 times

kalisprod 3 months, 3 weeks ago

**Selected Answer: D**

Agree with Nils241  
upvoted 1 times

## HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to create a dynamic user group that will include all the users that do NOT have a department defined in their user profile.

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.department

|        |        |
|--------|--------|
| -eq    | ""     |
| -match | null   |
| -ne    | \$null |
| -notIn | "null" |

**Answer Area**

(user.department

|               |             |
|---------------|-------------|
| -eq           | ""          |
| <b>-match</b> | <b>null</b> |
| -ne           | \$null      |
| -notIn        | "null"      |

Correct Answer:

kanag1 Highly Voted 4 months ago

Correct

(user.department -eq null)

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#use-of-null-values>  
upvoted 6 times

cgonIT Most Recent 1 month, 3 weeks ago

Answer is correct:

Box1: -eq  
Box2: null

Tested in lab.

upvoted 1 times

AK\_1234 1 month, 3 weeks ago

- eq  
- null  
upvoted 1 times

EmnCours 3 months, 3 weeks ago

Correct

(user.department -eq null)  
upvoted 1 times

You have an Azure AD Premium P2 tenant.

You create a Log Analytics workspace.

You need to ensure that you can view Azure AD audit log information by using Azure Monitor.

What should you do first?

- A. Modify the ~~Diagnostics~~ settings for Azure AD.
- B. Run the ~~Update-MgOrganization~~ cmdlet.
- C. Run the ~~Update-MgDomain~~ cmdlet.
- D. Create an Azure AD workbook.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **haazybanj** 4 weeks, 1 day ago

**Selected Answer: A**

The correct answer is A. Modify the Diagnostics settings for Azure AD.

To ensure that you can view Azure AD audit log information by using Azure Monitor, you must first modify the Diagnostics settings for Azure AD to enable streaming of those logs to Azure Monitor.

upvoted 1 times

 **cgonIT** 1 month, 3 weeks ago

**Selected Answer: A**

Think response is correct. A. Modify the Diagnostics settings for Azure AD.

upvoted 1 times

 **ACSC** 1 month, 4 weeks ago

**Selected Answer: A**

Correct answer

upvoted 1 times

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

You need to identify which users access Facebook from their devices and browsers. The solution must minimize administrative effort.

What should you do first?

- A. From the Microsoft 365 Defender portal, unsanction Facebook.
- B. Create a Defender for Cloud Apps access policy.
- C. Create an app configuration policy in Microsoft Intune.
- D. Create a Conditional Access policy.

**Correct Answer: A**

*Community vote distribution*

A (80%)      B (20%)

 **Sorrynotsorry** 2 weeks, 3 days ago

**Selected Answer: B**

Question didn't ask you to block Facebook, just check who is using it. This can be viewed from the discovered app list or create a policy to send notifications

upvoted 1 times

 **haazybanj** 4 weeks, 1 day ago

**Selected Answer: A**

The best answer is A. From the Microsoft 365 Defender portal, unsanction Facebook.

upvoted 1 times

 **JCkD4Ni3L** 1 month, 1 week ago

**Selected Answer: A**

To identify which users access Facebook from their devices and browsers with minimal administrative effort, you should first unsanction Facebook from the Microsoft 365 Defender portal<sup>1</sup>. By tagging apps in Cloud App Security as unsanctioned, those app domains are then pushed to Microsoft Defender ATP as custom network indicators in near real-time<sup>1</sup>. This is a single-click control that can significantly improve security posture and save time<sup>1</sup>. So, the correct answer is A. From the Microsoft 365 Defender portal, unsanction Facebook.

upvoted 1 times

 **shuhaidawahab** 1 month, 3 weeks ago

The correct answer is B. Create a Defender for Cloud Apps access policy.

According to the web search results, a Defender for Cloud Apps access policy is a rule that allows you to control and monitor the access to cloud apps from unmanaged devices or browsers<sup>1</sup>. You can use an access policy to identify which users access Facebook from their devices and browsers by creating a rule that matches the app name, the device type, and the browser type, and then applying an action such as Block, Allow, or Monitor<sup>2</sup>. You can also configure alerts and notifications for the access policy to get more visibility into the user activity<sup>3</sup>.

upvoted 2 times

 **ACSC** 1 month, 4 weeks ago

**Selected Answer: A**

Correct answer

upvoted 2 times

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

| Name  | Role                 |
|-------|----------------------|
| User1 | Global Administrator |
| User2 | User Administrator   |
| User3 | Groups Administrator |
| User4 | None                 |

From the tenant, you configure a naming policy for groups.

Which users are affected by the naming policy?

- A. User2 only
- B. User3only
- C. User2 and User3 only
- D. User3 and User4 only
- E. User1, User2, and User3 only
- F. User1, User2, User3, and User4

**Correct Answer: D**

*Community vote distribution*

D (83%)

B (17%)

 **haazybanj** 2 weeks, 6 days ago

**Selected Answer: D**

Admin override

Some administrators are exempted from these policies, across all group workloads and endpoints, so that they can create groups with these blocked words and with their desired naming conventions. The following are the list of administrator roles exempted from the group naming policy.

Global admin

Partner Tier 1 Support

Partner Tier 2 Support

User account admin

<https://learn.microsoft.com/en-us/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide#admin-override>

Some administrator roles are exempted from these policies, across all group workloads and endpoints, so that they can create groups using blocked words and with their own naming conventions. The following administrator roles are exempted from the group naming policy:

Global Administrator

User Administrator

<https://learn.microsoft.com/en-us/entra/identity/users/groups-naming-policy#roles-and-permissions>

upvoted 1 times

 **Nyamnyam** 3 weeks, 2 days ago

A comment on MSFT online documentation: It has 50% of passing/not-passing this exam.

Why? Because it is inconsistent.

<https://learn.microsoft.com/en-us/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide#admin-override>

Here it says:

roles exempted from the group naming policy.

Global admin

Partner Tier 1 Support

Partner Tier 2 Support

User account admin (sic!)

<https://learn.microsoft.com/en-us/entra/identity/users/groups-naming-policy#roles-and-permissions>

and here it says what you all have selected (D):

roles exempted from the group naming policy:

Global Administrator

User Administrator

Go get!

upvoted 1 times

✉ **JcKd4Ni3L** 1 month, 1 week ago

**Selected Answer: D**

When group naming policy is configured, the policy will be applied to new Microsoft 365 groups created by end users. Naming policy doesn't apply to certain directory roles, such as Global Administrator or User Administrator (please see below for the complete list of roles exempted from group naming policy). For existing Microsoft 365 groups, the policy won't immediately apply at the time of configuration. Once group owner edits the group name for these groups, naming policy will be enforced, even if no changes are made.

<https://learn.microsoft.com/en-us/entra/identity/users/groups-naming-policy#roles-and-permissions>

upvoted 2 times

✉ **itismadu** 1 month, 1 week ago

**Selected Answer: B**

I think it should be User 3 only

Some administrator roles are exempted from these policies, across all group workloads and endpoints, so that they can create groups using blocked words and with their own naming conventions. The following administrator roles are exempted from the group naming policy:

Global Administrator

User Administrator

<https://learn.microsoft.com/en-us/entra/identity/users/groups-naming-policy#roles-and-permissions>.

upvoted 1 times

✉ **ACSC** 1 month, 4 weeks ago

**Selected Answer: D**

Correct answer. Naming policy doesn't apply to certain directory roles, such as Global Administrator or User Administrator.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy#roles-and-permissions>.

upvoted 2 times

✉ **pUKer1990** 2 months ago

This should be 1 and 2 only, unless the exhibit has the groups positioned wrong. <https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy>

upvoted 2 times

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

| Name   | Role                     |
|--------|--------------------------|
| Admin1 | Account Administrator    |
| Admin2 | Service Administrator    |
| Admin3 | SharePoint Administrator |

You need to implement Azure AD Privileged Identity Management (PIM).

Which users can use PIM to activate their role permissions?

- A. Admin1 only
- B. Admin2 only
- C. Admin3 only
- D. Admin1 and Admin2 only
- E. Admin2 and Admin3 only
- F. Admin1, Admin2, and Admin3

**Correct Answer: A**

*Community vote distribution*

C (67%)

F (33%)

 **haazybanj** 2 weeks, 6 days ago

**Selected Answer: C**

Classic subscription administrator roles

You cannot manage the following classic subscription administrator roles in Privileged Identity Management:

Account Administrator  
Service Administrator  
Co-Administrator

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-roles>  
upvoted 2 times

 **OrangeSG** 3 weeks ago

**Selected Answer: F**

Azure AD Privileged Identity Management (PIM) allows users to activate their role permissions just-in-time. This means that users only have access to privileged roles when they need them, and for a limited amount of time.

To use PIM to activate their role permissions, users must be eligible for the role. Eligible users can be added to a role either directly, or by being added to a group that is assigned to the role.

In the table provided, all three users are assigned to privileged roles. Therefore, all three users are eligible to use PIM to activate their role permissions.

upvoted 1 times

 **fatilaura** 3 weeks ago

You cannot manage the following classic subscription administrator roles in Privileged Identity Management:

Account Administrator  
Service Administrator  
Co-Administrator  
upvoted 1 times

**HOTSPOT**

You have an Azure AD tenant.

You perform the tasks shown in the following table.

| Date     | Task                                                                                                                   |
|----------|------------------------------------------------------------------------------------------------------------------------|
| March 1  | Register four enterprise applications named App1, App2, App3, and App4.                                                |
| March 15 | From the tenant, update the following settings for App1: App roles, Users and groups, Client secret, and Self-service. |
| March 20 | From the tenant, update the following settings for App2: App roles, Users and groups, Client secret, and Self-service. |
| March 25 | From the tenant, update the following settings for App3: App roles, Users and groups, Client secret, and Self-service. |
| March 30 | From the tenant, update the following settings for App4: App roles, Users and groups, Client secret, and Self-service. |

On April 5, an administrator deletes App1, App2, App3, and App4.

You need to restore the apps and the settings.

Which apps can you restore on April 16, and which settings can you restore for App4 on April 16? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Apps:

- No apps
- App4 only
- App3 and App4 only
- App2, App3, and App4 only
- App1, App2, App3, and App4

App4 settings:

- No settings
- Self-service only
- App roles and Client secret only
- Users and groups and Self-service only
- App roles, Users and groups, Client secret, and Self-service

## Answer Area

Apps:

|                            |
|----------------------------|
| No apps                    |
| App4 only                  |
| App3 and App4 only         |
| App2, App3, and App4 only  |
| App1, App2, App3, and App4 |

Correct Answer:

App4 settings:

|                                                              |
|--------------------------------------------------------------|
| No settings                                                  |
| Self-service only                                            |
| App roles and Client secret only                             |
| Users and groups and Self-service only                       |
| App roles, Users and groups, Client secret, and Self-service |

曰  OrangeSG 3 weeks ago

After you delete an app registration, the app remains in a suspended state for 30 days. During that 30-day window, the app registration can be restored, along with all its properties.

Box 1: App1, App2, App3, and App4

Box 2: App roles, Users and groups, client secrets, and Self-service

<https://learn.microsoft.com/en-us/entra/identity-platform/howto-restore-app>

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 an Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.

You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the GitHub app connector.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **haazybanj** 4 weeks, 1 day ago

**Selected Answer: B**

No, the solution does not meet the goal.

Adding the GitHub app connector to Microsoft Defender for Cloud Apps will allow you to monitor OAuth authentication requests from GitHub to Microsoft 365. However, it will not allow you to monitor OAuth authentication requests to your AWS account, Google Workspace subscription, or Azure subscription.

upvoted 2 times

You have an Azure AD tenant.

You plan to implement Azure AD Privileged Identity Management (PIM).

Which roles can you manage by using PIM?

- A. Global Administrator only
- B. Global Administrator and Security Administrator only
- C. Global Administrator, Security Administrator, and Security Contributor only
- D. Account Administrator, Global Administrator, Security Administrator, and Security Contributor only

**Correct Answer: B**

*Community vote distribution*

C (100%)

✉ **haazybanj** 4 weeks, 1 day ago

You cannot manage the following classic subscription administrator roles in Privileged Identity Management:

Account Administrator  
Service Administrator  
Co-Administrator

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-roles>  
upvoted 2 times

✉ **haazybanj** 4 weeks, 1 day ago

**Selected Answer: C**

You cannot manage the following classic subscription administrator roles in Privileged Identity Management:

Account Administrator  
Service Administrator  
Co-Administrator  
upvoted 2 times

✉ **haazybanj** 4 weeks, 1 day ago

**Selected Answer: C**

The correct answer is C. Global Administrator, Security Administrator, and Security Contributor only.

Azure AD Privileged Identity Management (PIM) can be used to manage the following roles:

Global Administrator  
Security Administrator  
Security Contributor  
Account Administrator  
Privileged Role Administrator  
Identity Governance Administrator  
Other roles, such as User Administrator and Application Administrator, cannot be managed by using PIM.  
upvoted 2 times

**Topic 5 - Testlet 1**

## Introductory Info

Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named **Contoso\_Resources**. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

#### Question

You need to allocate licenses to the new users from ADatum. The solution must meet the technical requirements.

Which type of object should you create?

- A. a Dynamic User security group
- B. a distribution group
- C. an OU
- D. an administrative unit

#### Correct Answer: D

An administrative unit is an Azure AD resource that can be a container for other Azure AD resources. An administrative unit can contain only users, groups, or devices.

Administrative units restrict permissions in a role to any portion of your organization that you define.

Deployment scenario -

It can be useful to restrict administrative scope by using administrative units in organizations that are made up of independent divisions of any kind. Consider the example of a large university that's made up of many autonomous schools (School of Business, School of Engineering, and so on). Each school has a team of IT admins who control access, manage users, and set policies for their school.

Scenario: Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named

Adatum. The users will be located in London and Seattle.

Contoso identifies the following technical requirements: License allocation for new users must be assigned automatically based on the location of the user.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units>

*Community vote distribution*

A (100%)

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

A is the correct answer.

In the exam today

upvoted 11 times

 **JimmyPhelan** Highly Voted 1 year, 2 months ago

You cannot assign licenses to an Administrative Unit, only a Group, see here <https://learn.microsoft.com/en-us/answers/questions/955831/can-licenses-be-directly-assigned-to-an-administra.html>

A must be the correct answer

upvoted 7 times

 **haazybanj** Most Recent 4 weeks, 1 day ago

**Selected Answer: A**

A is the correct answer.

upvoted 1 times

 **ACSC** 1 month, 4 weeks ago

**Selected Answer: A**

Dynamic User security group  
upvoted 1 times

EmnCours 3 months, 3 weeks ago

**Selected Answer: A**

A. a Dynamic User security group  
upvoted 1 times

dule27 5 months ago

**Selected Answer: A**

A. a Dynamic User security group  
upvoted 1 times

ysm 10 months ago

Dynamic group with a query based on location  
upvoted 3 times

nshm90 11 months, 1 week ago

Seem like need AU and Dynamic group

AU to manage by location

Dynamic group to simplify license allocation and assigned automatically  
upvoted 1 times

nshm90 11 months, 1 week ago

Refer to technical requirement

" license allocation for new users MUST be assigned automatically based on the location of the user"

If AU, admin need to manually assign license to user within that AU only or assign another License Admin.

To meet the automatically assigned license requirements, we need to assign license to dynamic group  
upvoted 2 times

purek77 11 months, 1 week ago

I would say D - <https://learn.microsoft.com/en-us/azure/active-directory/roles/admin-units-assign-roles#roles-that-can-be-assigned-with-administrative-unit-scope>

Basically create AU, add group(s) and scope License Administrator.

upvoted 1 times

Jayeke 11 months, 1 week ago

license assignment needs to be done automatically, based on location. that can be accomplished by using dynamic groups. my vote is A  
upvoted 1 times

jack987 11 months, 1 week ago

**Selected Answer: A**

The correct answer is A.

upvoted 1 times

hastobedone2021 1 year, 1 month ago

"The helpdesk administrators must be able to manage licenses for ONLY the users in their respective office". How is the accomplished without creating an Admin Unit? From there you can create a dynamic group within the AU to take care of the group based licensing right?  
upvoted 3 times

Swarupam 1 year, 1 month ago

**Selected Answer: A**

License allocation for new users must be assigned automatically based on the location of the user."  
upvoted 1 times

ndawg07 1 year, 3 months ago

**Selected Answer: A**

A is correct  
upvoted 2 times

AStark1080 1 year, 3 months ago

**Selected Answer: A**

I would think the correct Answer would be A. Prompt states "License allocation for new users must be assigned automatically based on the location of the user." This would indicate a Dynamic Group with the Attribute of location to determine a License.  
upvoted 5 times

## Introductory Info

Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named **Contoso\_Resources**. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

#### Question

You need to sync the ADatum users. The solution must meet the technical requirements.

What should you do?

- A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.
- B. From PowerShell, run Set-ADSyncScheduler.
- C. From PowerShell, run Start-ADSyncSyncCycle.
- D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

#### Correct Answer: A

You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

*Community vote distribution*

A (100%)

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

A is the correct answer

In the exam today

upvoted 6 times

 **Teplah** 1 year, 1 month ago

I still do not understand why I can't use the PS cmdlet to just run the sync. After all, the OU is stacked up with the users and by default, all users/devices will be synced unless selection is made to select a particular OU. Did I miss something in the "requirement" part? Please help me understand this...

upvoted 1 times

 **TerraXplorer** 1 year, 1 month ago

You assume that the Synchronized Groups are already set, then the command for synchronizing makes sense. However, if the users are not synced before, this must first be configured via the AD Connect. You can restart the synchronization with the PowerShell command (the third one), but this will not change anything.

upvoted 3 times

 **Jhill777** 1 year ago

It says: Only the Contoso\_Resources OU is synced.

upvoted 4 times

 **VeIN** Highly Voted  11 months, 1 week ago

**Selected Answer: A**

A is correct

- Only Contoso\_Resources OU is synced (if you run PS command it will sync only this OU)
- You need to also sync new OU Adatum in Contonso AD where new users were created

To do it you need to run AAD Connect , open "customize synchronization options" and add Adatum OU.

All necessary details can be found here:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-installation-wizard#customize-synchronization-options>

upvoted 5 times

 **haazybanj** Most Recent  4 weeks, 1 day ago

**Selected Answer: A**

A is the correct answer  
upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: A**

A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.  
upvoted 1 times

 **purek77** 11 months, 1 week ago

**Selected Answer: A**

You have to add new OU to sync scope.  
upvoted 1 times

 **ACSC** 1 year ago

**Selected Answer: A**

Given explanation is correct  
upvoted 1 times

## Introductory Info

Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named **Contoso\_Resources**. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to https://contoso.com/auth-response.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

#### Question

HOTSPOT -

You need to meet the technical requirements for license management by the helpdesk administrators.

What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer Area

Object to create for each branch office:

|                               |
|-------------------------------|
| An administrative unit        |
| A custom role                 |
| A Dynamic User security group |
| An OU                         |

Tool to use:

|                                                |
|------------------------------------------------|
| Azure Active Directory admin center            |
| Active Directory Administrative Center         |
| Active Directory module for Windows PowerShell |
| Microsoft 365 admin center                     |

#### Answer Area

Object to create for each branch office:

|                               |
|-------------------------------|
| An administrative unit        |
| A custom role                 |
| A Dynamic User security group |
| An OU                         |

Correct Answer:

Tool to use:

|                                                |
|------------------------------------------------|
| Azure Active Directory admin center            |
| Active Directory Administrative Center         |
| Active Directory module for Windows PowerShell |
| Microsoft 365 admin center                     |

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units> <https://docs.microsoft.com/en-us/azure/active-directory/roles/admin-units-manage>

 **dule27** 5 months ago

An Administrative Units  
Azure AD Admin Center  
upvoted 2 times

 **b233f0a** 5 months, 1 week ago

Question says to meet the Technical requirements, which are "License allocation for new users must be assigned automatically based on the location of the user." Therefore answer is Dynamic Security group (Admin unit cannot be used to assign license based on location).

This is completed in the Azure AD Admin Centre

upvoted 4 times

□ **CheMetto** 4 months, 2 weeks ago

i think you miss "The helpdesk administrators must be able to manage licenses for only the users in their respective office.". The question ask how to satisfy technical requirements for the helpdesk administrator, not the license assignment generally. So that's why given answer are correct

upvoted 5 times

□ **Paul\_white** 3 months ago

CheMetto is right, read further down the technical requirements

"The helpdesk administrators must be able to manage licenses for only the users in their respective office."

upvoted 2 times

□ **Zak366** 9 months, 2 weeks ago

Given answer is correct.

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

"Administrative units restrict permissions in a role to any portion of your organization that you define. You could, for example, use administrative units to delegate the Helpdesk Administrator role to regional support specialists, so they can manage users only in the region that they support."

upvoted 3 times

□ **Mriji** 1 year, 1 month ago

I think key is the statement "What should you create first", this makes the answer correct.

upvoted 1 times

□ **JakeLi** 1 year, 1 month ago

The administrative units is designed for role management rather than license management. Hence, the correct answer for Q1 is A Dynamic User Security Group.

Refer to the article below.

<https://learn.microsoft.com/en-us/answers/questions/955831/can-licenses-be-directly-assigned-to-an-administra.html>

upvoted 3 times

□ **Jhill777** 1 year ago

You're missing the part about "The helpdesk administrators must be able to manage licenses for only the users in their respective office" and only looking at the the "assign licenses automatically". Answer is correct. Need and Administrative Unit to limit them to the users in their respective office.

upvoted 4 times

□ **DeepMoon** 1 year, 2 months ago

The given Answer is correct.

Q1: Administrative Units. This would limit the scope of admins as required.

Q2: AAD Admin Center (not the on-prem Active Directory Administrative Center)

upvoted 4 times

□ **existingname** 1 year, 3 months ago

correct

In the exam today

upvoted 4 times

## Introductory Info

Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named **Contoso\_Resources**. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

#### Question

You need to resolve the issue of the sales department users.

What should you configure for the Azure AD tenant?

- A. the Device settings
- B. the Access reviews settings
- C. the User settings
- D. Security defaults

#### Correct Answer: C

Scenario: There are Sales department users in London and in Seattle.

\* The users in the London office have the Microsoft 365 Phone System license unassigned.

\* The users in the Seattle office have the Yammer Enterprise license unassigned.

Use the Active users page to unassign licenses.

When you use the Active users page to unassign licenses, you unassign product licenses from users.

Unassign licenses from one user.

1. In the admin center, go to the Users > Active users page.
2. Select the row of the user that you want to unassign a license for.
3. In the right pane, select Licenses and Apps.
4. Expand the Licenses section, clear the boxes for the licenses that you want to unassign, then select Save changes.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/admin/manage/remove-licenses-from-users>

#### Community vote distribution

B (73%)      C (18%)      9%

 **Kawinho** Highly Voted 1 year, 2 months ago

I dont see any mention of the sale department in the case study...

upvoted 18 times

 **DeepMoon** Highly Voted 1 year, 2 months ago

Given Answer is Correct.

I don't see any mention of the sale department in the case study...But it seems they mean Marketing department mentioned here.

As I understand from the following:

Contoso plans to implement the following changes: -

Collaborate with the users at Fabrikam on a joint marketing campaign.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso identifies the following technical requirements: -

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

upvoted 6 times

 **DeepMoon** 1 year, 2 months ago

Never mind, ignore my previous conclusion. The given answer is wrong.

I meant to say B (Access Review)

upvoted 6 times

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

**Selected Answer: A**

Hi, my dearest. Don't waste your time, because the question belongs to another Case Study (the one about Litware from Vancouver).

In essence, the issue was:

Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD.

And here a reference for the obvious choice A:

<https://learn.microsoft.com/en-us/entra/identity/devices/manage-device-identities#configure-device-settings>

upvoted 1 times

 **ACSC** 1 month, 4 weeks ago

**Selected Answer: C**

User settings

upvoted 2 times

 **dule27** 5 months ago

**Selected Answer: B**

B. the Access reviews settings

upvoted 2 times

 **Sango** 5 months ago

The described Sales issue is: "The users in the London office have the Microsoft 365 Phone System license unassigned. The users in the Seattle office have the Yammer Enterprise license unassigned." The only answer that addresses fixing the "issue," i.e. assigning the license is A. User Settings > Assign the License.

upvoted 2 times

 **CheMetto** 4 months, 2 weeks ago

don't force it. You don't know why they do not have those license, maybe they do not need them? Who knows? I think it's related to marketing department the question, so the answer is access review. ( as you can see, there is no marketing department in contoso however is mentioned more times )

upvoted 1 times

 **Sango** 5 months ago

Sorry, C, not A.

upvoted 1 times

 **ExamStudy68** 7 months, 3 weeks ago

The question itself is completely confusing. I hope it isn't on the exam. If anyone sees it can you post it please

upvoted 1 times

 **LeTrinh** 9 months, 2 weeks ago

The users in the Seattle office have the Yammer Enterprise license unassigned.

So it would be to adjust the license for the Sale users in Seattle by using C.

The answer B is wrong because the access review is the planned review of the access needs, rights, and history of user access.

upvoted 1 times

 **AArif098** 9 months, 3 weeks ago

**Selected Answer: B**

voting for B, Access Reviews setting around the users having access to marketing department SP site.

upvoted 2 times

 **AMDF** 11 months, 4 weeks ago

**Selected Answer: B**

Voting for B

upvoted 1 times

 **ACSC** 1 year ago

**Selected Answer: B**

Access Review: Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days

upvoted 2 times

 **ACSC** 1 month, 4 weeks ago

Forget above. The answer is correct: C - User settings. It is about assigning licenses.

upvoted 1 times

 **Hot\_156** 1 year, 2 months ago

**Selected Answer: B**

This is what I understand here for this...

Contoso plans to implement the following changes:

- Collaborate with the users at Fabrikam on a joint marketing campaign.

Contoso identifies the following technical requirements:

- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Solution should be

- "D" The Access review settings.

Do any of you see something different? If so, can you elaborate and not just say the answer is "X"  
upvoted 1 times

✉ **geobarou** 1 year, 2 months ago

Fabricam collaborates for marketing campaign. It has nothing to do with Sales dpt. I think the answer is correct.  
upvoted 3 times

✉ **Hot\_156** 1 year, 2 months ago

If so, what are you supposed to change from "User Settings"? Also, the explanation given for that the selected answer is for changing this from office.com and the question asks "What would you change in AzureAD?"  
upvoted 1 times

✉ **geobarou** 1 year, 2 months ago

From User settings you may assign a license. I know it's not what we will do in a real scenario, but from the given answers it makes sense.  
But definitely Fabricam has nothing to do with sales dpt.

upvoted 3 times

✉ **dejo** 1 year, 1 month ago

No you can not assign licenses, User settings are related to consents, app registrations, guest user invite settings and guest access  
upvoted 3 times

## Topic 6 - Testlet 2

## Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

#### Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

### Question

HOTSPOT -

You need to configure the assignment of Azure AD licenses to the Litware users. The solution must meet the licensing requirements.

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

NOTE: Each correct selection is worth one point.

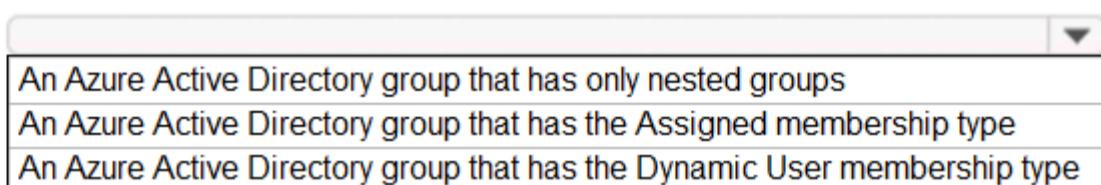
Hot Area:

#### Answer Area

Azure AD Connect settings to modify:



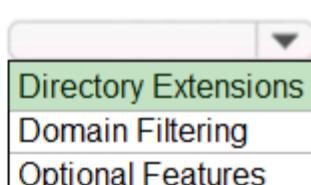
Assign Azure AD licenses to:



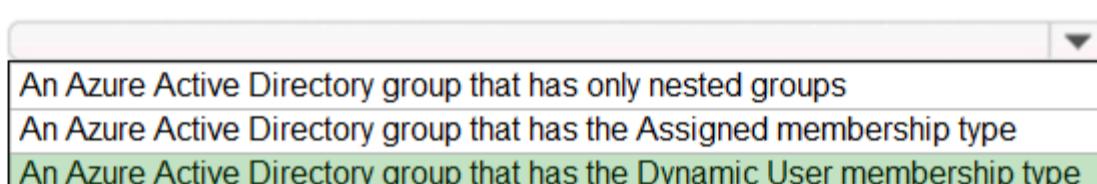
### Correct Answer:

#### Answer Area

Azure AD Connect settings to modify:



Assign Azure AD licenses to:



Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

✉️ patriline Highly Voted 2 years, 6 months ago

This is correct. <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-feature-directory-extensions>  
upvoted 16 times

✉️ melatocaroca 2 years, 5 months ago

You can use directory extensions to extend the schema in Azure Active Directory (Azure AD) with your own attributes from on-premises Active Directory. This feature enables you to build LOB apps by consuming attributes that you continue to manage on-premises. These attributes can be consumed through extensions.

upvoted 8 times

✉️ cgonIT Most Recent 1 month, 2 weeks ago

- Directory Extensions  
- An Azure Active Directory group that has the Dynamic User membership type  
upvoted 1 times

✉️ dule27 5 months ago

Directory Extensions

Azure AD Group that has the Dynamic user membership type

upvoted 1 times

 **Teplah** 1 year, 1 month ago

Answer correct!

upvoted 1 times

 **DeepMoon** 1 year, 2 months ago

The given Answers are correct.

Q1: Directory Extensions

You can use directory extensions to extend the schema in Azure Active Directory (Azure AD) with your own attributes from on-premises Active Directory. <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-feature-directory-extensions>

Q2: And AAD Group that has Dynamic User Membership Type

Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned

upvoted 3 times

 **azjimpang** 1 year, 5 months ago

TR: Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

A1: Directory Extensions

A2: Azure AD Group with Dynamic user membership

\*<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-feature-directory-extensions>\*

upvoted 4 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 2 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 3 times

 **BaderJ** 2 years, 2 months ago

Passed the exam today 23/09/2021

This question came in the exam.

upvoted 2 times

## Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

#### Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

### Question

You need to meet the authentication requirements for leaked credentials.

What should you do?

- A. Enable password hash synchronization in Azure AD Connect.
- B. Configure Azure AD Password Protection.
- C. Configure an authentication method policy in Azure AD.
- D. Enable federation with PingFederate in Azure AD Connect.

#### Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity>

Community vote distribution

A (100%)

Val\_0 Highly Voted 2 years, 6 months ago

@spinnetho - the correct answer is A - <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#common-questions>

upvoted 25 times

Hot\_156 Highly Voted 1 year, 2 months ago

Selected Answer: A

The question is Tricky! it mentions "meet authentication requirements" and if you just read this and go back up to read the "Authentication Requirements" there is nothing that mentioned anything related to needing PHS. HOWEVER!!!!!! If you read the whole question again "You need to meet the authentication requirements FOR LEAKED CREDENTIALS", you realize there is nothing that mentioned LEAKED CREDENTIALS on the "Authentications Requirements" related to it.

The answer is A because none of the other ones has anything to do with LEAKED CREDENTIALS.

You don't use B for anything related to LEAKED CREDENTIALS - You would use this one for addressing the requirement

You don't use C for anything related to LEAKED CREDENTIALS

You don't use D for anything related to LEAKED CREDENTIALS

I had to read this multiple times!!! LOL

upvoted 7 times

AK\_1234 Most Recent 1 month, 4 weeks ago

Catch is " leaked credentials" . B is correct.

upvoted 2 times

Nyamnyam 3 weeks, 2 days ago

I also thought initially that Password Protection should be correct, based on its global banned password. But in the online documentation, MSFT notes: The global banned password list isn't based on any third-party data sources, including compromised password lists. So, yes, after all, MSFT obviously uses another trick in Entra ID Protection (P1 and P2) to "Detect risks" such as "Leaked credentials". But for this it needs the data, and this can only be the password hashes, or hashes of hashes, as they say, but who knows exactly ;)  
<https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection#detect-risks>

upvoted 1 times

dule27 5 months ago

Selected Answer: A

A. Enable password hash synchronization in Azure AD Connect.

upvoted 1 times

DeepMoon 1 year, 2 months ago

The Users with leaked credentials report in Azure AD warns of username and password pairs, which have been exposed publically. An incredible volume of passwords is leaked via phishing, malware, and password reuse on third-party sites that are later breached. Microsoft finds many of these leaked credentials and will tell you, in this report, if they match credentials in your organization – but only if you enable password hash sync

or have cloud-only identities.

<https://learn.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity#protect-against-leaked-credentials-and-add-resilience-against-outages>  
upvoted 2 times

□ **Efficia** 1 year, 5 months ago

**Selected Answer: A**

Password hash synchronization

"Risk detections like leaked credentials require the presence of password hashes for detection to occur. For more information about password hash synchronization, see the article, Implement password hash synchronization with Azure AD Connect sync."

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#password-hash-synchronization>  
upvoted 4 times

□ **sapien45** 1 year, 5 months ago

>Password Hash Sync also enables leaked credential detection for your hybrid accounts. Microsoft works alongside dark web researchers and law enforcement agencies to find publicly available username/password pairs. If any of these pairs match those of our users, the associated account is moved to high risk.

upvoted 1 times

□ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 3 times

□ **WS\_21** 1 year, 8 months ago

**Selected Answer: A**

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#leaked-credentials>  
upvoted 1 times

□ **stromnessian** 1 year, 9 months ago

**Selected Answer: A**

It's A. Everyone knows that leaked credentials detection comes with PHS, right? Not sure why all the debate. Next question...

upvoted 5 times

□ **andersonlrlima** 1 year, 10 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises#design-principles>  
The software isn't dependent on other Azure AD features. For example, Azure AD password hash sync (PHS) isn't related or required for Azure AD Password Protection.

upvoted 2 times

□ **Jdburner** 1 year, 11 months ago

This clearly states that PSH isn't required

<https://docs.microsoft.com/en-us/learn/modules/manage-user-authentication/5-deploy-manage-password-protection>

upvoted 1 times

□ **007Ali** 1 year, 10 months ago

PHS is not required for "Password Protection" which enables the use of a "Custom Banned Password List" on prem. To protect against the requirement of "Leaked Passwords" an Identity Protection / User Risk Policy is required and that requires passwords in Azure AD, therefore PHS is required.

upvoted 5 times

□ **girikedar** 1 year, 12 months ago

Azure ad password protection is configured when there is requirement of including Banned password. how can anyone configure leaked credential in banned password section so the answer should be Password Hash Synchronization. as a same time if there was no password hash synchronization option in answer section the it should be answer D

upvoted 2 times

□ **girikedar** 1 year, 12 months ago

i think answer should be A because without password hash synchronization password protection cannot be implemented for the on-premises users.

upvoted 1 times

□ **melatocaroca** 2 years, 4 months ago

July16, update,

Enable password hash synchronization in Azure AD Connect. (new answer) not longer in this question new one an valid response

A. Configure an authentication method policy in Azure AD.

You can configure AuthenticationMethods policy

[https://portal.azure.com/#blade/Microsoft\\_AAD\\_IAM/AuthenticationMethodsMenuBlade/AdminAuthMethods](https://portal.azure.com/#blade/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/AdminAuthMethods)  
upvoted 2 times

□ **melatocaroca** 2 years, 4 months ago

Password hash synchronization

Risk detections like leaked credentials require the presence of password hashes for detection to occur.

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#common-questions>

#### User risk policy

Identity Protection can calculate what it believes is normal for a user's behavior and use that to base decisions for their risk.

- User risk is a calculation of probability that an identity has been compromised.
- Administrators can plan based on this risk score signal to enforce organizational requirements.
- Administrators can choose to block access, allow access, or allow access but require a password change using Azure AD self-service password reset.

upvoted 2 times

 **melatocaroca** 2 years, 4 months ago

Requirements. Authentication Requirements, need to Implement a banned password list for the litware.com forest. So for this you need to Configure Azure AD Password Protection, so IMHO answer must be B

upvoted 1 times

 **melatocaroca** 2 years, 5 months ago

The answer is correct In the event of an on-premises outage (for example, in a ransomware attack) you can switch over to using cloud authentication using password hash sync.

From reference link

upvoted 1 times

## Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

#### Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

### Question

HOTSPOT -

You need to identify which roles to use for managing role assignments. The solution must meet the delegation requirements.

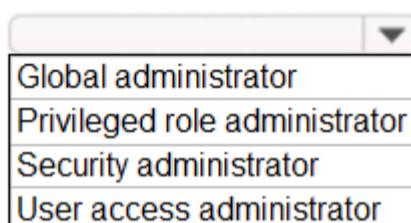
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

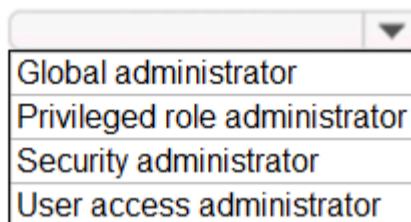
Hot Area:

#### Answer Area

To manage Azure AD built-in role assignments, use:

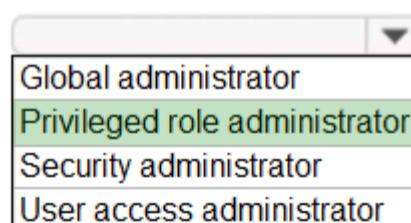


To manage Azure built-in role assignments, use:



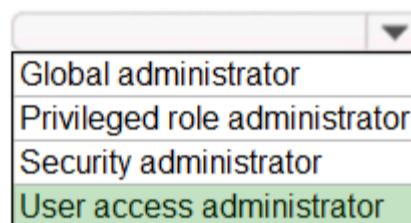
#### Answer Area

To manage Azure AD built-in role assignments, use:



Correct Answer:

To manage Azure built-in role assignments, use:



Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal> <https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

✉️ **sapien45** Highly Voted 1 year, 5 months ago

For Azure AD roles in Privileged Identity Management, only a user who is in the Privileged Role Administrator or Global Administrator role can manage assignments for other administrators. Global Administrators, Security Administrators, Global Readers, and Security Readers can also view assignments to Azure AD roles in Privileged Identity Management.

For Azure resource roles in Privileged Identity Management, only a subscription administrator, a resource Owner, or a resource User Access administrator can manage assignments for other administrators. Users who are Privileged Role Administrators, Security Administrators, or Security Readers do not by default have access to view assignments to Azure resource roles in Privileged Identity Management.

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

upvoted 12 times

✉️ **jack987** 11 months, 1 week ago

This is very too to explain the answer. Thanks!

upvoted 1 times

✉️ **jack987** 11 months, 1 week ago

This is very good\* to explain the answer. Thanks!

upvoted 1 times

leeuw86 [Highly Voted] 2 years, 6 months ago

that's correct

upvoted 6 times

dule27 [Most Recent] 5 months ago

Azure AD build-in role: Privileged role Administrator

Azure build-in role: User Access Administrator

upvoted 1 times

Nonyabuz 1 year, 2 months ago

Step 4. Check your prerequisites

To assign roles, you must be signed in with a user that is assigned a role that has role assignments write permission, such as Owner or \*\*\*User Access Administrator\*\*\* at the scope you are trying to assign the role. Similarly, to remove a role assignment, you must have the role assignments delete permission.

Microsoft.Authorization/roleAssignments/write

Microsoft.Authorization/roleAssignments/delete

If your user account doesn't have permission to assign a role within your subscription, you see an error message that your account "does not have authorization to perform action 'Microsoft.Authorization/roleAssignments/write'." In this case, contact the administrators of your subscription as they can assign the permissions on your behalf.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps>

upvoted 1 times

RandomNickname 1 year, 5 months ago

Given answer is correct.

For Azure AD role see;

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

And the subsequent link for;

<https://docs.microsoft.com/en-us/azure/active-directory/roles/manage-roles-portal>

For Azure built-in role see;

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

And the subsequent link for;

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps>

upvoted 2 times

Jun143 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 2 times

TheGuy 1 year, 8 months ago

Second question is referring to Azure built-in roles and NOT Azure AD built-in roles, hence user access administrator

Azure Roles: <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

Azure AD Roles: <https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

upvoted 3 times

Bulldozer 1 year, 8 months ago

Since the user access administrator role does not exist. For me, it is the Privileged Administrator role that should be selected for both answers.

upvoted 2 times

chikorita 8 months, 1 week ago

Azure AD: User Administrator

Azure RBAC: User Access Administrator

upvoted 1 times

Paimon 1 year, 8 months ago

It does exist for Azure.....not Azure AD. But it can't manage Azure roles - only access to resources. So you still got the correct answer. Global admin can also do both.

upvoted 2 times

Paimon 1 year, 8 months ago

.....but PIM is the requirement, so privileged admin role is correct.

upvoted 1 times

Pravda 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

 **melatocaroca** 2 years, 4 months ago

Requirements. Delegation Requirements

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom catalogs and custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege. (To assign Azure roles, you must have User Access Administrator or Owner)

For Azure AD roles in Privileged Identity Management, only a user who is following roles

- Privileged Role Administrator

o or

- Global Administrator

can manage assignments for other administrators

For Azure AD roles in Privileged Identity Management view assignments only a user who is following roles.

- Global Administrators,

- Security Administrators,

- Global Readers:

- Security Readers

User administrator

Create and manage all aspects of users and groups, manage support tickets, monitor service health, Change passwords for users, Helpdesk administrators, and other User Administrators

upvoted 2 times

## Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

### Question

HOTSPOT -

You need to create the LWGroup1 group to meet the management requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

|                                                                                                  |                          |
|--------------------------------------------------------------------------------------------------|--------------------------|
| (user.objectId -ne <input type="checkbox"/> ) and (user.userType - eq <input type="checkbox"/> ) | <input type="checkbox"/> |
| "Guest"                                                                                          | <input type="checkbox"/> |
| "Member"                                                                                         | <input type="checkbox"/> |
| Null                                                                                             | <input type="checkbox"/> |

|          |                          |
|----------|--------------------------|
| "Guest"  | <input type="checkbox"/> |
| "Member" | <input type="checkbox"/> |
| Null     | <input type="checkbox"/> |

### Answer Area

|                                                                                                                  |                                     |
|------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| Correct Answer: (user.objectId -ne <input type="checkbox"/> ) and (user.userType - eq <input type="checkbox"/> ) | <input type="checkbox"/>            |
| "Guest"                                                                                                          | <input checked="" type="checkbox"/> |
| "Member"                                                                                                         | <input checked="" type="checkbox"/> |

|          |                                     |
|----------|-------------------------------------|
| "Guest"  | <input checked="" type="checkbox"/> |
| "Member" | <input checked="" type="checkbox"/> |
| Null     | <input type="checkbox"/>            |

✉ [Removed] Highly Voted 2 years, 6 months ago

Null and Member. ObjectId is the GUID of the user  
upvoted 48 times

✉ AS007 2 years, 6 months ago

Why. They want to exclude guests  
upvoted 2 times

✉ WMG 1 year, 4 months ago

For anyone wondering, the query references user.ObjectId. This means you cannot use "Guest", as that is a UserType attribute.  
upvoted 3 times

✉ User92 Highly Voted 2 years, 5 months ago

Correct is indeed (user.ObjectId -ne null) and (user.userType -eq "Member"). See: <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/use-dynamic-groups#creating-a-group-of-members-only>  
upvoted 39 times

✉ jack987 11 months, 1 week ago

I agree with R1cardo92.  
The correct answer is (user.ObjectId -ne null) and (user.userType -eq "Member")

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/use-dynamic-groups#creating-a-group-of-members-only>  
upvoted 2 times

✉ oberte007 2 years, 2 months ago

you're alright  
upvoted 4 times

✉ dr22 1 year, 1 month ago

You're alright too dude, have a great day.  
upvoted 3 times

✉ JCKD4Ni3L Most Recent 2 months ago

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#create-an-all-users-rule>  
upvoted 1 times

dule27 4 months, 4 weeks ago

objectID -ne null ; userType -eq "member"

Pay attention!

On exam beside null and member you have to chose -ne or -eq and quotation marks as well .

upvoted 4 times

dule27 5 months ago

Null

Member

upvoted 1 times

Sango 5 months ago

This meets the requirements as -ne means to not equal (!=) " Guest" and then "Member for Group membership. Therefore, the correct syntax:  
(user.objectId -ne "Guest") and (user.userType -eq "Member")

upvoted 1 times

Taigr 9 months, 3 weeks ago

If you want your group to exclude guest users and include only members of your organization, you can use the following syntax:

(user.objectId -ne null) -and (user.userType -eq "Member")

It is directly on Microsoft web page <https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>

upvoted 5 times

w00t 1 year, 2 months ago

It's NULL and MEMBER

This link explains it 100% - <https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#:~:text=If%20you%20want%20your,user.userType%20%2Deq%20%22Member%22>

upvoted 6 times

mwasif25 1 year, 4 months ago

anyone having sc-300 exam dumps please share.. thanks

upvoted 3 times

sapien45 1 year, 5 months ago

user.ObjectId -ne null means all users

And among all the users

onlyt the members

upvoted 2 times

subhuman 1 year, 5 months ago

Given answer is wrong.

Correct answer is (user.ObjectId -ne null) and (user.userType -eq "Member") .

This is the link : <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/use-dynamic-groups>

upvoted 3 times

azjImpang 1 year, 5 months ago

REQ: Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Creating a group of members only

If you want your group to exclude guest users and include only members of your tenant, create a dynamic group as described above, but in the Rule syntax box, enter the following expression:

(user.ObjectId -ne null) and (user.userType -eq "Member")

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/use-dynamic-groups#creating-a-group-of-members-only>

upvoted 2 times

TP447 1 year, 7 months ago

Agreed this should be "Null" and "Member" - Guest is a User Type and not a reference for Object ID.

upvoted 3 times

Jun143 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 1 times

stromnessian 1 year, 9 months ago

null and member. Simples.

upvoted 1 times

stromnessian 1 year, 9 months ago

null, "Member" - simples.

upvoted 1 times

D7my 2 years, 2 months ago

i would go with null & member as mentioned in doc  
upvoted 2 times

### Topic 7 - Testlet 3

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

## Introductory Info

Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named **Contoso\_Resources**. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to https://contoso.com/auth-response.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

#### Question

HOTSPOT -

You need to meet the technical requirements for the probability that user identities were compromised.

What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer Area

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

#### Answer Area

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

Correct Answer:

You must configure:

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

 **DPRamone** Highly Voted  2 years, 6 months ago

IMO, you would need to set up MFA before SSPR when as per requirement protecting against leaked credentials by implementing a sign-in risk remediation policy without blocking access. Ref. <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identityprotection-remediate-unblock>.

upvoted 19 times

 **007Ali** 1 year, 10 months ago

I agree that in reality, you would enable MFA as that is the best way to protect accounts, but I think this question is about setting up a User Risk Policy, and in that policy one of the settings is "Identity Protection -> User Risk Policy -> Controls -> Allow access -> Require password change". Therefore setting up SSPR is required to complete this task.

upvoted 16 times

 **densyo** Highly Voted  2 years, 2 months ago

The answers are correct.

The question is about probability that user identities were compromised

User risk is a calculation of probability that an "identity" has been compromised.

Administrators can choose to block access, allow access, or allow access but require a password change using Azure AD self-service password reset.

upvoted 12 times

✉️ **Borbz** 2 years ago

You are correct.

upvoted 1 times

✉️ **dule27** [Most Recent] 5 months ago

SSPR

A user risk policy

upvoted 1 times

✉️ **wsrudmen** 10 months, 1 week ago

It's really hard to say. The Microsoft says the pros and cons.

"To perform secure password change to self-remediate a user risk:

The user must have registered for Azure AD MFA."

and after some lines

"

Self-remediation with self-service password reset

If a user has registered for self-service password reset (SSPR), then they can also remediate their own user risk by performing a self-service password reset."

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock>

upvoted 2 times

✉️ **Faheem2020** 1 year, 2 months ago

MFA and user risk policy is the answer for me.

"When a user risk policy triggers:

Administrators can require a secure password reset, requiring Azure AD MFA be done before the user creates a new password with SSPR, resetting the user risk."

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>

upvoted 5 times

✉️ **w00t** 1 year, 2 months ago

It's User Risk and SSPR

Within a User Risk policy, when setting the Controls - Access section, you only have two options:

- 1) you completely block the user
- 2) you allow the user access still, but they "Require password change"

MFA would be related to Sign-In risk policy, not User Risk.

upvoted 4 times

✉️ **Faheem2020** 1 year, 3 months ago

MFA is a requirement here.

upvoted 1 times

✉️ **sapien45** 1 year, 5 months ago

MFA and SSPR are two distinct setups that look similar and therefore lots of people are getting confused. That is why Azure is now forcing the combined setup :

Before combined registration, users registered authentication methods for Azure AD Multi-Factor Authentication and self-service password reset (SSPR) separately. People were confused that similar methods were used for Multi-Factor Authentication and SSPR but they had to register for both features. Now, with combined registration, users can register once and get the benefits of both Multi-Factor Authentication and SSPR.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-registration-mfa-sspr-combined>

But since there is no mention of combined setup SSPR it is

upvoted 4 times

✉️ **RandomNickname** 1 year, 5 months ago

MFA is a requirement for enabling SSPR and there's no mention in the Introductory Info that MFA is already setup.  
See below URL for reference;

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr>

So for me it's MFA and User Risk Pol

upvoted 4 times

✉️ **Xyz\_40** 1 year, 5 months ago

Users-risky situation. Users must first have SSPR enabled first. And then you will need to configure User-risk policy

upvoted 2 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question. MFA + User Risk Policy

upvoted 4 times

 **TheGuy** 1 year, 8 months ago

IMO, it is SSPR since MFA is not one of the requirements making me assuming MFA is already enabled. Also, in order to automate a password reset, SSPR needs to be enabled when the risky-user policy kicks in.

upvoted 1 times

 **stromnessian** 1 year, 9 months ago

Require the user to reset password - Requiring the users to reset passwords enables self-recovery without contacting help desk or an administrator. This method only applies to users that are registered for Azure AD MFA and SSPR. For users that haven't been registered, this option isn't available.

upvoted 2 times

 **stromnessian** 1 year, 9 months ago

Yes, correct.

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022

upvoted 2 times

 **Senior** 1 year, 9 months ago

The correct answers are:

MFA and user risk

ref: <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>

Warning:

Users must register for Azure AD MFA and SSPR before they face a situation requiring remediation. Users not registered are blocked and require administrator intervention.

Password change (I know my password and want to change it to something new) outside of the risky user policy remediation flow does not meet the requirement for secure password reset.

upvoted 6 times

 **lillyMS** 1 year, 4 months ago

Shouldn't it be MFA and sign in risk?

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

upvoted 1 times

## Topic 8 - Testlet 4

## Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

#### Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

### Question

You need to configure the MFA settings for users who connect from the Boston office. The solution must meet the authentication requirements and the access requirements.

What should you include in the configuration?

- A. named locations that have a private IP address range
- B. named locations that have a public IP address range
- C. trusted IPs that have a public IP address range
- D. trusted IPs that have a private IP address range

#### Correct Answer: B

#### Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

#### Community vote distribution

B (88%) 13%

007Ali Highly Voted 1 year, 10 months ago

Named Locations are part of Conditional Access Policies whereas "Trusted IPs" are in the legacy MFA settings, which would not be preferred. The IP address will appear to be coming into Azure from the NAT'd public address not the internal network private address. So I'd say: B. named locations that have a public IP address range

upvoted 22 times

AMZ 5 months, 3 weeks ago

Agree on B

Multifactor authentication trusted IPs

Using the trusted IPs section of multifactor authentication's service settings is no longer recommended. This control only accepts IPv4 addresses and should only be used for specific scenarios covered in the article Configure Azure AD Multifactor Authentication settings - <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#multifactor-authentication-trusted-ips>

upvoted 2 times

JaspaJami 1 year, 8 months ago

you can use trusted IP:s also in conditional access

upvoted 1 times

Gus909 1 year, 4 months ago

I think you are thinking of marking a Named Located in Conditional Access as Trusted via the "Mark as Trusted Location" setting. This is not the same as Trusted IP's though. Trusted IP's is a legacy setting that could be set in MFA and SharePoint Admin Center

upvoted 1 times

RandomNickname Highly Voted 1 year, 5 months ago

#### Selected Answer: B

Named locations for public IP is correct.

See:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

upvoted 6 times

dule27 Most Recent 5 months ago

#### Selected Answer: B

B. named locations that have a public IP address range

upvoted 1 times

LeTrinh 9 months, 2 weeks ago

Wrong.

It must be D for the reasons below:

1/ - Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

2/ Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection.  
3/ From Microsoft: The trusted IPs can include private IP ranges only when you use MFA Server. For cloud-based Azure AD Multi-Factor Authentication, you can use only public IP address ranges.  
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips>  
upvoted 1 times

fojoxa1092 1 year ago

Answer is C.

Trusted IP = Legacy MFA setting.  
Named Location = Conditional Access setting.

Setting up a Trusted IP automatically bypasses MFA, but setting up a Named Location does NOTHING. A Named Location by itself is just a fancy description for your IP addresses range. When creating a Named Location you check "mark as Trusted Location" AND after that you must create also a Conditional Access Policy where you specify MFA - Exclude Trusted Locations.

I reiterate it: by itself a Named Location cannot meet the requirements. You must mark it as a Trusted Location and add it to a Conditional Access Policy.

upvoted 1 times

KrisDeb 11 months, 3 weeks ago

The question is 'What should you include in the configuration' so the answer doesn't have to be a complete solution.

upvoted 1 times

Faheem2020 1 year, 3 months ago

The requirement is to use conditional access where you configure named location and not trusted IP. So B is the answer

upvoted 2 times

CharlieMike 1 year, 4 months ago

Selected Answer: C  
Trusted IPs is directly related to this question. It can be configured on the same location.

upvoted 1 times

purek77 11 months, 1 week ago

You have to follow other requirements as well, including "Control all access to all Azure resources and Azure AD applications by using conditional access policies."

You have to use Named Location + CA

upvoted 1 times

w00t 1 year, 2 months ago

Legacy option. Named Location is what you'd use. The answer is B

upvoted 1 times

sapien45 1 year, 5 months ago

C

The trusted IPs feature of Azure AD Multi-Factor Authentication bypasses multi-factor 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 Azure AD Multi-Factor Authentication prompt. The trusted IPs feature requires Azure AD Premium P1 edition.

The trusted IPs can include private IP ranges only when you use MFA Server. For cloud-based Azure AD Multi-Factor Authentication, you can use only public IP address ranges.

upvoted 2 times

Jun143 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 2 times

stromnessian 1 year, 9 months ago

B is the right answer.

upvoted 2 times

Pravda 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

melatocaroca 2 years, 4 months ago

Location offer your country set, IP ranges MFA trusted IP and corporate network

VPN gateway IP address: This is the public IP address of the VPN device for your on-premises network. The VPN device requires an IPv4 public IP address. Specify a valid public IP address for the VPN device to which you want to connect. It must be reachable by Azure

Client Address space: List the IP address ranges that you want routed to the local on-premises network through this gateway.

You can add multiple address space ranges. Make sure that the ranges you specify here do not overlap with ranges of other networks your virtual network connects to, or with the address ranges of the virtual network itself.

upvoted 2 times

 **[Removed]** 1 year, 11 months ago

Whats the answer that you go for ?

upvoted 2 times

 **Groot** 2 years, 5 months ago

C is the correct one

upvoted 2 times

 **ccarlton** 2 years, 5 months ago

B or C are both correct answers...

upvoted 1 times

 **NawafAli** 1 year, 11 months ago

I think B is correct as we need to configure using conditional access policy

upvoted 1 times

 **JaspaJami** 1 year, 8 months ago

you can use trusted IP:s also in conditional access. I would say both are correct but the named location is better.

upvoted 1 times

## Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

#### Question

HOTSPOT -

You need to support the planned changes and meet the technical requirements for MFA.

Which feature should you use, and how long before the users must complete the registration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer Area

Feature:

|                                                 |
|-------------------------------------------------|
| An authentication method policy                 |
| A Conditional Access policy                     |
| An MFA registration policy                      |
| The Multi-Factor Authentication Server settings |

Grace period:

|         |
|---------|
| 7 days  |
| 14 days |
| 28 days |

Correct Answer:

## Answer Area

Feature:

|                                                 |
|-------------------------------------------------|
| An authentication method policy                 |
| A Conditional Access policy                     |
| An MFA registration policy                      |
| The Multi-Factor Authentication Server settings |

Grace period:

|         |
|---------|
| 7 days  |
| 14 days |
| 28 days |

Box 1: A Conditional Access policy

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Box 2: 14 days -

Multi-factor authentication (MFA): multi-factor authentication is a type of authentication that requires the use of two or more verification factors to gain access to a system. Azure MFA offers a 14 day grace period after being initiated.

Reference:

<https://www.syskit.com/blog/using-azure-conditional-access-when-security-defaults-isnt-enough/>

✉ **Hot\_156** Highly Voted 1 year, 2 months ago

Well, this is something confuse... They ask you to force MFA using CA policy. If you use it, you will be forced to register for MFA YES or YES and there will not be any 14 days grace period. This happens when you use CA, so if they are giving you the option to choose grace days, the answer cannot be MFA CA policy. It has to be MFA registration.

I TESTED THIS! there you have, if they ask you for something with 14 days grace period, it cannot be MFA CA policy, if they don't give you that option on the exam, you can go for MFA CA.

upvoted 12 times

✉ **zed026** Highly Voted 1 year, 3 months ago

First answer should be MFA registration policy. <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy#policy-configuration>

upvoted 12 times

✉ **w00t** 1 year, 2 months ago

But the requirement literally says:

"Implement multi-factor authentication (MFA) for all Litware users by using CONDITIONAL ACCESS POLICIES." lol

upvoted 1 times

✉ **prelek1984** 1 year, 2 months ago

but Conditional access doesn't offer 14 day grace period

upvoted 12 times

✉ **ACSC** Most Recent 1 month, 4 weeks ago

MFA registration policy

14 days

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy#what-is-the-azure-ad-multifactor-authentication-registration-policy>

upvoted 2 times

✉ **Leon1969** 2 months, 2 weeks ago

MFA registration policy: <https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy>

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

upvoted 2 times

□ **ServerBrain** 3 months ago

What are the technical requirements to be implemented to meet MFA??

These are:

- Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.
- Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- Enforce MFA when accessing on-premises applications.
- Control all access to all Azure resources and Azure AD applications by using conditional access policies.
- Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

So,,, if you need Conditional Access Policies, not CA Registration policy..

upvoted 1 times

□ **JN\_311** 5 months ago

Based on the MS link: <https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy#what-is-the-azure-ad-multifactor-authentication-registration-policy>

Answer:

MFA Registration Policy

14 Days

upvoted 2 times

□ **dule27** 5 months ago

A Conditional access policy

14 days

upvoted 1 times

□ **AK\_1234** 1 month, 3 weeks ago

Incorrect.

- MFA Registration policy
- 14 days

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy#what-is-the-azure-ad-multifactor-authentication-registration-policy>

upvoted 1 times

□ **dobriv** 8 months ago

I think the first answer is MFA registration policy :

.....for the 14 day grace period to apply to users when registering for MFA, there are two ways to achieve this. One way would be to enable Security Defaults which would enable MFA for the entire tenant. This option does not need additional licenses and can be enabled from the AAD portal.

## Topic 9 - Testlet 5

upvoted 1 times

□ **estyj** 12 months ago

I would say conditional access policy since it said to Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies. 14 day grace period.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

upvoted 3 times

□ **chikorita** 8 months, 1 week ago

this made the most sense to me

upvoted 1 times

□ **Jacordoba** 1 year, 2 months ago

MFA registration Policy 14 days should be the answer

upvoted 6 times

## Introductory Info

Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named **Contoso\_Resources**. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

#### Question

You need to meet the planned changes and technical requirements for App1.

What should you implement?

- A. a policy set in Microsoft Endpoint Manager
- B. an app configuration policy in Microsoft Endpoint Manager
- C. an app registration in Azure AD
- D. Azure AD Application Proxy

#### Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

Community vote distribution

C (100%)

 **zed01** Highly Voted 2 years, 6 months ago

C looks like a correct answer.  
upvoted 10 times

 **Azurefox79** Highly Voted 2 years, 5 months ago

Correct forsure, you can assign a redirect URI as part of the registration process.  
upvoted 7 times

 **dule27** Most Recent 5 months ago

Selected Answer: C  
C. an app registration in Azure AD  
upvoted 1 times

 **Jawad1462** 1 year, 1 month ago

Selected Answer: C  
Correct answer  
upvoted 4 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022  
upvoted 3 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.  
upvoted 1 times

 **stromnessian** 1 year, 9 months ago

I like easy questions :-) C is correct.  
upvoted 1 times

 **ServerBrain** 3 months ago

well, we all do to pass  
upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022

upvoted 2 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 1 times

 **BaderJ** 2 years, 2 months ago

Passed the exam today 23/09/2021

This question came in the exam.

upvoted 1 times

 **Che1** 2 years, 5 months ago

It is correct answer, question is talking about Azure web app. Azure Application proxy is used to access on-premise application without need of VPN & users are authenticated in Azure AD.

upvoted 5 times

## Topic 10 - Testlet 6

## Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

#### Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

### Question

HOTSPOT -

You need to implement on-premises application and SharePoint Online restrictions to meet the authentication requirements and the access requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

For on-premises applications:

- Configure Cloud App Security policies.
- Modify the User consent settings for the enterprise applications.
- Publish the applications by using Azure AD Application Proxy.

For SharePoint Online:

- Configure app-enforced restrictions.
- Modify the User consent settings for the enterprise applications.
- Publish an application by using Azure AD Application Proxy.

Correct Answer:

### Answer Area

For on-premises applications:

- Configure Cloud App Security policies.
- Modify the User consent settings for the enterprise applications.
- Publish the applications by using Azure AD Application Proxy.

For SharePoint Online:

- Configure app-enforced restrictions.
- Modify the User consent settings for the enterprise applications.
- Publish an application by using Azure AD Application Proxy.

Reference:

<https://docs.microsoft.com/en-us/sharepoint/app-enforced-restrictions> <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>

 **dule27** 5 months ago

On-premise: Publish the applications by using Azure AD Application Proxy

SharePoint: Configure app-enforced restrictions

upvoted 1 times

 **rachee** 1 year, 4 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy>

upvoted 1 times

 **sapien45** 1 year, 5 months ago

now called Conditional Access App Control  
upvoted 2 times

✉ **Jacquesvz** 1 year, 3 months ago

App Enforce Restrictions (<https://aka.ms/caapprestrictions>) are for supported apps only: Office 365, Exchange Online and Sharepoint Online. Conditional access app Control (<https://aka.ms/mcaslearnmore>) supports various Cloud Apps not supported by App Enforced Restrictions.  
upvoted 3 times

✉ **subhuman** 1 year, 5 months ago

Given answers are correct  
upvoted 1 times

✉ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.  
upvoted 1 times

✉ **stromnessian** 1 year, 9 months ago

Super easy. Given answers are correct.  
upvoted 1 times

✉ **Pravda** 1 year, 10 months ago

On the exam 1/20/2022  
upvoted 2 times

✉ **melatocaroca** 2 years, 4 months ago

IMHO first boss option is wrong, second is right

Configure Cloud App Security policies

Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Access and session policies are used within the Cloud App Security portal to further refine filters and set actions to be taken on a user.

Configure app-enforced settings

Conditional Access App Control uses a reverse proxy architecture and integrates with your IdP. When integrating with Azure AD Conditional Access, you can configure apps to work with Conditional Access App Control with just a few clicks, allowing you to easily and selectively enforce access and session controls on your organization's apps based on any condition in Conditional Access..

Protect apps with Microsoft Cloud App Security Conditional Access App Control

<https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad#featured-apps>

<https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad#how-it-works>

upvoted 2 times

✉ **waituna** 2 years, 3 months ago

The requirement for on-premise applications is "Enforce MFA when accessing ...", as we have already  
\* Implement MFA for all Litware users (via Azure AD)  
\* Litware implements Azure AD Application Proxy

we just need to "Publish the applications by using Azure AD Application Proxy" - this will force users to use their Azure AD account (and MFA) to access the on-premise applications.

upvoted 21 times

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

Agreed. Originally I got hung up on "Litware implements Azure AD Application Proxy" and assumed that they are already publishing the apps because who would implement the proxy and do nothing with it? Litware! Apparently MS thinks (or knows?) there are some dummies out there who need an average IT guy to point out the obvious. "Publish that app!" LMAO :-D

upvoted 1 times

## Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

#### Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

#### Question

HOTSPOT -

You need to configure app registration in Azure AD to meet the delegation requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer Area

Azure AD tenant-level setting to modify:

- Allow users to register application
- Users can consent to apps accessing company data on their behalf
- Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

- Application administrator
- Application developer
- Cloud application administrator

Correct Answer:

#### Answer Area

Azure AD tenant-level setting to modify:

- Allow users to register application
- Users can consent to apps accessing company data on their behalf
- Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

- Application administrator
- Application developer
- Cloud application administrator

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles>

✉ hwoarang Highly Voted 1 year, 11 months ago

The answer is Correct!

1: Requirements for delegation clearly says " Prevent users to register applications"

2: User1 would need App Developer to register an app in tenant using "principle of least privilege"

upvoted 12 times

✉ jack987 11 months, 1 week ago

The answer is correct.

Application Developer

Users in this role can create application registrations when the "Users can register applications" setting is set to No. This role also grants permission to consent on one's own behalf when the "Users can consent to apps accessing company data on their behalf" setting is set to No. Users assigned to this role are added as owners when creating new application registrations.

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

upvoted 1 times

 **JCKD4Ni3L** 1 month, 4 weeks ago

Why would the first answer of "Allow users to register application" be correct when it is clearly stated "Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant." ?

The Application Developer role is correct for the second choice tho.

upvoted 2 times

 **JimboJones99** 1 month, 1 week ago

It's asking which setting you would modify, not what you would set it to

upvoted 1 times

 **RandomNickname**  1 year, 5 months ago

Given answer is correct.

For both questions see URL provide in answer section of question;

<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles#restrict-who-can-create-applications>

and extraction from URL's

#1 "On the User settings page for your organization, set the Users can register applications setting to No. This will disable the default ability for users to create application registrations."

#2 "By default in Azure AD, all users can register applications and manage all aspects of applications they create. Everyone also has the ability to consent to apps accessing company data on their behalf. You can choose to selectively grant those permissions by setting the global switches to 'No' and adding the selected users to the Application Developer role."

These meet question answers

upvoted 7 times

 **Nyamnyam**  3 weeks, 2 days ago

Second answer is not correct.

Here the case study delegation requirement:

"Ensure that User1 can create enterprise applications in Azure AD"

Now search for "create enterprise application" here: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-by-task>

It is the Cloud Application Administrator.

Application Developer can "Create application registration when ability is disabled for all users", indeed, but no mention on Enterprise Apps description.

Well, you can start arguing here that he has the microsoft.directory/servicePrincipals/createAsOwner permission, and I'd reply "where is the requirement for User1 to be automatically assigned owner?" And what is the practical use of the whole dumb MSFT question? Such questions are a pure chicanery.

If you follow the instructions below, the prerequisites are on ALL steps to be Application Administrator.

<https://learn.microsoft.com/en-us/entra/identity/app-proxy/application-proxy-add-on-premises-application#prerequisites>

upvoted 1 times

 **Intrudire** 1 month, 2 weeks ago

#1: Users Can Register Apps

#2: Cloud Application Administrator

"Ensure that User1 can create enterprise applications in Azure AD."

External Identities/B2C:

Task/Least privileged role/Additional Roles

Create enterprise applications/Cloud Application Administrator/Application Administrator

<https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task>

upvoted 1 times

 **Intrudire** 1 month, 2 weeks ago

I'm changing my answer. Given answer is correct.

#1: Users Can Register Apps

You would configure this to "NO"

That solves this sentence:

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

#2: Application Developer

"Assign the Application Developer role to grant the ability to create application registrations when the Users can register applications setting is set to No."

<https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles#grant-individual-permissions-to-create-and-consent-to-applications-when-the-default-ability-is-disabled>

upvoted 1 times

 **Intrudire** 1 month, 2 weeks ago

I don't know anymore. Cloud App Admin and App Admin all talk about the ability to register ENTERPRISE apps, which is part of the question. Application Developers apparently don't have that ability.

<https://learn.microsoft.com/en-us/answers/questions/270680/app-registration-vs-enterprise-applications>

Maybe it is Cloud App Admin afterall.....

upvoted 1 times

 **penatuna** 2 months ago

For the role to assign to User1:

I'm still not sure about this. The question says:

- Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

- Ensure that User1 can create enterprise applications in Azure AD.

With enterprise apps, it has to be at least Cloud application administrator. But, if you have to also set up application proxy, then it should be Application administrator.

I'll go with Cloud application admin, but I'm not 100% sure about it.

upvoted 1 times

 **northgaterebel** 3 months, 1 week ago

1: Allow users to register application

2: Application administrator. Requirement: Ensure that User1 can create "enterprise applications" in Azure AD. To add an enterprise application to your Azure AD tenant, you need one of the following roles: Global Administrator, or Application Administrator.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal>

upvoted 1 times

 **einkaufacs** 4 months, 2 weeks ago

Weired. In the text they are talking about enterprise app. There you would need cloud application admin. In the question they are asking for app registration. There App Developer would be enough.

upvoted 2 times

 **dule27** 5 months ago

Allow users to register application

Application developer

upvoted 1 times

 **JN\_311** 5 months ago

What you be able to back up your answer?

upvoted 1 times

 **JN\_311** 5 months, 2 weeks ago

For second one, it clearly states: Ensure that User1 can create enterprise applications in Azure AD, not register application., two different things.  
The key word is Create Enterprise Applications. You need Cloud Application Administrator

upvoted 3 times

 **LeTrinh** 9 months, 3 weeks ago

1. A

2.C

From Microsoft link:

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

Assign the Application Developer role to grant the ability to create application registrations when the Users can register applications setting is set to No. This role also grants permission to consent on one's own behalf when the Users can consent to apps accessing company data on their behalf setting is set to No.

upvoted 2 times

 **divyakanth** 9 months, 4 weeks ago

note that in the deligation requirements it had been cleary mentioned that the user! had to be able to creatae enterpirse appliacations which can be done by CAA via least previlage. App developer doesnt have the ability to create enterprise apps. HBope this clears.

upvoted 1 times

 **BB6919** 10 months, 3 weeks ago

The second answer should be CAA. App developer role can't create app via enterprise application

upvoted 1 times

 **LP223** 10 months, 3 weeks ago

It 100% should be Cloud App Admin according to the least privileged roles documentation for "Create Enterprise Application" action:  
<https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#groups>

upvoted 2 times

 **ThotSlayer69** 10 months, 1 week ago

Not only does your link say Application Developer is the least privilege role for this (<https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#application-proxy>), but also you should know that Cloud Application \*Administrator\* is equal to Application Administrator except for App Proxy, both of which are much more privileged than Application Developer

upvoted 3 times

 **Faheem2020** 1 year, 2 months ago

There is a difference between application and creating an enterprise application. Application developer role cannot add an enterprise application in Azure AD

"To add an enterprise application to your Azure AD tenant, you need:

An Azure AD user account. If you don't already have one, you can Create an account for free.

One of the following roles: Global Administrator, Cloud Application Administrator, or Application Administrator."

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal>

upvoted 3 times

□ **Faheem2020** 1 year, 2 months ago

Typo: There is a difference between application registration and creating an enterprise application. Application developer role cannot add an enterprise application in Azure AD

upvoted 2 times

□ **Hot\_156** 1 year, 2 months ago

I tested this and also found this,

- One of the following roles: Global Administrator, Cloud Application Administrator, or Application Administrator.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal#add-an-enterprise-application>

1 - Allow Users to register applications

2 - Cloud Application Administrator (You cannot register Enterprise Apps with APPLICATION DEVELOPER and Application Administrator gives you Application proxy access)

upvoted 4 times

□ **Zak366** 9 months, 2 weeks ago

Correct. I am going with:

1. Allow users to register application

2. Cloud Administrator

(<https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#enterprise-applications>)

Application Developer CANNOT create enterprise application. Requirements say Ensure that user1 can create enterprise applications in Azure AD

upvoted 1 times

□ **kakakayayaya** 1 year, 6 months ago

I don't think 1 answer is correct.

What does "Allow users to register app" mean? To allow it you should go;

Azure AD-->User settings-->App registrations --> Users can register applications -->yes

Is it requirement? No.

upvoted 2 times

□ **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 1 times

□ **stromnessian** 1 year, 9 months ago

App developers can create app registrations, thereby also creating an associated Enterprise App instance.

upvoted 1 times

## Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

#### Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

### Question

HOTSPOT -

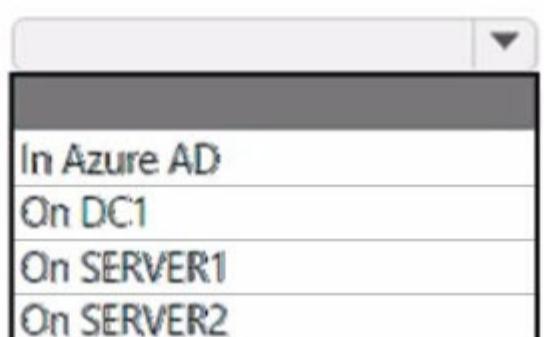
How should the access be setup to the on-premises applications?

Hot Area:

Configure the Azure AD Password Protection proxy service on:

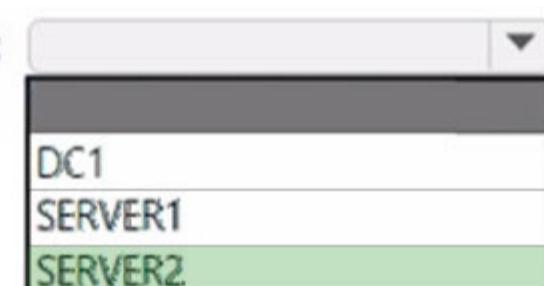


Configure the password list:

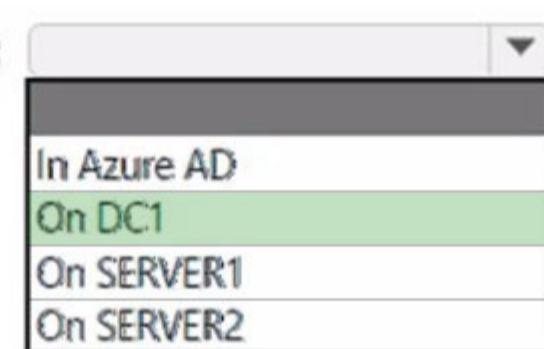


Correct Answer:

Configure the Azure AD Password Protection proxy service on:



Configure the password list:



Box 1: Server2

Incorrect:

Not Server 1: If you've deployed Azure AD Password Protection Proxy, do not install Azure AD Application Proxy and Azure AD Password Protection Proxy together on the same machine. Azure AD Application Proxy and Azure AD Password Protection Proxy install different versions of the Azure AD Connect Agent

Updater service. These different versions are incompatible when installed together on the same machine.

Server1 runs the Azure AD application Proxy connector.

To use Application Proxy, you need a Windows server running Windows Server 2012 R2 or later. You'll install the Application Proxy connector on the server. This connector server needs to connect to the Application Proxy services in Azure, and the on-premises applications that you plan to publish.

Scenario:

Requirements. Authentication Requirements include:

Enforce MFA when accessing on-premises applications.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Box 2: DC1 -

The Azure AD Password Protection proxy service is typically on a member server in your on-premises AD DS environment. Once installed, the Azure AD

Password Protection proxy service communicates with Azure AD to maintain a copy of the global and customer banned password lists for your Azure AD tenant.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application>

✉  **Mriji** Highly Voted 1 year ago

Correct answer is Server 2, then Azure AD. The password protection proxy is installed on a member server. You enable the banned p/w list in Azure AD, the proxy downloads it and passes it to the DCs in the domain.

upvoted 14 times

✉  **Nyamnyam** 3 weeks, 2 days ago

Agree with the majority here: Custom banned password list is configured on Azure AD, now Entra ID portal

BTW the first part is very suspect, because AD Connect also has the "Microsoft Entra Connect Agent Updater" service as part of its installation routine. In real life you'd prefer a separate, additional member server.

<https://learn.microsoft.com/en-us/entra/identity/hybrid/verify-sync-tool-version>

upvoted 1 times

✉  **Faheem2020** Highly Voted 1 year, 2 months ago

Answer should be SERVER2 and Azure AD

Configure the password list in Azure AD, the password protection proxy makes it available on you on prem DC, refer to the diagram in the link: <https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

upvoted 9 times

✉  **hw121693** Most Recent 4 months, 2 weeks ago

Look at this page

<https://learn.microsoft.com/en-us/training/modules/manage-user-authentication/6-deploy-manage-password-protection>

First one should be server 2

upvoted 1 times

✉  **dule27** 5 months ago

AD password protection proxy service: Server 2

Configure the password list: on DC1

upvoted 1 times

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

AD password protection cannot be on proxy server so it is = Server 2  
and DC needs the list of banned passwords PTA so = on DC1

upvoted 1 times

✉  **dobriv** 8 months ago

It is a SERVER 2 answer ! Here is written very clear :

!! Warning !!!

Azure AD Password Protection proxy and Azure AD Application Proxy install different versions of the Microsoft Azure AD Connect Agent Updater service, which is why the instructions refer to Application Proxy content. These different versions are incompatible when installed side by side and doing so will prevent the Agent Updater service from contacting Azure for software updates, so you should never install Azure AD Password Protection Proxy and Application Proxy on the same machine.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

upvoted 2 times

✉  **chikorita** 8 months, 1 week ago

Reasons why we need Password protection service on Server 2:

DC1: this usually doesn't have connectivity to internet, so not a viable option

Server1: please keep in mind that AAD password protection service and AAD Application proxy uses different versions of AAD. Gives rise to compatibility issue

Server2: only possible option left

upvoted 1 times

jack987 11 months, 1 week ago

The correct answer is Server2 and Azure AD.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection>

upvoted 3 times

martinods 1 year, 2 months ago

password list should be configured on Azure AD not on DC !

upvoted 8 times

geobarou 1 year, 2 months ago

No. It must be on DC. We have pass-through authentication.

upvoted 2 times

martinods 1 year, 2 months ago

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection#configure-custom-banned-passwords>. Point 1 Sign in to the Azure portal using an account with global administrator permissions.

upvoted 1 times

geobarou 1 year, 2 months ago

The question says: "Connect uses pass-through authentication and has password hash synchronization disabled."

It means that ADDS is doing the authentication. How the Azure AD will be asked if the password is in banned list? Your link says nothing about hybrid environment as we have here. The link in the answer has the information.

upvoted 1 times

Hot\_156 1 year, 2 months ago

Check this link,

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises>

Under "How Azure AD PP works" you will find this,

The DC Agent service is responsible for initiating the download of a new password policy from Azure AD. The first step is to locate an Azure AD Password Protection Proxy service by querying the forest for proxy serviceConnectionPoint objects.

and if you keep reading, you will find that there is no such thing as a password banned listed on-prem for modification. Everything is downloaded from Azure AD

With that, I will stay with

-Server2

-Azure AD

upvoted 8 times

Hot\_156 1 year, 2 months ago

If you read their reasoning for choosing The DC, it is still clear that the list is downloaded from Azure

Box 2: DC1 -

The Azure AD Password Protection proxy service is typically on a member server in your on-premises AD DS environment. Once installed, the Azure AD

Password Protection proxy service communicates with Azure AD to maintain a copy of the global and customer banned password lists for your Azure AD tenant.

upvoted 1 times

## Introductory Info

Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named **Contoso\_Resources**. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

#### Question

You create a Log Analytics workspace.

You need to implement the technical requirements for auditing.

What should you configure in Azure AD?

- A. Company branding
- B. Diagnostics settings
- C. External Identities
- D. App registrations

#### Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring>

Community vote distribution

B (100%)

 **MajorUrs** Highly Voted 2 years, 6 months ago

Correct (B)

upvoted 10 times

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

**Selected Answer: B**

B. Diagnostics settings

upvoted 1 times

 **marot** 4 months, 1 week ago

**Selected Answer: B**

Step 2: Portal > Search for Azure Active Directory > In Monitoring section, click Diagnostic setting. > On the Diagnostic settings page, click Add diagnostic setting. > Under Category details, select AuditLogs and SigninLogs. > Under Destination details, select Send to Log Analytics, and then select your new log analytics workspace. > Save

<https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard#configure-a-workspace>  
upvoted 1 times

 **dule27** 5 months ago

**Selected Answer: B**

B. Diagnostics settings

upvoted 1 times

 **yj90** 1 year, 6 months ago

Any answers with Diagnostics settings = Correct

upvoted 3 times

 **Yelad** 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 1 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 2 times

- **stromnessian** 1 year, 9 months ago

Selected Answer: B

B for sure.

upvoted 1 times

- **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022

upvoted 1 times

- **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 2 times

- **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 2 times

- **melatocaroca** 2 years, 4 months ago

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/design-logs-deployment>

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-control-logging-monitoring>

upvoted 1 times

## Introductory Info

Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named **Contoso\_Resources**. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to https://contoso.com/auth-response.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

#### Question

HOTSPOT -

You need to implement the planned changes and technical requirements for the marketing department.

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

NOTE: Each correct selection is worth one point.

Hot Area:

#### Answer Area

To configure user access:

|                             |
|-----------------------------|
| An access package           |
| An access review            |
| A conditional access policy |

To enable collaboration with fabrikam.com:

|                          |
|--------------------------|
| An accepted domain       |
| A connected organization |
| A custom domain name     |

#### Answer Area

To configure user access:

|                             |
|-----------------------------|
| An access package           |
| An access review            |
| A conditional access policy |

Correct Answer:

To enable collaboration with fabrikam.com:

|                          |
|--------------------------|
| An accepted domain       |
| A connected organization |
| A custom domain name     |

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-organization>

 MajorUrs Highly Voted 2 years, 6 months ago

Correct

upvoted 12 times

 dule27 Most Recent 5 months ago

An access package

A connected organization

upvoted 1 times

 d3j4n 1 year, 4 months ago

Correct! Tested in lab today!

upvoted 2 times

 Yelad 1 year, 8 months ago

On the exam - March 28, 2022

upvoted 2 times

 **Jun143** 1 year, 8 months ago

just pass the exam today. This came in the question.

upvoted 2 times

 **stromnessian** 1 year, 9 months ago

Answers are correct.

upvoted 1 times

 **TonytheTiger** 1 year, 9 months ago

On the exam today - March 4, 2022

upvoted 1 times

 **zmlapq99** 1 year, 10 months ago

On exam few days ago.

upvoted 1 times

 **Pravda** 1 year, 10 months ago

On the exam 1/20/2022

upvoted 2 times

 **BaderJ** 2 years, 2 months ago

Passed the exam today 23/09/2021

This question came in the exam.

upvoted 1 times

## Introductory Info

Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named **Contoso\_Resources**. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

#### Question

You need to meet the planned changes for the User administrator role.

What should you do?

- A. Create an access review.
- B. Create an administrative unit.
- C. Modify Active assignments.
- D. Modify Role settings.

#### Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user?tabs=new>

Community vote distribution

Che1 Highly Voted 2 years, 5 months ago

Role settings is the correct answer.

upvoted 19 times

Hot\_156 1 year, 2 months ago

For those who are saying the correct answer is "C" Modify Active Assignment, where does it say the Role is assigned as Active? Don't assume things if the Use Case doesn't specify that unless is the default configuration!

Using the information provided in the study case, The correct answer is D - Role settings.

upvoted 1 times

Domza Highly Voted 2 years, 5 months ago

Role Setting details is where you need to be: Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Default Setting State

Require justification on activation Yes

Require ticket information on activation No

On activation, require Azure MFA Yes

Require approval to activate No

Approvers None

upvoted 15 times

marsot Most Recent 4 months, 1 week ago

Selected Answer: D

Azure Portal > Azure AD > Identity Governance > (Privileged Identity Management-Heading)Azure AD Roles > (Manage-Heading) Settings > Search for User Administrator > Edit > Require justification on activation : Yes and Require approval to activate: Yes

Or in the documentation here:

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings>

upvoted 2 times

dule27 5 months ago

Selected Answer: D

D. Modify Role settings

upvoted 2 times

✉ **TafMuko** 5 months, 3 weeks ago

**Selected Answer: D**

Spent a few minutes debating this until I found this. <https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings>

upvoted 1 times

✉ **sbnpj** 7 months, 3 weeks ago

Role Settings

upvoted 1 times

✉ **AWS56** 9 months, 3 weeks ago

**Selected Answer: D**

Role setting

upvoted 2 times

✉ **wooyourdaddy** 10 months, 1 week ago

There are 3 pieces of data that are relevant. In the overview, it states:

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Under problem statement is:

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

Under planned changes is:

Configure the User administrator role to require justification and approval to activate.

The question is how to meet the planned changes, which is to configure the user administrator role. So Answer D can be the only logical choice.

upvoted 2 times

✉ **jack987** 11 months, 1 week ago

**Selected Answer: D**

I agree with Hot\_156.

The correct answer is D - Role settings.

upvoted 1 times

✉ **estyj** 12 months ago

D. Modify Role settings - "Configure the User administrator role to require justification and approval to activate." So need to modify the AD Role settings and change to eligible and require justification to yes. Notice that it is in the Azure AD role section.  
<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user?tabs=new>

upvoted 1 times

✉ **Jhill777** 1 year ago

Role>Role Setting>Check the box for "Require Justification on Activation".

upvoted 3 times

✉ **Lion007** 1 year, 4 months ago

**Selected Answer: C**

Correct: C. Modify Active assignments.

Planned Changes --> Configure the User administrator role to require justification and approval to activate. --> answer should be around PIM -- which makes "Modify Active assignments" is the only correct answer.

upvoted 1 times

✉ **rachee** 1 year, 4 months ago

D. for sure. <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings>

upvoted 1 times

✉ **subhuman** 1 year, 5 months ago

**Selected Answer: D**

Correct answer is D. its in Role settings where this is defined

upvoted 1 times

✉ **RandomNickname** 1 year, 5 months ago

**Selected Answer: C**

For me the given answer is correct.

C:

Sure you'd need to start by modify in PIM the assigned role the user is a member of, but that doesn't specifically answer the question. To answer the question, which is asking how you'd ensure the User Admin role requires justification and approval to activate you'd need to "Modify the Active assignments" to "Eligible assignments" to ensure "business justification, or requesting approval from designated approvers" to activate.

So I believe the question is testing if you know the difference in PIM what Eligible and Active assignments are.

upvoted 1 times

 **RandomNickname** 1 year, 5 months ago

I stand corrected!! While it's correct to have it changed to eligible since this has the following;

"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."

As opposed to active

"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 at all times."

From: <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user>

Which answers the question.

However, to define these required approval and justification settings would be done in "Role Settings"

So D is correct rather than C

upvoted 2 times

 **jasonga** 1 year, 5 months ago

**Selected Answer: C**

role settings

upvoted 1 times

 **InformationOverload** 1 year, 6 months ago

For me its C. "Configure the User administrator role to require justification and approval to activate." This is done when role assignment is eligible and not set to active

upvoted 2 times

## Introductory Info

Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named **Contoso\_Resources**. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

#### Question

You need to modify the settings of the User administrator role to meet the technical requirements.

Which two actions should you perform for the role? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Select Require justification on activation.
- B. Select Require ticket information on activation.
- C. Modify the Expire eligible assignments after setting.
- D. Set all assignments to Eligible.
- E. Set all assignments to Active.

#### Correct Answer: AE

Scenario: Configure the User administrator role to require justification and approval to activate.

A: Require justification.

You can require that users enter a business justification when they activate. To require justification, check the Require justification on active assignment box or the

Require justification on activation box.

E: You can choose from two assignment duration options for each assignment type (eligible and active) when you configure settings for a role.

You can choose one of these active assignment duration options:

Allow permanent active assignment: Global admins and Privileged role admins can assign permanent active assignment.

Expire active assignment after: Global admins and Privileged role admins can require that all active assignments have a specified start and end date.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings>

#### Community vote distribution

AD (86%) 14%

 **fcesheng** Highly Voted 1 year, 2 months ago

Should it be AD instead of AE?

To require justification need assignment to be Eligible instead of Active

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>  
upvoted 20 times

 **simonseztech** Highly Voted 11 months, 3 weeks ago

**Selected Answer: AD**

You should be eligible to be able to activate the role with a justification

upvoted 5 times

 **ServerBrain** Most Recent 3 months ago

**Selected Answer: AD**

AD, the combination of AE simply does not make sense

upvoted 2 times

 **marsot** 4 months, 1 week ago

**Selected Answer: AD**

Why D & E confuse us: E requires justification for a person who assigns the role and NOT for the assignee. This means that this person should justify why they made this role active.

On the other hand, D refers to the member with the role and privileges to perform an action. With eligible roles, we can set members to get approval before they act.

The question refers to the latter case. What we need is for whoever uses the User Admin role to have approval.

upvoted 1 times

 **OK2020** 4 months, 4 weeks ago

**Selected Answer: AD**

"Eligible" require action to activate, which then can be set as "require approval"

upvoted 2 times

 **dule27** 5 months ago

**Selected Answer: AD**

- A. Select require justification on activation  
D. Set all assignments to Eligible

upvoted 3 times

店铺：专业认证88

 **Sango** 5 months ago

A and D. The requirements "Configure the User administrator role to require justification and approval to activate" means that it must be Eligible and "Require Justification on Activation." An Active Role (option E) means no approval or justification is required, therefore, does not meet the requirements.

upvoted 2 times

 **penatuna** 7 months ago

**Selected Answer: AD**

Question says:

- Configure the User administrator role to require justification and approval to activate.

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.

<https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#assign>

upvoted 3 times

 **sbnpj** 7 months, 3 weeks ago

(AE) is the correct answer, when you assign PIM role, assignment type =Active allows you the type justification.

upvoted 1 times

 **AWS56** 9 months, 3 weeks ago

**Selected Answer: AD**

Agree AD

upvoted 2 times

 **ThotSlayer69** 10 months, 1 week ago

**Selected Answer: AD**

Activation = Eligible

Active = Permanently active

Justification on activation implies Eligible

They also want to make approval in addition to justification a requirement to activate User Administrator, so clearly it is eligible and not active permanently

upvoted 2 times

店铺：专业认证88

 **AMDF** 11 months, 3 weeks ago

**Selected Answer: AD**

I think AD is correct. Need to be eligible

upvoted 2 times

 **estyj** 12 months ago

A&D - "Configure the User administrator role to require justification and approval to activate." so need to set to eligible and select require justification for activation. If it was set all assignments to active wouldn't need to require justification.

upvoted 3 times

 **estyj** 1 year ago

Need to set all assignments to Eligible not Active. User will need to activate PIM and enter justification.

upvoted 1 times

 **Buzz8** 1 year ago

**Selected Answer: AE**

It's correct - Hot\_156 "To require justification need assignment to be Eligible instead of Active" You've got it the wrong way around, it's "To require justification the assignment must be set to Active" I've just tested it and if you select Active, a box pops up below asking for Justification, whereas with Eligible there isn't any further input required and you can just click "Assign".

upvoted 4 times

 **technocorgi** 8 months, 4 weeks ago

Buzz8 you are 100% right, I just tested out in my own env and Active = require Justification while Eligible does not require justification  
upvoted 1 times

 **DeepMoon** 1 year, 1 month ago

Confusion between D & E are because those are not settings available on screen.

See: <https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings#assignment-duration>

More than likely when we see the question on the exam this would be corrected.

Correct Setting should be "Allow permanent active role assignment" YES.  
This is what is required under planned changes section.

upvoted 2 times

 **Hot\_156** 1 year, 2 months ago

**Selected Answer: AD**

To require justification need assignment to be Eligible instead of Active

upvoted 2 times

## Introductory Info

Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named **Contoso\_Resources**. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

#### Question

You need to resolve the issue of the guest user invitations.

What should you do for the Azure AD tenant?

- A. Configure the Continuous access evaluation settings.
- B. Configure a Conditional Access policy.
- C. Configure the Access reviews settings.
- D. Modify the External collaboration settings.

#### Correct Answer: C

Scenario: The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Manage guest access with Azure AD access reviews.

With Azure Active Directory (Azure AD), you can easily enable collaboration across organizational boundaries by using the Azure AD B2B feature. Guest users from other tenants can be invited by administrators or by other users. This capability also applies to social identities such as Microsoft accounts.

You also can easily ensure that guest users have appropriate access. You can ask the guests themselves or a decision maker to participate in an access review and recertify (or attest) to the guests' access. The reviewers can give their input on each user's need for continued access, based on suggestions from Azure AD.

When an access review is finished, you can then make changes and remove access for guests who no longer need it.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-guest-access-with-access-reviews>

#### Community vote distribution

D (92%) 8%

 **zygmant** Highly Voted  1 year, 1 month ago

D.

"You need to resolve the issue of the guest user invitations." Guest user invitations is the key.

Invitation settings are in "External collaboration settings" blade.

You can allow anyone in the organization to invite guest users, or restrict it to the specific admin role and grant users permission to the Guest Inviter role.

Access reviews have nothing in common with user invitations.

upvoted 6 times

 **f2bf85a** Highly Voted  7 months, 2 weeks ago

#### Selected Answer: D

The question asks to resolve the "issue". This focuses on the issues defined in the Case Study.

The only issue mentioning the guest users is:

"The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps."

So, I believe the question refers to the invitation / registration part of the Guest users, not reviewing their access...

The purpose is to offload the Helpdesk Admins from managing all guest access registrations, not reviewing stale accounts.

So the answer "D. Modify the External collaboration settings." fits better to the purpose.

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure#configure-settings-in-the-portal>

(See Enable guest self-service sign up via user flows & Member users and users assigned to specific admin roles can invite guest users including guests with member permissions)

upvoted 5 times

✉  **cgonIT** 1 month, 2 weeks ago

Agree with you.

upvoted 2 times

✉  **cgonIT** Most Recent 1 month, 2 weeks ago

**Selected Answer: D**

Correct answer: D. Modify the External collaboration settings.

upvoted 2 times

✉  **b233f0a** 5 months, 1 week ago

**Selected Answer: C**

Could be interpreted as either C or D. "The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps."

C - "Configure the Access reviews settings" will enable existing Guest users to determine if they still need access, but this will not invite new users.  
D - "Modify the External collaboration settings" will allow Guest invite options, but does not help manage the existing users access.

The key part of this question seems to be "too much time provisioning internal and guest access". External Collaboration settings does not help with managing Internal users, so I vote for C

upvoted 1 times

✉  **wooyourdaddy** 10 months, 1 week ago

I believe the given answer is correct:

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/clean-up-stale-guest-accounts>

As users collaborate with external partners, it's possible that many guest accounts get created in Azure Active Directory (Azure AD) tenants over time. When collaboration ends and the users no longer access your tenant, the guest accounts may become stale. Admins can use Access Reviews to automatically review inactive guest users and block them from signing in, and later, delete them from the directory.

upvoted 4 times

✉  **AMDF** 11 months, 3 weeks ago

**Selected Answer: D**

D is correct

upvoted 1 times

✉  **ACSC** 1 year ago

**Selected Answer: D**

Azure AD / External Identities / External collaboration settings / Guest invite settings

upvoted 3 times

✉  **Jawad1462** 1 year, 1 month ago

**Selected Answer: D**

Is the correct answer

upvoted 1 times

✉  **DeepMoon** 1 year, 1 month ago

After more consideration I still think it is D.

Here is the link that gets to the point:

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure#configure-settings-in-the-portal>

You can add enable 'Guest Inviter' role. But you cannot enable self-service role for 'Office 365' apps. So far, that is only available for apps you build. See here

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/self-service-sign-up-user-flow#enable-self-service-sign-up-for-your-tenant>

upvoted 1 times

✉  **Faheem2020** 1 year, 2 months ago

The issue here is "The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps"

Looks like D : 'Modify the External Collaboration Settings' to me where you can enable guest users self service flow

upvoted 3 times

✉  **dejo** 1 year, 2 months ago

...but "You can associate user flows with apps built by your organization. User flows can't be used for Microsoft apps, like SharePoint or Teams."  
<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/self-service-sign-up-user-flow#enable-self-service-sign-up-for-your-tenant>

So I don't see a correct answer here :D

upvoted 2 times

✉  **DeepMoon** 1 year, 2 months ago

I would think the guest user issue that needs resolving would be: "Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days". If that is the case answer should be D.

upvoted 2 times

✉  **Hot\_156** 1 year, 2 months ago

You identify the issue, so how do you remove the access automatically by changing External Collaboration settings? The answer is C "Access review"

upvoted 6 times

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

店铺：专业认证88

## Introductory Info

Case Study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named **Contoso\_Resources**. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

▪

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

#### Question

You need to sync the ADatum users. The solution must meet the technical requirements.

What should you do?

- A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.
- B. From PowerShell, run Set-ADSyncScheduler.
- C. From PowerShell, run Start-ADSyncSyncCycle.
- D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

#### Correct Answer: A

You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

*Community vote distribution*

A (100%)

 DeepMoon Highly Voted 1 year, 1 month ago

Answer A is correct.

The following link gets to the point.

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

Gives more info.

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis#azure-ad-connect-sync-topics>  
upvoted 8 times

 Gesbie Most Recent 4 months, 3 weeks ago

On exam 12th July 2023

upvoted 2 times

 dule27 5 months ago

**Selected Answer: A**

A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.

upvoted 2 times

 JN\_311 5 months, 2 weeks ago

**Selected Answer: A**

Answer A. Thats an Easy one

upvoted 1 times

 kmk\_01 7 months, 3 weeks ago

**Selected Answer: A**

Yes it's A.

upvoted 1 times

**Topic 12 - Testlet 8**

## Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

#### Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

#### Question

You need to configure the detection of multi-staged attacks to meet the monitoring requirements.

What should you do?

- A. Customize the Microsoft Sentinel rule logic.
- B. Create a workbook.
- C. Add Microsoft Sentinel data connectors.
- D. Add an Microsoft Sentinel playbook.

#### Correct Answer: A

*Community vote distribution*

A (100%)

 **DeepMoon** Highly Voted 1 year, 1 month ago

Given Answer A is correct. Because it is the most specific thing you can do from the given choices (A, C & D).  
<https://learn.microsoft.com/en-us/azure/sentinel/configure-fusion-rules#configure-fusion-rules>

upvoted 6 times

 **dule27** Most Recent 5 months ago

Selected Answer: A

A. Customize the Microsoft Sentinel rule logic.

upvoted 1 times

 **ACSC** 1 year ago

Selected Answer: A

<https://learn.microsoft.com/en-us/azure/sentinel/configure-fusion-rules#configure-fusion-rules>

upvoted 2 times

 **zman\_83** 1 year, 2 months ago

Hmm, why not

C. Add Microsoft Sentinel data connectors.?

upvoted 3 times

 **LHADUK** 1 year ago

connectors are already added, it's listed in existing environment:

"The subscription contains an Azure Sentinel instance that uses the AAD connector and the Office 365 connector."

upvoted 5 times

## Introductory Info

Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

Use custom programs for Identity Governance.

Ensure that User1 can create enterprise applications in Azure AD.

Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to a

Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

Implement multi-factor authentication (MFA) for all Litware users by using conditional access policies.

Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.

▪

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

#### Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

### Question

You need to track application access assignments by using Identity Governance. The solution must meet the delegation requirements.

What should you do first?

- A. Modify the User consent settings for the enterprise applications.
- B. Create a catalog.
- C. Create a program.
- D. Modify the Admin consent requests settings for the enterprise applications.

#### Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview>

Community vote distribution

C (60%)      B (40%)

 **zakyntos** Highly Voted 2 years, 2 months ago

Should be C. Requirement is for program which is a part of Access Reviews. Catalog is for Access Packages  
upvoted 19 times

 **RylandN** Highly Voted 1 year, 6 months ago

Where are the rest of the questions?  
upvoted 9 times

 **martonne** Most Recent 2 months ago

To track application access assignments by using Identity Governance in Microsoft Azure while meeting delegation requirements, you should start by creating a catalog. Therefore, option B, "Create a catalog," is the correct first step in this scenario.

Creating a catalog is typically the first step in setting up Identity Governance to manage access to applications and resources. It allows you to define and organize your resources, including enterprise applications, and is a foundational element in the Identity Governance framework.

Options A, C, and D do not directly address the initial setup of Identity Governance and tracking application access assignments, so they are not the first steps in this context.

upvoted 4 times

 **JCkD4Ni3L** 1 month, 4 weeks ago

martonne is right.  
upvoted 1 times

 **ServerBrain** 3 months ago

**Selected Answer: B**

Correct answer is B.

I can't see how C is being substantiated in these comments. No links were provided.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview#how-do-i-control-who-gets-access>  
upvoted 2 times

 **marsot** 4 months, 1 week ago

**Selected Answer: C**

Catalog is for Access Packages.  
For Access reviews, we are using Programs.  
Program is a 'container' that helps us to group reviews logically (for departments, projects, etc.)  
upvoted 2 times

 **hw121693** 4 months, 4 weeks ago

What is meant by creating a program? What program?  
upvoted 3 times

 **dule27** 5 months ago

**Selected Answer: C**

C. Create a program.  
upvoted 2 times

 **cris\_exam** 8 months, 1 week ago

So I have been reading about this topic for the past 30 min and still can't really decide which is better - catalog or program. haha :))

So I asked ChatGPT few questions forming an answer and this is what it said about this topic - hence going with the program option.

"If you want to track application access and manage privileged access in a more controlled and auditable way, creating a program in Azure AD Privileged Identity Management (PIM) would be a better option than creating a catalog

So, if your main goal is to track application access and manage privileged access in a more secure and auditable way, creating a program in Azure AD PIM would be the better choice."

upvoted 3 times

 **Taigr** 9 months, 3 weeks ago

**Selected Answer: B**

In the Azure portal, select Azure Active Directory and then select Identity Governance. In the left menu, select Access packages and then open the access package. Select Assignments to see a list of active assignments. Select a specific assignment to see more details.

I think that it is Catalog

In the request is mentioned directly Identity Governance. In IG you have in Entitlement management options to set up :  
Access packages  
Catalogs  
Connected applications  
...

In catalogs you can have Access packages and member of access package can be applications.

upvoted 3 times

 **Nazir97** 11 months ago

**Selected Answer: B**

Right answer is B  
upvoted 1 times

 **shaden2000** 12 months ago

**Selected Answer: B**

I went for B aswell.  
You must group those applications in a catalog and can manage access and it meets the delegation pre.  
<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create>  
upvoted 2 times

 **ACSC** 1 year ago

**Selected Answer: C**

Requirement: Use custom programs for Identity Governance.  
Need: You need to track application access assignments by using Identity Governance.

By default, Access reviews are organized into Programs, which you will find listed under the relevant tab on the left. Programs are just containers for the actual review controls, they don't serve any other purpose than to help you organize the reviews. You can select the Default Program, or just as easily create a new Program by clicking the Add program button and providing name and description.

upvoted 3 times

 **DeepMoon** 1 year, 1 month ago

I am confused. Can somebody explain to me what a program is?

Here is the root of the docs relating Identity Governance. Nothing in the next subpages come up with the search term 'Program'. Or creating a program.  
<https://learn.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview>

Nothing here under Entitlement Management talks about a program either.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview>

Nor is the word program come up here in setting up access reviews.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/manage-access-review>

Norr here where it talks about access reviews

<https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

upvoted 4 times

 **zaspamer** 1 year, 4 months ago

**Selected Answer: C**

The Answer is C - Programs as stated they are requiring the use of custom programs  
Litware identifies the following delegation requirements:  
Use custom programs for Identity Governance.

upvoted 3 times

 **rachee** 1 year, 4 months ago

B. I think it is the wording of the question that is confusing. "You need to track application access assignments by using..." The "application assignments" being a single identity; the access packages would identify the assignments which have to be in a catalog. For those thinking "C" because it is closest to "access reviews" , I think you are reading "application" and "assignments" as separate identities.

upvoted 3 times

 **sapien45** 1 year, 5 months ago

B

The question insists on Delegation

A container of related resources and access packages. Catalogs are used for delegation, so that non-administrators can create their own access packages. Catalog owners can add resources they own to a catalog.

upvoted 2 times

 **RandomNickname** 1 year, 5 months ago

**Selected Answer: B**

Given answer is correct.

B:

Information is provided in the link;

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview>

With information from the link;

"An access package is always contained in a catalog. You would create a new access package for a scenario in which users need to request access."

upvoted 2 times