Question #1 *Topic 1*

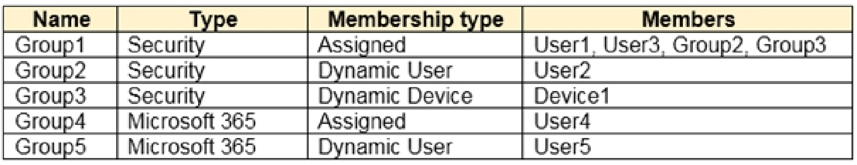
You have an Azure Active Directory (Azure AD) tenant that contains the following objects:

✑ 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

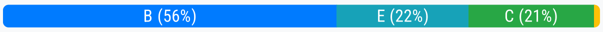
E. Group1, Group2, Group4, and Group5 only

Suggested Answer: *C*

Reference:

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

Community vote distribution



sezza_blunt Highly Voted 3 years, 6 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 87 times

Acbrownit 3 months, 3 weeks ago

The "SecurityEnabled" attribute isn't set to true by default, and devices can only be licensed with the Desktop App license. So Group 1 and 2 are the "most correct" answer and MS likes to put in these "most best good answer" questions because they think they demonstrate a more thorough knowledge base for test takers.

upvoted 1 times

klayytech 8 months, 2 weeks ago

Microsoft does allow licenses to be assigned to device groups. This is particularly useful for devices that are shared by many users, such as in a classroom or a kiosk. When a device has a license, anyone who uses that device can use Microsoft 365 Apps for enterprise2

https://learn.microsoft.com/en-us/deployoffice/device-based-licensing

upvoted 2 times

Acbrownit 3 months, 3 weeks ago

The apps for enterprise license covers only the Desktop installed apps for Office. The question here is asking specifically about E5 licenses, as rick mentioned, which means you have to assign the license to users.

upvoted 1 times

rick_leye2 4 months ago

Yes but the license here is MS 365 E5

upvoted 1 times

tamisius 3 years ago

I have tried as well and could add all the groups. The answer is B. We don't have much informations so it is difficult...

upvoted 3 times

TJ001 2 years, 11 months ago

Agree - the licenses can be applied to all groups created in Azure AD via portal.

upvoted 3 times

Beitran Highly Voted 👍 3 years, 8 months ago

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

upvoted 21 times

Shaz 3 years, 8 months ago

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

upvoted 7 times

Borbz 3 years, 5 months ago

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

upvoted 6 times

researched_answer_boi 3 months, 1 week 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

Bulldozzer 2 years, 10 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 3 years, 2 months 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

ATimTimm Most Recent ⏲ 3 weeks, 2 days ago

Selected Answer: E

You cannot assign license to Dynamic Device group.

upvoted 1 times

Mole857 1 month, 2 weeks ago

The Answer is E - you can't allocate a license to a device

upvoted 1 times

Sakraf 2 months ago

Selected Answer: E

If you have security groups, mail enabled groups, or Microsoft 365 groups, you can assign or unassign licenses for those groups on the Licenses page in the Microsoft 365 admin center. We refer to this as group-based licensing.

https://learn.microsoft.com/en-us/microsoft-365/admin/manage/manage-group-licenses?view=o365-worldwide

upvoted 2 times

BRZSZCL 2 months ago

For those getting confused about Group 3. I have created a Security Group 'Dynamic Device' type and lisence attached (Microsoft 365 E5) to it, so answer B is correct, we could attached the E5 lisence directly to all groups

upvoted 3 times

aocferreira 2 months, 3 weeks ago

I've tested this and the most correct answer available should be C (Group1 and Group2 only).

Even though MS documentation still says that licenses can be assigned to M365 groups if securityEnabled = True, it seems that's not the case anymore. I've created 2 M365 groups in Entra portal and i've confirmed fro MS Graph that these groups have the flag securityEnabled = true. However, from M365 admin centre, it's not possible to assign the licenses to these groups -> this means Group4 and Group5 are excluded.

Regarding Group3, it's actually possible to assign the E5 license to a group that contains a device, even though it doesn't make much sense because this is targeted for users.

Based on this, if there was an answer with Group1 Group2 and Group3 I would say it was the correct one.

As we don't have it, Group1 and 2 should be correct answer -> C

upvoted 1 times

RandomNickname 3 months, 1 week ago

Selected Answer: B

I'm with the B camp, however there's not enough imformation here.
But, any group which is mail enable and created in AZAD has securityEnabled: true be default, allowing licenses to be added the the required groups.

See:
https://docs.microsoft.com/en-us/graph/api/group-post-groups?view=graph-rest-1.0&tabs=http#request-body

Security and O365 groups can have group based licenses assigned, see (under, Limitations and known issues):
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced

You can assign enterprise license to devices, see:
https://docs.microsoft.com/en-us/microsoft-365/commerce/licenses/manage-licenses-for-devices?view=o365-worldwide

upvoted 4 times

w00t 3 months, 1 week ago

Selected Answer: B

Answer should be "B".
The question is simply asking "WHICH OF THESE GROUPS CAN BE ASSIGNED A LICENSE?"
The answer, is ALL OF THEM.
It doesn't matter if a Device Group can't USE an E5 license. That's not the question. The question is can the group be assigned the license. The answer is yes, yes it can.

I tested in my lab env with E5 licensing.

ALL GROUPS CAN BE ASSIGNED AN E5 LICENSE, regardless of if that license will be used properly. Of course, a device can't be assigned E5 licensing. That license wouldn't get used if assigned to a Device Group, BUT, you can still assign it to that group.

B.

upvoted 2 times

geobarou 3 months, 1 week ago

Selected Answer: B

You can create a SG having devices, groups and users. So you can add a license to this group. AAD does not know if a SG has devices, groups or users. Of course the license will assigned only to the users of this group. So Group 3 is eligible. M365 groups have only users. Both groups can be assigned with a license.

upvoted 2 times

Hot_156 3 months, 1 week ago

Selected Answer: B

The Membership Type and Members are just to confuse all of you. The question is "To which groups can you assign a Microsoft Office 365 Enterprise E5 license directly?" if you test this, you can assign this to any group created in Azure even groups with Azure AD roles set to yes

upvoted 1 times

Taigr 3 months, 1 week ago

Selected Answer: C

This qeuestion is one of Microsoft examples and right answer there is C. But this example question is 2 years old, so who knows....

upvoted 1 times

⊟ **Garito** 3 months, 1 week ago

Selected Answer: C

The same question appears in offical SC-300 Measureup practice exam question 22 and answer is: Group 1 and group 2 only.

Offical explanations:

You can not assign licens to group 3 becvause it is a device group. You can not assign licenses to device groups.

You can not assign licences to group 4 and group 5. YOu can not assign licences to Microsoft 365 groups.

upvoted 7 times

⊟ **Holii** 1 year, 7 months ago

If this is true, then we are missing the crucial information that these groups were created in the M365 Admin Portal.

If you create the M365 Group in the Azure AD portal, they will have the necessary flag permissions to be able to directly assign licenses.

upvoted 2 times

⊟ **flimarc** 3 months, 1 week ago

E

You can assign Azure AD P1 licenses to Group1, Group2, and Group 4 only. You can assign licenses to security groups containing users only or containing users and other groups. This includes both assigned and dynamic user groups. You can also assign licenses to Microsoft 365 Groups. You cannot assign Azure AD P1 licenses to Group3 because it is a device group. You cannot assign licenses to device groups.

upvoted 2 times

⊟ **sherifhamed** 3 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 3 times

⊟ **Davidf** 3 months, 1 week ago

Measure up have a near identical question

Group 1 - Security - assigned user
Group 2 - Security - dynamic user
Group 3 - Security - dynamic device
Group 4 - M365 - dynamic user

Which groups can you assigned Azure AD Premium P1 licenses?

Answer = Group 1 and 2 only

Reasoning - You can assign licenses to security groups containing users only or user and other group. This includes both assigned and dynamic user groups.

You cannot assign licenses to group 3 as it is device group.

You cannot assign a license to group 4. You cannot assign licenses to M365 groups.

Take what you will from that.... I will probably go with them but leave a comment on the question if it comes up.

upvoted 7 times

⊟ **melatocaroca** 3 months, 1 week ago

You can use group-based licensing with any security group, which means it can be combined with Azure AD dynamic groups.
Multiple licenses for the same product can overlap, and they result in all enabled services being applied to the user
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.
The feature can only be used with security groups, and Microsoft 365 groups that have securityEnabled=TRUE.
The Microsoft 365 admin center does not currently support group-based licensing. If a user inherits a license from a group, this license appears in the Office admin portal as a regular user license. If you try to modify that license or try to remove the license, the portal returns an error message. Inherited group licenses cannot be modified directly on a use
So, you need to use PowerShell to change Normal Office 365 group to Office 365 security enabled
#Elevate Office 365 group to security group
Set-AzureADGroup -ObjectId XXX -SecurityEnabled:$true

upvoted 1 times

⊟ **melatocaroca** 3 years, 5 months ago

You can choose what to assume, but because default is not enabled, my assumption is to discard Office 365, because they ask assign a Microsoft Office 365 Enterprise E5 license directly, and you need to commit a previous step that is set SecurityEnabled:$true
Security groups can contain users or devices. Creating a security group for devices can be used with mobile device management services, such as Intune.
If you have Microsoft 365 Apps for enterprise (device) or Microsoft 365 Apps for Education (device), you can assign licenses to devices by using Azure AD groups.
When a device has a license, anyone who uses that device can use Microsoft 365 Apps for enterprise (previously named Office 365 ProPlus).
You can assume that device will be assigned with a license, but there is no option, for Group1 and Group2 and Group3 only
So, IMHO given answer C. Group1 and Group2 only

upvoted 2 times

⊟ **melatocaroca** 3 years, 5 months ago

The trick is directly, not if can be used or not not if can be used or not to assign licenses, you just assume defaults, Office 365 group need previous work and groups with devices as well

upvoted 1 times

Question #2 *Topic 1*

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

Suggested 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 3 years, 6 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 31 times

avdan16 Highly Voted 11 months, 1 week ago

I assume that when the exam gets updates, the answer will be Update-MgPolicyAuthorizationPolicy. Msonline is becoming obsolete.

upvoted 8 times

Labelfree Most Recent 2 months ago

To prevent users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services, you should use the Set-MsolCompanySettings cmdlet. This cmdlet allows you to configure various settings for your organization, including disabling self-service sign-up.

Here's an example of how you can use it:

Set-MsolCompanySettings -AllowAdHocSubscriptions $false

This command disables the ability for users to sign up for self-service subscriptions1.

upvoted 1 times

RahulX 6 months, 3 weeks ago

Correct Ans: A. Set-MsolCompanySettings Most Voted

upvoted 1 times

dc864d4 7 months ago

MSOL is EOL

upvoted 1 times

RahulX 1 year, 1 month ago

A. Set-MsolCompanySettings.

upvoted 2 times

sherifhamed 1 year, 3 months 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 1 year, 5 months ago

Selected Answer: A

A. Set-MsolCompanySettings

upvoted 1 times

dule27 1 year, 7 months ago

Selected Answer: A

A. Set-MsolCompanySettings

upvoted 1 times

francescoc 1 year, 9 months ago

Selected Answer: A

The correct answer is A

upvoted 1 times

jack987 2 years ago

The correct answer is A.

upvoted 1 times

[Removed] 2 years 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:~:text=How%20do%20the%20controls%20work%20together%3F

upvoted 1 times

KrisDeb 2 years, 1 month ago

Selected Answer: A

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

upvoted 1 times

clem24 2 years, 7 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 2 years, 8 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

xurxosan 2 years, 10 months ago

Selected Answer: A

A is correct

upvoted 2 times

stromnessian 2 years, 10 months ago

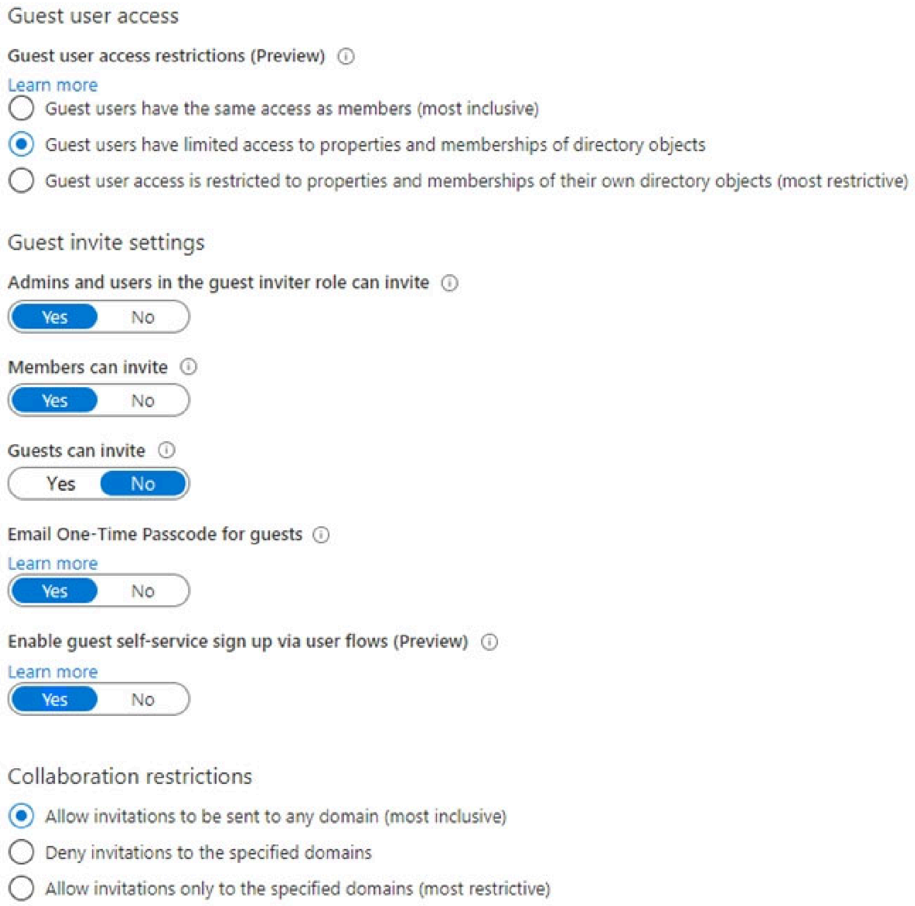
Selected Answer: A

A is correct.

upvoted 2 times

Question #3 *Topic 1*

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

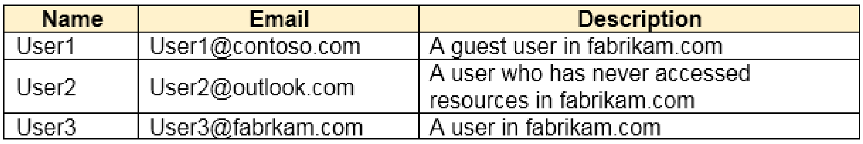
Collaboration restrictions

● 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@fabrkam.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

Suggested Answer: *A*

Reference:

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

Community vote distribution

B (53%) A (41%) 6%

⊟ **Eltooth** Highly Voted 3 years, 7 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 85 times

topipe 3 weeks, 1 day ago
Yay! thank you! Because NONE of the three users listed here would receive a passcode according to
https://docs.google.com/document/d/1nCz7jJ9Mu-J_LwfwUmeoPjzrNRZgeyfaeAACSzrBa9k
User1 has an existing guest account, so no passcode. User2 has a Microsoft account, so no passcode. User3 is a tenant user, so no passcode.
But a NEW user with a personal Gmail account WOULD receive a passcode!
upvoted 1 times

klayytech 8 months, 2 weeks ago
He asking about who will sign with Passcod he not asking about MFA OTP
Passcode only allows for non-entra email users and non-Microsoft accounts like Gmail
upvoted 4 times

Alcpt 8 months, 3 weeks ago
the answer is A because the one-time passcode authentication is exactly that - it is required only once to authenticate an external account onto your EntraID "forever". There no two-time passcodes required.
This is only to authenticate the external account onto your Entra. Its not a repetitive invitation.
"Even the older \ legacy guest users who redeemed an invitation before email one-time passcode was enabled will continue to use their same authentication method.
upvoted 3 times

pheb 3 years, 4 months ago
idk why this has so many upvotes. it cleary 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 45 times

RahulX 6 months, 3 weeks ago
Correct I have done the RnD.
upvoted 1 times

JN_311 1 year, 6 months 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 6 times

Kiano 2 years, 7 months ago
Just because you have an Outlook.com account does not mean you have a Microsoft account. A Microsoft account is he account you associate with microsoft services at the time of need. It can be a gmail accoount or any kind of private account. I believe the ight answer is A, Users2 only. Exactly as explianed by Eltooth
upvoted 5 times

itismadu 2 years 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
upvoted 3 times

scotty_123 Highly Voted 2 years, 10 months ago
In exam today(23/2/22) this question was changed slightly
"User3 : user3@gmail.com : personal gmail account"
Options were,
(a) user 1 only
(b) user 2 only
(c) user 3 only

(d) user1 and user2 only

(e) user1, user2 and user3

upvoted 16 times

SnottyPudding 2 years, 9 months ago

Yay! thank you! Because NONE of the three users listed here would receive a passcode according to https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode. User1 has an existing guest account, so no passcode. User2 has a Microsoft account, so no passcode. User3 is a tenant user, so no passcode. But a NEW user with a personal Gmail account WOULD receive a passcode!

upvoted 5 times

test123123 Most Recent 1 week, 4 days ago

Selected Answer: B

The "Email One-Time Passcode for guests" feature in Microsoft Entra (formerly Azure AD) allows external users (guests) to authenticate using a temporary passcode sent to their email.

Temporary Passcode: When a guest user tries to access your resources, they can request a one-time passcode, which is sent to their email address. They use this passcode to complete the sign-in process.

Sign-In Process: During sign-in, the guest user selects the option to sign in with a one-time passcode. They receive the passcode via email and enter it to gain access.

Enabling the Feature

Sign In: Log in to the Microsoft Entra admin center as an Authentication Policy Administrator.

Navigate: Go to Identity > External Identities > All identity providers.

Configure: On the Built-in tab, next to email one-time passcode, select Configured.

Enable: Ensure the toggle is set to Yes and click Save.

upvoted 1 times

Frank9020 2 weeks, 3 days ago

Selected Answer: A

User1: Will not receive a new OTP since they have logged in before.

User2: Will receive a passcode because they have never accessed resources in fabrikam.com.

User3: Will not receive a passcode as they are an internal user.

upvoted 1 times

photon99 2 weeks, 5 days ago

User 2 Only. Read the doc: 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

upvoted 1 times

survivor 1 month, 1 week ago

Selected Answer: B

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.

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.

User 1, other identity provider unkonown

User 2, Microsoft Account

User 3 Microsoft Entra

upvoted 2 times

Labelfree 2 months ago

The current "Most Voted" answer is incorrect. With these settings, the behavior for each user would be as follows:

User1@contoso.com: Since User1 is already a guest user in fabrikam.com, they will not need a passcode.

user2@outlook.com: As User2 has never accessed resources in fabrikam.com, they will be emailed a one-time passcode to authenticate.

user3@fabrikam.com: Being an internal user of fabrikam.com, User3 will not need a passcode.

Therefore, the correct answer remains:

A. User2 only

These settings confirm that new external users (like User2) will receive a one-time passcode for authentication, while existing guest users (like User1) and internal users (like User3) will not.

upvoted 4 times

⊟ **AlexBrazil** 2 months ago

Selected Answer: A

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.
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

⊟ **AlexBrazil** 2 months ago

Selected Answer: A

User 1 is already a registered guest user in fabrikam.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.

upvoted 1 times

⊟ **BRZSZCL** 2 months, 2 weeks ago

User 2 only is correct because he is not in the company fabrikam, not even as a guest.

upvoted 1 times

⊟ **Olami** 2 months, 3 weeks ago

To the best of my knowledge,
User 3 is A USER in the fabrikam domain so will not receive the OTP
User 2 is a user who is NOT an existing guest user in fabrikam.com, nor has accessed fabrikam resources (A new guest) but meets the "any domain" category will get the invite with the OTP.
User 1 is ALREADY A GUEST USER in fabrikam.com, so will continue to use its access without requiring an OTP.
User 2 - A is the answer
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

⊟ **kkrGmail** 3 months, 1 week ago

Selected Answer: C

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

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

Open for discussion.

upvoted 2 times

⊟ **geggio** 5 months, 4 weeks ago

B
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.
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 1 times

⊟ **RahulX** 6 months, 3 weeks ago
Correct Ans:

A. User2 only
upvoted 1 times

⊟ **9711d59** 7 months, 2 weeks ago
The email one-time passcode feature is now turned on by default for all new tenants and for any existing tenants where you haven't explicitly turned it off. This feature provides a seamless fallback authentication method for your guest users. If you don't want to use this feature, you can disable it, in which case users will be prompted to create a Microsoft account. I vote for A - user1
upvoted 1 times

⊟ **Nobody2002** 7 months, 2 weeks ago
There is no right answer.

User1 - Is already a quest user in fabrikan.com so they will not receive an OTP:
"Guest users who redeemed an invitation before email one-time passcode was enabled will continue to use their same authentication method."
User2 - This is an outlook account which is naturally seen as a Microsoft account without registering it as such. User will be prompted to just register with their Microsoft account and not have the option of OTP:
"Accounts such as an outlook.com, hotmail.com, live.com, or msn.com account, are managed by Microsoft, and therefore already considered Microsoft accounts."

User3 - this is just a normal user, not a quest user so they will not receive anything.

Source: https://learn.microsoft.com/en-us/entra/external-id/one-time-passcode
And a quick google search if outlook accounts are automatically Microsoft accounts which they are.

Correct answer:
E. None
upvoted 1 times

⊟ **klayytech** 8 months, 3 weeks ago
Selected Answer: B
passcode apply only to None Microsoft Entra or Microsoft account like (outlook or MSN)
upvoted 1 times

Question #4 *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 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

Suggested 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 3 years, 3 months ago
In the exam the cmdlet was Set-MsolUserLicense, the right one!
upvoted 39 times

photon99 2 weeks, 6 days ago
MSOnline is deprecated in favour of Set-MgUserLicense https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users.actions/set-mguserlicense?view=graph-powershell-1.0
upvoted 1 times

TJ001 2 years, 11 months ago
just note it only works with Windows Power shell and not Powershell core..
upvoted 2 times

Beitran Highly Voted 3 years, 8 months ago
Correct!
upvoted 12 times

Frank9020 Most Recent 2 weeks, 3 days ago
Selected Answer: C
To remove the Office 365 Enterprise E3 licenses from the users with the least amount of administrative effort, you should use:

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

This option allows you to manage licenses in bulk, making it easier to remove the E3 licenses from all 2,500 users efficiently
upvoted 1 times

photon99 2 weeks, 6 days ago
Unfortunately they have included in exam but the documnetation is still incomplete for powesrhell Module : https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users.actions/set-mguserlicense?view=graph-powershell-1.0
upvoted 1 times

ross9876986 4 months ago

since the interface lets you do only 20 at a time, a script is needed thus Set-MsolUserLicense or Set-AzureAdUserLicense

upvoted 1 times

RahulX 10 months, 3 weeks ago

B. the Set-AzureAdUser cmdlet.

https://learn.microsoft.com/en-us/powershell/module/azuread/set-azureaduserlicense?view=azureadps-2.0

upvoted 1 times

onelove01 1 year ago

Selected Answer: C

correct answer is C

upvoted 1 times

lojlkdnfvlirez 1 year ago

C. the Licenses blade in the Azure Active Directory admin center allows you to assign or unassign licenses for up to 20 users at a time, not 2,500 users

upvoted 1 times

lojlkdnfvlirez 1 year ago

The correct answer is B. the Set-AzureAdUser cmdlet.

The Set-AzureAdUser cmdlet allows you to modify the properties of a user in Azure Active Directory, including their assigned licenses. You can use this cmdlet to remove the Office 365 Enterprise E3 licenses from the users in bulk, by using a text file that contains the user principal names of the users

upvoted 2 times

EmnCours 1 year, 5 months ago

Selected Answer: C

Correct Answer: C

upvoted 1 times

dule27 1 year, 6 months ago

Selected Answer: C

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

upvoted 1 times

Faheem2020 2 years, 3 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 2 years, 8 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 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** 2 years, 5 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 2 times

Sh1rub10 2 years, 9 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** 2 years, 9 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** 2 years, 10 months ago

No correct answer here.

upvoted 1 times

⊟ **TP447** 2 years, 12 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

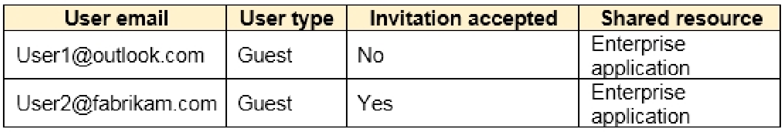
Question #5 *Topic 1*

HOTSPOT -

You have a Microsoft 365 tenant named contoso.com.

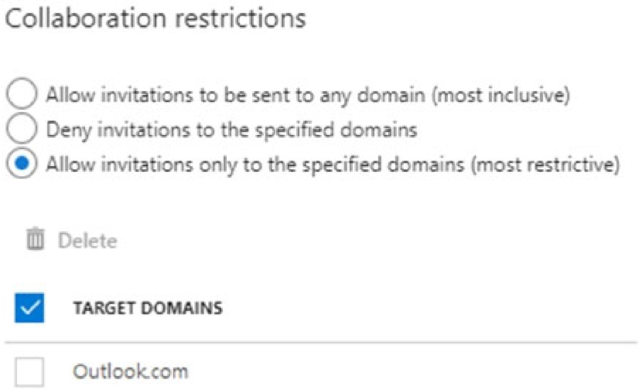
Guest user access is enabled.

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)

☑ TARGET DOMAINS

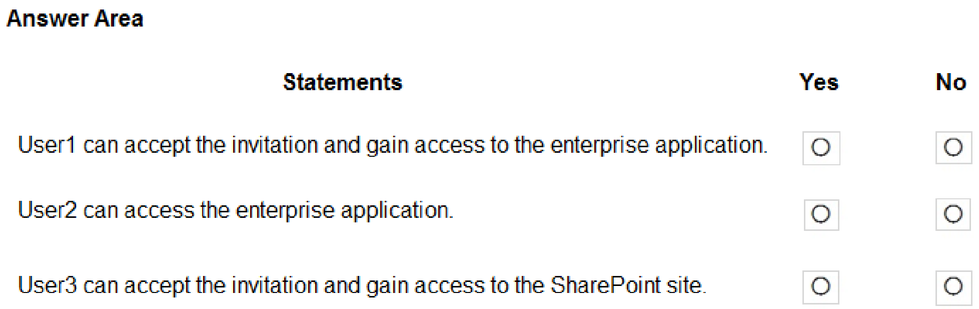
☐ Outlook.com

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.

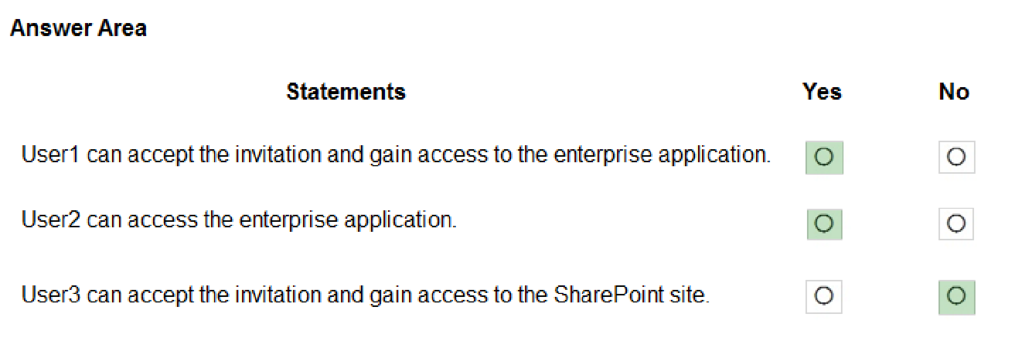
Hot Area:



Answer Area

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	○	○
User2 can access the enterprise application.	○	○
User3 can accept the invitation and gain access to the SharePoint site.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	[✓ ○]	○
User2 can access the enterprise application.	[✓ ○]	○
User3 can accept the invitation and gain access to the SharePoint site.	○	[✓ ○]

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 👍 3 years, 8 months ago

Yes/Yes/No - @Reyrain - 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 54 times

⊟ **reddevil01** 3 months, 1 week 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 to user.

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 12 times

⊟ **TJ001** 2 years, 11 months ago

very straight forward question and answer

upvoted 5 times

⊟ **f2bf85a** 1 year, 8 months 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

⊟ **m4rv1n** Most Recent ⊙ 3 months, 1 week 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** 1 year, 8 months 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 questioni 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 1 year, 8 months ago

Correction: Just tested the exact scenario, and althouth 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

HartMS 8 months, 3 weeks ago

Answer: YYN

upvoted 1 times

RahulX 10 months, 3 weeks ago

Ans: Yes, because only user1@outlook.com will received the invitation as per ext collaboration.
Ans: Yes, User2 already accept the invitation to access the enterprise the app.
Ans: User3 is not mentioned in user list and domain is also not there.

upvoted 1 times

EmnCours 1 year, 4 months ago

YES
YES
No

upvoted 1 times

dule27 1 year, 7 months ago

YES
YES
NO

upvoted 1 times

JCkD4Ni3L 1 year, 7 months ago

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

upvoted 2 times

JunetGoyal 1 year, 8 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

itannajones 1 year, 9 months 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 1 year, 11 months 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 2 years ago

Yes, Yes, No

Checked in my tenant

upvoted 4 times

BTL_Happy 2 years, 1 month ago

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

upvoted 1 times

ali_pin 2 years, 6 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

DemekeAd 2 years, 8 months ago

YES

YES

No

upvoted 2 times

janshal 2 years, 8 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

LynaSophia 2 years, 9 months ago

what is the right answer?

upvoted 1 times

Sammy786 2 years, 11 months ago

How can user 2 access the enterprise application when @fabrikam.com is not a target domain?

upvoted 1 times

> **stromnessian** 2 years, 10 months ago
>
> Because the invitation has already been accepted.
>
> upvoted 2 times

Question #6 *Topic 1*

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

Suggested 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 👍 3 years, 8 months ago
correct
upvoted 16 times

AlexBrazil Most Recent 🕒 2 months ago
Selected Answer: AB
According to MS docs in https://learn.microsoft.com/en-us/entra/external-id/tutorial-bulk-invite, open the .csv template and add a line for each guest user containing:

1. Email address to invite - the user to whom you want to send an invitation.
2. Redirection url - the URL to which the invited user is forwarded after accepting the invitation.

upvoted 2 times

sherifhamed 3 months, 1 week 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 4 times

RahulX 6 months, 3 weeks ago
Correct Ans:
A. email address
B. redirection URL
upvoted 1 times

grimrodd 7 months, 3 weeks ago
Selected Answer: AB
correct
upvoted 1 times

RahulX 10 months, 3 weeks ago

A. email address

B. redirection URL

upvoted 1 times

⊟ **RahulX** 1 year, 1 month ago

A. email address

B. redirection URL

upvoted 1 times

⊟ **EmnCours** 1 year, 4 months ago

Selected Answer: AB

A. email address

B. redirection URL

upvoted 1 times

⊟ **dule27** 1 year, 7 months ago

Selected Answer: AB

A. email address

B. redirection URL

upvoted 1 times

⊟ **ShoaibPKDXB** 1 year, 7 months ago

Selected Answer: AB

AB are correct.

upvoted 1 times

⊟ **jojoseph** 1 year, 11 months ago

Selected Answer: AB

correct

upvoted 1 times

⊟ **Jhill777** 2 years, 1 month ago

Selected Answer: AB

AB. Column one is Email address to invite [inviteeEmail] Required

Column 2 is Redirection url [inviteRedirectURL] Required

upvoted 1 times

⊟ **trxs1** 2 years, 5 months ago

Selected Answer: AB

correct

upvoted 1 times

⊟ **gwerin** 2 years, 10 months ago

Selected Answer: AB

Correct

upvoted 1 times

⊟ **GPerez73** 2 years, 11 months ago

Selected Answer: AB

Correct. Just download the template and you can see it

upvoted 1 times

⊟ **Eltooth** 3 years, 7 months ago

Correct.

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

Required values are:

Email address to invite - the user who will receive an invitation

Redirection url - the URL to which the invited user is forwarded after accepting the invitation. If you want to forward the user to the My Apps page, you must change this value to https://myapps.microsoft.com or https://myapplications.microsoft.com.

upvoted 4 times

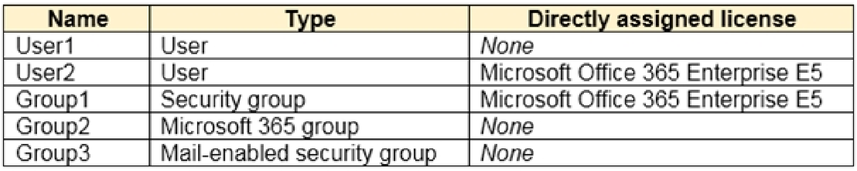
⊟ **B0** 3 years, 8 months ago

correct

upvoted 4 times

Question #7 Topic 1

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	*None*
User2	User	Microsoft Office 365 Enterprise E5
Group1	Security group	Microsoft Office 365 Enterprise E5
Group2	Microsoft 365 group	*None*
Group3	Mail-enabled security group	*None*

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

Suggested Answer: *E*

Reference:

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

Community vote distribution

E (71%) D (29%)

Cheguevarax Highly Voted 3 years, 7 months ago

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

upvoted 84 times

loukyexamtopic 5 months, 1 week ago

did you tested this in 365 admin centre or AAD

upvoted 1 times

hhaywood 3 years, 7 months ago

Agreed, also tested. However I found you can assign 'equipment users' e.g. Projectors with no license - odd one.

upvoted 4 times

lime568 2 years, 9 months ago

because the equipments have a mailbox

upvoted 4 times

Arjanussie 1 year, 10 months ago

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

upvoted 1 times

Discuss4certi 3 years, 3 months ago

I do not agree. I also tested this. Indeed if you look at it from the groups tab you cannot find the user in the list to add it to the MESG. But if you go to the user you can add a membership to the group.

upvoted 6 times

007Ali 2 years, 11 months ago

On a Security Group, going to Group Memberships -> Add Memberships, locating a Mail Enabled Security Group is greyed out and states "Mail-enabled security groups are not allowed."

upvoted 1 times

mackypatio 2 years, 8 months ago

I agree, I literally have hundreds of unlicensed users that are members of mail-enabled security groups in my production tenant, both in-cloud and synced from onprem.

upvoted 1 times

Diginomad Highly Voted 3 years 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 19 times

xupiter 2 years, 11 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 6 times

zol95 2 years, 3 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

zol95 2 years, 3 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 2 years, 2 months ago

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

upvoted 3 times

Chris7910 1 year, 7 months 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

Matt19 Most Recent 1 week, 5 days ago

Selected Answer: D

Unlicensed user can be added to a MESG NOW on Entra so D

upvoted 2 times

doori88 2 months, 2 weeks ago

Selected Answer: D

I tested it, and a user with no license can be added to the MESG, done in it from the entra admin center

upvoted 2 times

MaxLily 3 months, 1 week ago

Add a group to another group
You can add an existing Security group to another existing Security group (also known as nested groups), creating a member group (subgroup) and a parent group. The member group inherits the attributes and properties of the parent group, saving you configuration time.

Important

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

upvoted 2 times

loukyexamtopic 5 months, 1 week ago

The question is clearly about the AAD/Entra ID not 365admin portal. Please let us know how you exactly do the lab in detail, as I see allot of labs done that are not important with this question

upvoted 1 times

HartMS 8 months, 3 weeks ago

No license - No Money

upvoted 2 times

HartMS 8 months, 3 weeks ago

Selected Answer: E

User2 Only

upvoted 1 times

penatuna 10 months, 3 weeks ago

Selected Answer: D

Tested in my tenant. D is the correct answer, if you can use M365 admin center.

Azure portal / Entra - Cannot add members to mail enabled group. Cannot add Mail-enabled groups to users.

Microsoft 365 admin center - Can add only User2 to Group3. Can add Group3 to both User2 and User3.

Exchange portal - Can add only User2 to Group3. Cannot add groups to users, cause there's no user blade in Exhange portal.

upvoted 3 times

RahulX 10 months, 3 weeks ago

E. User2 only, because only mailboxed users can be added to the MailEnable Security Group.
Tested

upvoted 1 times

lojlkdnfvlirez 1 year ago

the correct anwser is "D": User1 and User2 only, the question is Which objects can you add as members to Group3?

upvoted 1 times

RahulX 1 year, 1 month 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 year, 2 months 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 2 times

Softeng 1 year, 3 months ago

Selected Answer: E

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

upvoted 2 times

Bear4 1 year, 3 months ago

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

upvoted 1 times

syougun200x 1 year, 4 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 1 year, 4 months 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

Question #8 *Topic 1*

DRAG DROP -

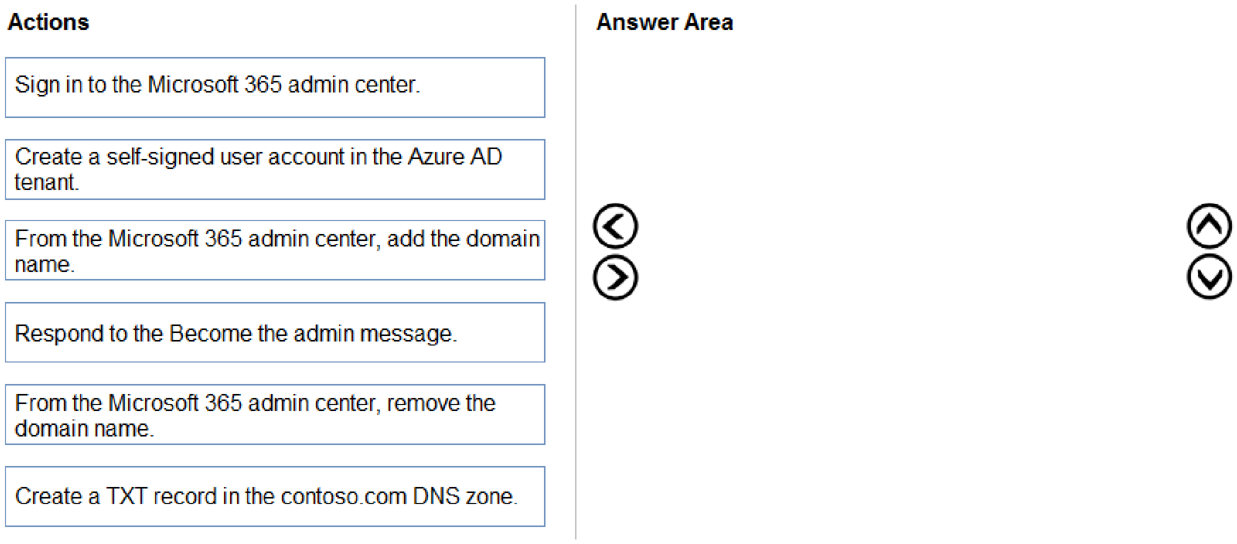
You have an on-premises Microsoft Exchange organization that uses an SMTP address space of contoso.com.

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:

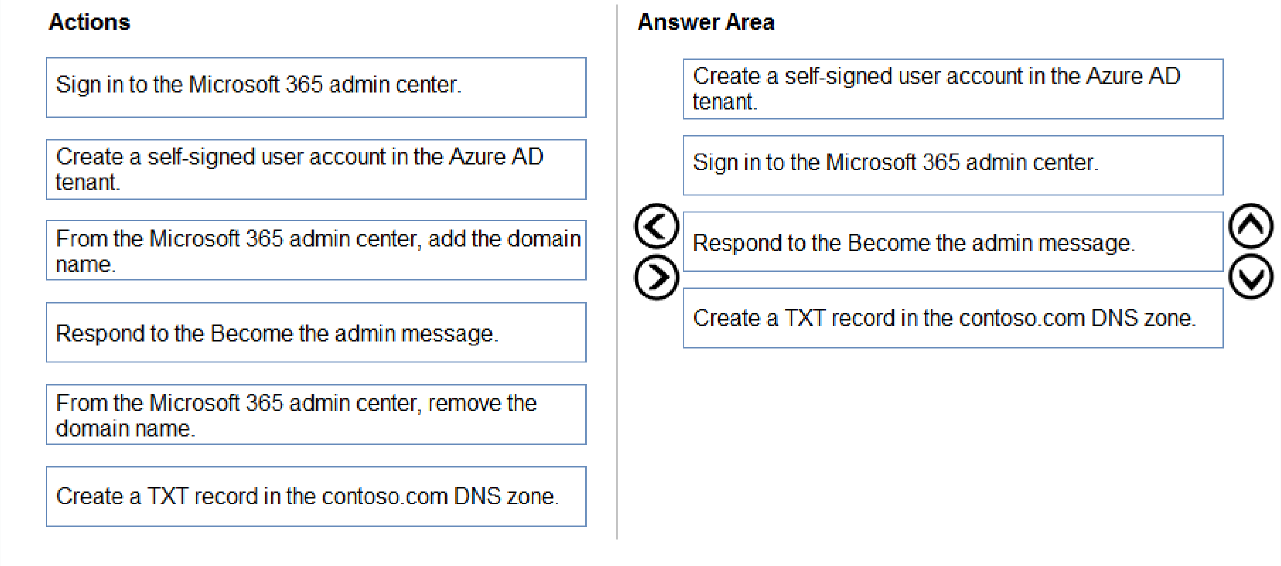


Actions

- 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

Suggested 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 3 years, 2 months ago

Seems correct judging by the link.

upvoted 23 times

slayer78 Highly Voted 2 years, 8 months 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 19 times

casti 2 years, 8 months 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 2 years, 5 months ago

It would appear this 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 8 times

Jhill777 1 year, 7 months ago

Yessir. Had to do this many times.

upvoted 1 times

RahulX Most Recent 4 months, 3 weeks ago

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

Sign in to the Microsoft 365 Admin Center.

Respond to become the admin message.

Create a TXT record in the costoso.com DNS Zone.

upvoted 1 times

lojlkdnfvlirez 6 months, 2 weeks ago

The correct order is :

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

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

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

Respond to the become the admin message.

The reason is that you need to add and verify the domain name before you can respond to the Become the Admin message. The TXT record is used to prove that you own the domain name

upvoted 3 times

EmnCours 10 months, 4 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

dule27 1 year, 1 month 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 1 year, 1 month 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

stromnessian 2 years, 3 months ago

Given answer is correct IMO.

upvoted 1 times

saadnadir 2 years, 4 months ago

Create a Self Signed user account in azure AD tenant

Sign in to the Microsoft 365 admin cehnter respond to the become the admin message

create a ttxt record in the contoso.com DNS zone

upvoted 1 times

⊟ **casti** 2 years, 8 months 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, 8 months 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

⊟ **Ibukun** 2 years, 6 months ago

This is a mistake

upvoted 1 times

⊟ **Mohammad_Alomari** 1 year, 11 months ago

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

upvoted 1 times

⊟ **Domza** 3 years ago

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

Ooof, these kinda questions

upvoted 4 times

⊟ **jilly78** 2 years, 1 month ago

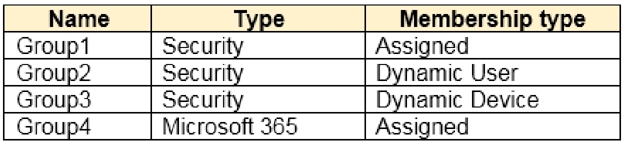
yes it lacks context

upvoted 1 times

Question #9 *Topic 1*

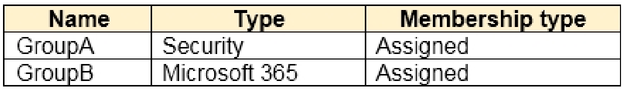
HOTSPOT -

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.

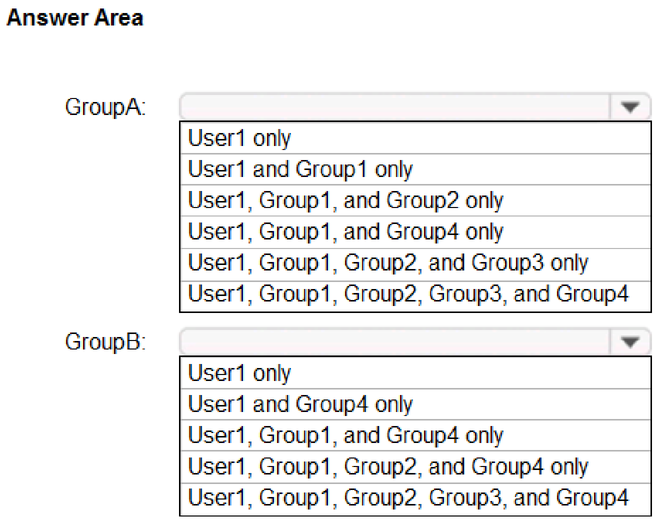


Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

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

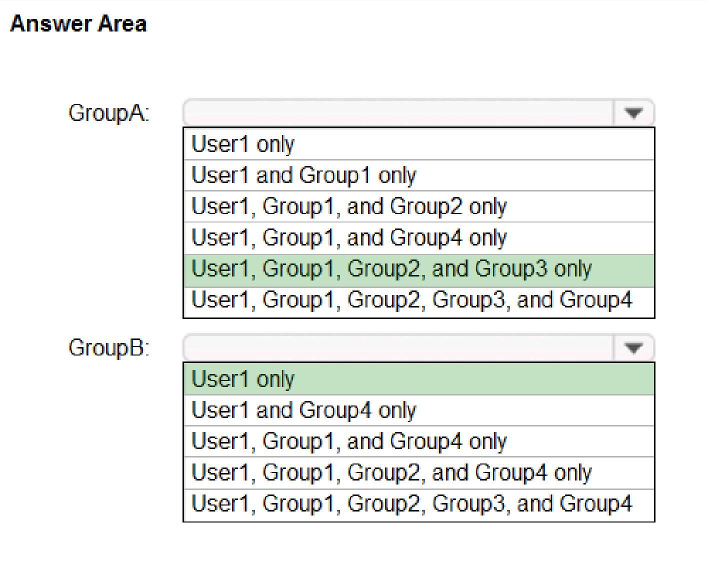
GroupA:

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

Suggested Answer:



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

Reference:

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

Val_0 Highly Voted 3 years, 2 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 89 times

AmazingKies 2 years, 9 months ago

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

upvoted 7 times

lime568 2 years, 3 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 21 times

GryffindorOG Highly Voted 1 year, 10 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 6 times

Jhill777 1 year, 7 months 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, 10 months ago

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

upvoted 3 times

RahulX Most Recent 4 months, 3 weeks ago

GroupA: User1, Group1, Group2, Group3.
GroupB: User1
Note: We can't add M365 group under security group.
Only user can add in M365 Group,

upvoted 4 times

syougun200x 10 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 3 times

EmnCours 10 months, 4 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 1 year, 1 month ago

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

upvoted 3 times

ShoaibPKDXB 1 year, 1 month ago

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

upvoted 1 times

anaSH 1 year, 6 months ago

Answer is correct, tested in my tenant

upvoted 4 times

cameron0485 1 year, 7 months ago

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

upvoted 1 times

ANDRESCB1988 1 year, 8 months ago

Correct.

GroupA allow add users, Dynamic User, Dynamic Devices.

GroupB only permit add users.

upvoted 2 times

sapien45 2 years 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 2 years, 1 month 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.

User1 and User2 only

A-User1 and User3 only

B-Only User2 and User3

C-Only User1, User2 and User3

D-User1, User2, User3 and User4

upvoted 1 times

BTL_Happy 1 year, 7 months ago

To answer your question above - B

upvoted 1 times

bleedinging 2 years, 1 month ago

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

upvoted 2 times

thiennp1982 2 years, 1 month ago

Correct

upvoted 1 times

DemekeAd 2 years, 2 months ago

correct answer

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

upvoted 1 times

⊟ **GPerez73** 2 years, 5 months ago

Correct. I have tested it

upvoted 2 times

⊟ **TJ001** 2 years, 5 months ago

Correct Answer given

- Security Group (Assigned) - can add Users and all other types of Security Groups as members (Assigned, Dynamic User/Device)

-MS365 group - only support adding Users

upvoted 1 times

Question #10 *Topic 1*

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

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

You have 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

Suggested 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

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 19 times

glazdub 1 year, 9 months ago

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

upvoted 2 times

EmnCours Most Recent 4 months, 3 weeks ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

dule27 7 months, 2 weeks ago

Selected Answer: B

B. No is correct

upvoted 1 times

ShoaibPKDXB 7 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

ANDRESCB1988 1 year, 1 month ago

correct, answer is No

upvoted 1 times

bleedinging 1 year, 7 months ago

Objection, your honor: Irrelevant.

upvoted 4 times

WMG 1 year, 9 months ago

Selected Answer: B

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

upvoted 2 times

Iamjudeicon 2 years 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

Question #11 *Topic 1*

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

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

You have 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

Suggested Answer: *A*

Reference:

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

Community vote distribution

A (100%)

melatocaroca Highly Voted 3 years, 5 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 17 times

AlexBrazil Most Recent 2 months ago

Selected Answer: A

Microsoft Entra pass-through authentication can solve this issue.

upvoted 1 times

RahulX 10 months, 3 weeks ago

Yes, Pass-through Authentication and ADFS uses on-premises account policy at the time of sign-in in M365.

upvoted 1 times

EmnCours 1 year, 4 months ago

Selected Answer: A

Correct Answer: A

upvoted 3 times

dule27 1 year, 7 months ago

Selected Answer: A

A: YES - pass-through authentication.

upvoted 2 times

ANDRESCB1988 2 years, 1 month ago

correct, answer is yes

upvoted 2 times

shine98 2 years, 6 months ago

On the exam - June 12, 2022

upvoted 1 times

DemekeAd 2 years, 8 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

⊖ **Iamjudeicon** 3 years ago

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

upvoted 1 times

Question #12 *Topic 1*

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

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

You have 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

Suggested 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, 6 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 9 times

⊟ **MajorUrs** Highly Voted 2 years, 7 months ago

Correct (B - No)

upvoted 7 times

⊟ **Stevo74** Most Recent 4 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 thats why answer is B.

upvoted 2 times

⊟ **EmnCours** 4 months, 3 weeks ago

Selected Answer: B

Correct (B - No)

upvoted 2 times

⊟ **dule27** 7 months, 2 weeks ago

Selected Answer: B

B. No is the correct answer

upvoted 2 times

⊟ **[Removed]** 1 year ago

Selected Answer: B

No is the correct answer.

upvoted 2 times

⊟ **ANDRESCB1988** 1 year, 1 month ago

correct, answers is NO

upvoted 1 times

⊟ **Tokiki** 1 year, 6 months ago

B is correct

upvoted 1 times

⊟ **Fico** 1 year, 7 months ago

Selected Answer: B

has been verified https://docs.microsoft.com/en-us/answers/questions/3221/disable-account-sync.html

upvoted 2 times

⊟ **WMG** 1 year, 9 months ago

Selected Answer: B

Conditional Access will not help.

upvoted 1 times

⊟ **glazdub** 1 year, 9 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

⊟ **Eltooth** 2 years, 7 months ago

Agreed - answer is no.

upvoted 3 times

Question #13 *Topic 1*

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

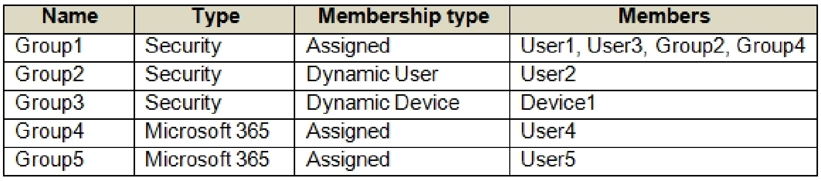
✑ A device named Device1

✑ 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

Suggested Answer: *B*

Reference:

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

Community vote distribution

B (100%)

gills Highly Voted 3 years, 5 months ago

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

upvoted 64 times

jt63 3 years ago

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

upvoted 7 times

Dobby_41 Highly Voted 3 years, 7 months ago

Group 4 cannot be a member of group 1.

upvoted 32 times

sapien45 2 years, 6 months ago

Good catch

upvoted 5 times

AlexBrazil Most Recent 2 months ago

Selected Answer: B

Agreed: "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."

upvoted 3 times

srysgbvjumozmail 4 months, 3 weeks ago

Group4 (MS365) in Group1(Security) is it possible?

contraduction with Topic1-Question9

upvoted 2 times

[Removed] 6 months, 1 week ago

the answer is 2. Very simple char

upvoted 1 times

BigDogAG 10 months, 1 week ago

But why is it 2 and not 1?

upvoted 1 times

Futfuyfyjfj 8 months, 3 weeks ago

The er is no 1 option amongst the possible answer options right?

upvoted 1 times

RahulX 10 months, 3 weeks ago

B: 2 licenses, because nested group do not inherit licenses and M365 Group can not be member of Security Group.

upvoted 3 times

mikekrt 1 year, 3 months ago

Selected Answer: B

2 licenses

upvoted 1 times

EmnCours 1 year, 4 months 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 2 times

EmnCours 1 year, 5 months ago

Selected Answer: B

Answer is correct.

upvoted 1 times

dule27 1 year, 7 months ago

Selected Answer: B

B: 2 licenses

upvoted 2 times

f2bf85a 1 year, 9 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 1 year, 10 months ago

Selected Answer: B

agree it is b

upvoted 1 times

jojoseph 1 year, 11 months ago

B. nested group do not inherit licenses

upvoted 3 times

ANDRESCB1988 2 years, 1 month ago

correct, nesting is not support to assing license

upvoted 1 times

Lion007 2 years, 5 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 2 years, 6 months ago

agree, B

upvoted 1 times

Question #14 Topic 1

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.

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal

Community vote distribution

D (85%) Other

⊟ **Jt909** Highly Voted 3 years, 3 months ago
Probably in the exam the cmdlet New-AzureADMSInvitation is proposed and correct
upvoted 24 times

⊟ **AS007** Highly Voted 3 years, 7 months ago
Looks good given external collaboration is allowed/ default settings
upvoted 8 times

⊟ **WMG** 2 years, 9 months ago
Unless noted, all MS questions assume default settings.
upvoted 4 times

⊟ **Labelfree** Most Recent 2 months ago
D is Correct.

To provide the contractor with access to App1 using their credentials (user1@outlook.com), you should use Azure AD B2B (Business-to-Business) collaboration. This allows external users to access your Azure AD resources using their own credentials.

Steps to Provide Access
Invite the Contractor as a Guest User:
Go to the Azure AD admin center: https://aad.portal.azure.com.
Navigate to Azure Active Directory > Users > New guest user.
Enter the contractor's email address (user1@outlook.com) and send the invitation.
Assign the Guest User to App1:
After the contractor accepts the invitation, go to Azure Active Directory > Enterprise applications.
Select App1 from the list of applications.
Go to Users and groups and click on Add user/group.
Search for the guest user (user1@outlook.com) and assign them to App1.
Configure Permissions:
Ensure that the guest user has the necessary permissions to access App1. This might involve assigning specific roles or permissions within the application.
upvoted 3 times

⊟ **Labelfree** 2 months ago
Replying to my own. Interesting - this was copilot's answer to the Q, surprised to see it still referencing Azure AD rather than Entra, but can't modify it now, but either way D should be the correct answer and the aad.portal.azure.com link redirects to Entra.
upvoted 2 times

⊟ **bardock100** 8 months, 2 weeks ago

Selected Answer: C

https://learn.microsoft.com/pl-pl/training/modules/implement-manage-external-identities/13-configure-identity-providers

upvoted 1 times

bardock100 8 months, 2 weeks ago

C)

https://learn.microsoft.com/pl-pl/training/modules/implement-manage-external-identities/13-configure-identity-providers

Here you have why C is the proper answer:
End-user experience
With SAML/WS-Fed IdP federation, guest users sign in to their Microsoft Entra tenant with their own organizational account. When they access shared resources and are prompted to sign in, users are redirected to their identity provider. Upon successful sign-in, users are returned to their Microsoft Entra ID to access resources. If a Microsoft Entra session expires or becomes invalid, and the federated identity provider has SSO enabled, the user uses SSO. If the federated user's session is valid, the user is not prompted to sign in again. Otherwise, the user will be redirected to their identity provider for sign-in.
labedzkis

upvoted 1 times

Labelfree 2 months ago

Using Microsoft Entra External ID (formerly Azure AD B2B) to invite the contractor as a guest user is generally a better solution than adding a WS-Fed identity provider for several reasons:

Simplicity and Ease of Use
Direct Invitation: Inviting the contractor as a guest user is straightforward and can be done directly through the Microsoft Entra admin center. This process is user-friendly and doesn't require complex configurations.
No Additional Setup: Adding a WS-Fed identity provider involves more steps, including configuring federation settings and ensuring compatibility with the external identity provider1.

upvoted 1 times

belyo 10 months, 1 week ago

Selected Answer: D

smtp suffix is outlook.com so its a MSFT account
this is configured as one of the default identity providers and cannot delete it...
so there is nothing you can configure in external collab, guess you have to invite user

upvoted 3 times

RahulX 10 months, 3 weeks ago

Microsoft Entra application access to external user:
1. Setup the External Collaboration setting.
2. Invite the user, once the user accept the invitation they will become a guest user of your tenant.
3. assign the user the app1.

upvoted 2 times

siffy 11 months, 1 week ago

shouldnt D say invite the user not create it?

upvoted 2 times

ak4exams 9 months, 3 weeks ago

That is what I feel.. it should be invite rather than create

upvoted 1 times

EmnCours 1 year, 5 months ago

Selected Answer: D

Answer is correct.

upvoted 1 times

LOEG 1 year, 7 months ago

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

upvoted 1 times

kanew 1 year, 8 months 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 1 year, 7 months 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 1 year, 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 1 year, 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 3 times

DorelPopKun 1 year, 8 months ago

Correct answer is D.

New-AzADUser is used to create a new active directory user as work/school account

upvoted 1 times

Taigr 1 year, 11 months 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 1 year, 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

Jhill777 2 years, 1 month ago

Selected Answer: D

Correct, given external collaboration is set to defaults

upvoted 1 times

ANDRESCB1988 2 years, 1 month ago

correct option D

upvoted 1 times

Magis 2 years, 2 months ago

Selected Answer: D

Correct. B2B is the only option in this scenario.

upvoted 2 times

Question #15 *Topic 1*

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.

Suggested 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%)

jtlucas99 2 months, 4 weeks ago

signing in to the server running Microsoft Entra Connect Sync using an account that is a member of the ADSyncAdmins security group.

Launch the Synchronization Rules Editor from the Start menu.

In the editor, create an inbound synchronization rule to filter out (not synchronize) all users where extensionAttribute15 has the value NoSync.

Apply the necessary filter conditions to exclude these users during synchronization 1.

upvoted 3 times

RahulX 4 months, 3 weeks ago

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

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-configure-filtering#negative-filtering-do-not-sync-these

upvoted 2 times

EmnCours 10 months, 4 weeks ago

Selected Answer: C

C is correct

upvoted 2 times

dule27 1 year, 1 month ago

Selected Answer: C

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

upvoted 1 times

ShoaibPKDXB 1 year, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

m4rv1n 1 year, 2 months 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 2 times

OrangeSG 1 year, 5 months 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 3 times

purek77 1 year, 6 months 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

BTL_Happy 1 year, 7 months ago

this came out in my test.

upvoted 2 times

palito1980 1 year, 8 months 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 4 times

DeepMoon 1 year, 9 months ago

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

It should be A.

upvoted 4 times

> **DeepMoon** 1 year, 8 months ago
>
> Active Directory Domain Service is an entirely different service that is not part of the question.
>
> upvoted 1 times

Geolem 1 year, 11 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, 9 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 2 years ago

C is correct

upvoted 1 times

Sh1rub10 2 years, 3 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

WS_21 2 years, 3 months ago

Selected Answer: C

upvoted 4 times

hwoarang 2 years, 5 months ago

Selected Answer: C

the answer is correct and tricky question,

they already said "What you configure in *Azure AD Connect*"

upvoted 4 times

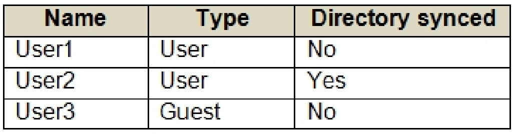
jt63 2 years, 6 months ago

Answer is correct.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#select-the-domains-to-be-synchronized-using-the-synchronization-service

This is the doc the question is referring to:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#negative-filtering-do-not-sync-these
upvoted 3 times

Question #16 *Topic 1*

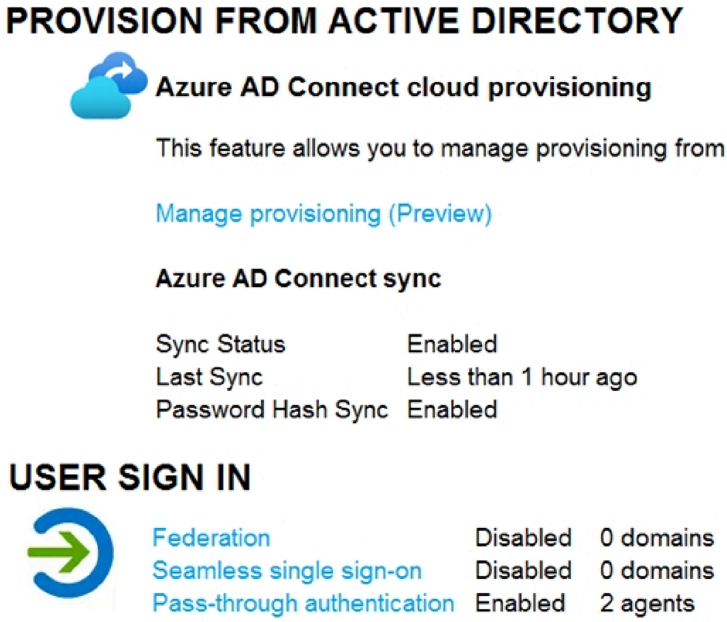
Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.



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

Suggested 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 3 years, 5 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 37 times

⊟ **AmazingKies** Highly Voted 3 years, 3 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 15 times

SebArgy Most Recent 2 weeks, 1 day ago

Selected Answer: C

Reponse C.

1 - The password is sync

2 - TPHS ensures that users can authenticate to cloud services even if the on-premises AD is down.

3 - The tenant is not Federate, that means that tenant is Managed.

Like that, you can directly authenticate with Entra.

upvoted 1 times

AlexBrazil 2 months ago

Selected Answer: A

According to https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta-current-limitations:

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 Microsoft Entra Connect. If the server running Microsoft Entra Connect goes down, you'll require help from Microsoft Support to turn off Pass-through Authentication.

upvoted 1 times

Olami 2 months, 3 weeks ago

Connectivity to on-prems directory to the internet is lost, not the users' connectivity to the internet. I think User 1 and User 3 are not syncing with the on-prems directory. They are on the Azure AD. Only User 2 will have difficulty to sign in to Azure AD because of the Password Hash Sync btw on-prems and Azure AD.

Answer is A

upvoted 2 times

melatocaroca 3 months, 1 week ago

Answer C

Both password hash sync and pass-through are enabled, no password change in the question, just login

Only on-premises domain to the internet is lost

User1 and User 3 are users that will log in with their hash in AAD, User3 is an AAD guest will log with his own credentials created guest on AAD, so IMHO answer must be C

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.

The password hash synchronization process runs every 2 minutes.

When a user attempts to sign into Azure AD and enters their password, the password is run through the same MD4+salt+PBKDF2+HMAC-SHA256 process. If the resulting hash matches the hash stored in Azure AD, the user has entered the correct password and is authenticated.

upvoted 1 times

Jonasweimar 2 years, 3 months ago

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

"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

rachee 3 months, 1 week ago

C. Per https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-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 6 times

Tuvshinjargal 11 months ago

I agree with that. Since the Password Hash Synchronization is enabled, it must have been synched an hour ago, and also the password is saved in Azure AD. It remains when the on-premise AD lost the connection to the internet. See below article.

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta-faq
When you use Microsoft Entra Connect to switch the sign-in method from password hash synchronization to Pass-through Authentication, Pass-through Authentication becomes the primary sign-in method for your users in managed domains. All users' password hashes that are previously synchronized by password hash synchronization remain stored on Microsoft Entra ID.
upvoted 1 times

RahulX 10 months, 3 weeks ago

If password hash synchronization is enabled, all synced users can login with an AD pwd hash value if DC connectivity is lost, and if any user changes their pwd during this period, the hash will remain until the connection is restored. If you have enabled PTA earlier or have installed the PTA DC agent, it will show the pass-through authentication. Enabled 1 or 2 agents under User Sign-In status in azure ad portal.
upvoted 1 times

[Removed] 3 months, 1 week ago

Selected Answer: A

Answer A is correct. PTA cannot be used for directory synchronised objects when the connectivity is lost.
upvoted 1 times

simonseztech 3 months, 1 week 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

f2bf85a 3 months, 1 week ago

Selected Answer: A

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

NotanAdmin 7 months, 2 weeks ago

I got correct answer, but maybe my logic is off? All users work remotely, so wouldnt they log in to AAD, not on prem? Assuming User 2 uses a VPN to login through AD on-prem, I read it as User 2 is already synced. Therefore, A.
upvoted 1 times

RahulX 10 months, 3 weeks ago

A. User1 and User3 only correct ans.
upvoted 1 times

RahulX 10 months, 3 weeks ago

Sorry, The correct ans will be C. User1, User2, and User3.
upvoted 1 times

EmnCours 1 year, 4 months ago

Selected Answer: A

Correct Answer : A
upvoted 3 times

Sango 1 year, 6 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** 1 year, 7 months ago

Selected Answer: A

A. User1 and User3 only

upvoted 1 times

⊟ **estyj** 2 years, 2 months ago

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

upvoted 1 times

⊟ **Tokiki** 2 years, 6 months ago

Agree .A

upvoted 1 times

Question #17 *Topic 1*

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

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

You have 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

Suggested Answer: *B*

Community vote distribution

B (100%)

kijken Highly Voted 1 year, 1 month 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 11 times

melatocaroca Highly Voted 3 years, 5 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 7 times

[Removed] Most Recent 3 months, 1 week ago

Selected Answer: B

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

upvoted 2 times

kalyankrishna1 1 year, 3 months ago

Selected Answer: B

PTA is the only thing that'll work

upvoted 2 times

dule27 1 year, 7 months ago

Selected Answer: B

B: NO is the correct answer

upvoted 1 times

OrangeSG 2 years 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 4 times

⊟ **ANDRESCB1988** 2 years, 1 month ago

correct, is NO

upvoted 1 times

⊟ **Jawad1462** 2 years, 2 months ago

Selected Answer: B

Is the correct answer

upvoted 1 times

⊟ **Iamjudeicon** 3 years ago

NO NO NO

The Given Answer Is Correct!!!

upvoted 2 times

⊟ **sapien45** 2 years, 6 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 3 times

⊟ **Ed2learn** 3 years, 6 months ago

very clearly no - the given answer is correct

upvoted 1 times

Question #18 *Topic 1*

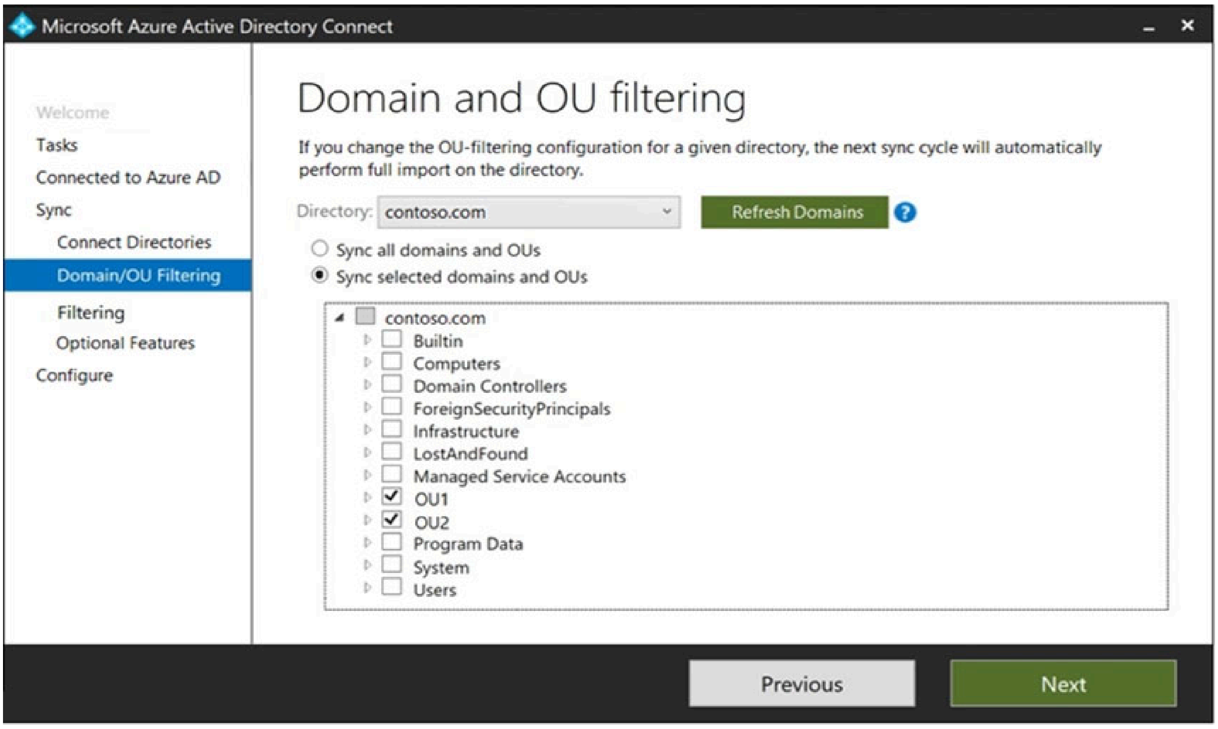
HOTSPOT -

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.)



Microsoft Azure Active Directory Connect

Domain and OU filtering

If you change the OU-filtering configuration for a given directory, the next sync cycle will automatically perform full import on the directory.

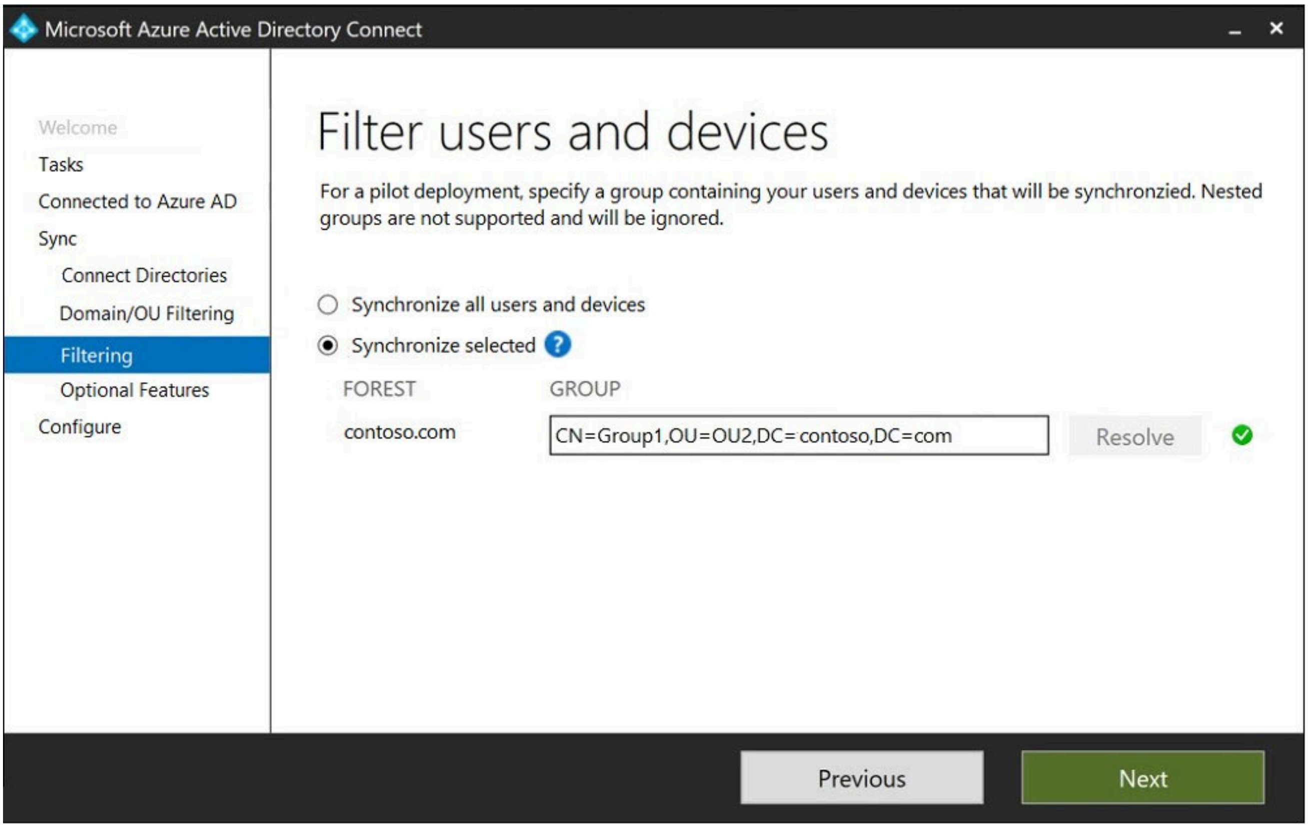
Directory: contoso.com

○ Sync all domains and OUs

● Sync selected domains and OUs

- □ contoso.com
  - □ Builtin
  - □ Computers
  - □ Domain Controllers
  - □ ForeignSecurityPrincipals
  - □ Infrastructure
  - □ LostAndFound
  - □ Managed Service Accounts
  - ☑ OU1
  - ☑ OU2
  - □ Program Data
  - □ System
  - □ Users

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 synchronzied. Nested groups are not supported and will be ignored.

○ Synchronize all users and devices

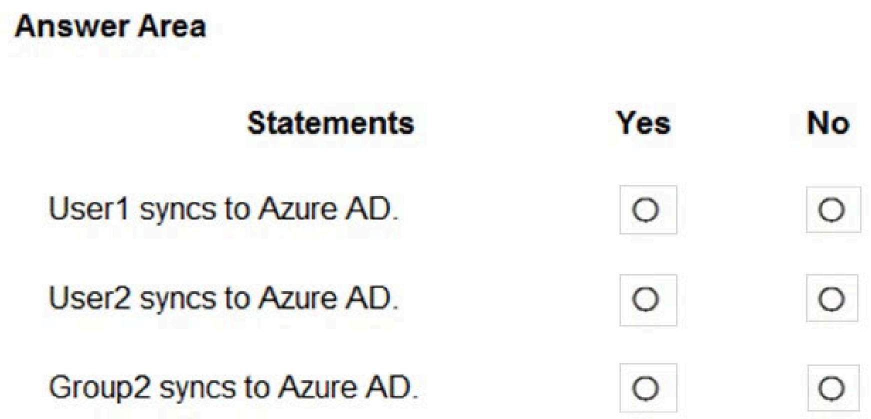
● Synchronize selected

FOREST	GROUP
contoso.com	CN=Group1,OU=OU2,DC=contoso,DC=com

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

NOTE: Each correct selection is worth one point.

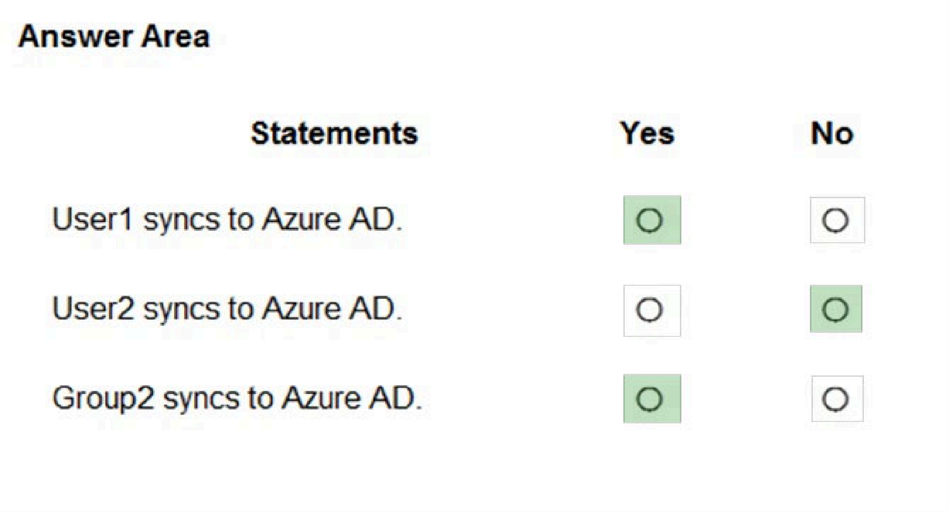
Hot Area:



Answer Area

Statements	Yes	No
User1 syncs to Azure AD.	○	○
User2 syncs to Azure AD.	○	○
Group2 syncs to Azure AD.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 syncs to Azure AD.	[✓ ○]	○
User2 syncs to Azure AD.	○	[✓ ○]
Group2 syncs to Azure AD.	[✓ ○]	○

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

Jhill777 Highly Voted 👍 1 year, 7 months 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 31 times

its_tima 1 year, 5 months 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 1 year, 5 months ago

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

upvoted 2 times

DrMe Highly Voted 👍 2 years, 8 months 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%

upvoted 22 times

RahulX Most Recent ⊙ 4 months, 3 weeks ago

YES
NO
YES

upvoted 1 times

Nivos23 8 months ago

YES
NO
YES

upvoted 1 times

EmnCours 10 months, 4 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%

upvoted 1 times

dule27 1 year, 1 month ago

YES
NO
YES

upvoted 1 times

Efficia 1 year, 12 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 5 times

Tokiki 2 years ago

Correct, YNY

upvoted 1 times

rachee 2 years 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 the users and devices in a nested group won't sync, or the group won't sync either?
upvoted 2 times

⊟ **RandomNickname** 2 years, 1 month ago
See articles pasted by other members and on answer sections for refereance 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 becaused 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 excert 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 9 times

⊟ **TP447** 2 years, 2 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** 2 years, 3 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** 1 year, 2 months 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 OU1 are in scope then the filter removes (filters!) anyone not in Group 1. It doesn't matter which OU Group 2 is in. It synchs 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

⊟ **gugamotarj** 2 years, 3 months ago
Group 2 is Nested and it will be ignored.
Y, N, N is the correct.
upvoted 4 times

⊟ **SnottyPudding** 2 years, 3 months ago
Also, Group2 is in OU1 and will be ignored. "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 1 times

⊟ **lime568** 2 years, 3 months ago
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 3 times

⊟ **GPerez73** 2 years, 5 months ago
In my opinion, user2 also syncs to AAD. it is located in OU1, and OU1 syncs to AAD
upvoted 2 times

⊟ **A_K99** 2 years, 4 months ago
OU1 doesn't sync to the AAD, just Group1 and OU2
upvoted 1 times

⊟ **GPerez73** 2 years, 3 months ago
It is true, you are right.

upvoted 1 times

⊟ **teriaavibes** 2 years, 3 months ago

OU2 doesn't sync, that is just path to group one in the pilot, if you want to sync the whole OU you don't run pilot.

upvoted 1 times

⊟ **btk_1** 2 years, 5 months ago

If Filter users and devices (for a pilot deployment) further refines the Domain and OU filtering, then only Group1 (OU2) syncs. YES - User1 is a member of Group1, NO - User2 is not a member of Group1, NO - Group2 is a member of Group1, but nested groups are ignored in Filter users and devices.

upvoted 3 times

⊟ **valgaw** 2 years, 5 months ago

According to DrMe link, answers is correct

Group2 will be added / synced as a member of Group1, but not members of that group:

" When you add a group as a member, only the group itself is added. Its members aren't added"

upvoted 2 times

⊟ **summut** 2 years, 5 months ago

Actually to be honest this would probably cause Azure Connect to fail for Group 1 and Group 2 because by what I can see there is circular Group nesting in place. But if you ignore that then the answer is correct.

upvoted 1 times

Question #19 *Topic 1*

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

Suggested 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 3 years 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 9 times

WS_21 Highly Voted 2 years, 9 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 7 times

haazybanj Most Recent 3 months, 1 week 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 3 times

sherifhamed 3 months, 1 week 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 2 times

RahulX 10 months, 3 weeks ago
C. a linked subscription Mo
upvoted 1 times

EmnCours 1 year, 4 months ago
Selected Answer: C
C. a linked subscription
upvoted 1 times

dule27 1 year, 7 months ago

Selected Answer: C

C. a linked subscription

upvoted 1 times

ShoaibPKDXB 1 year, 7 months ago

C Linked Subscription

upvoted 1 times

KennethYY 3 years ago

When I study from Microsoft learning, doesnt see this feature need cost ...... :>_<:

upvoted 3 times

zaqwsx 3 years, 4 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

Question #20 *Topic 1*

DRAG DROP -

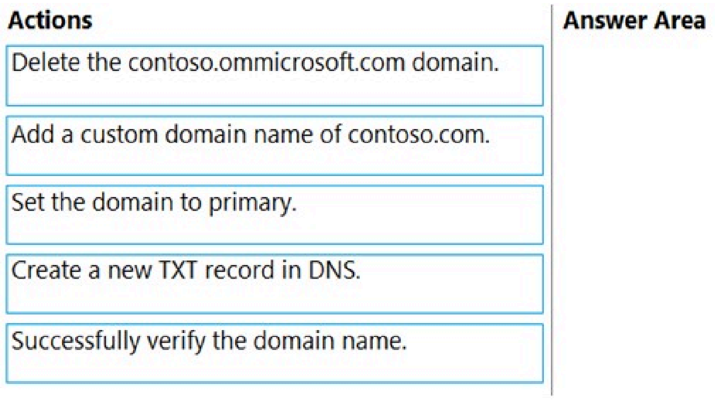
You have a new Microsoft 365 tenant that uses a domain name of contoso.onmicrosoft.com.

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:

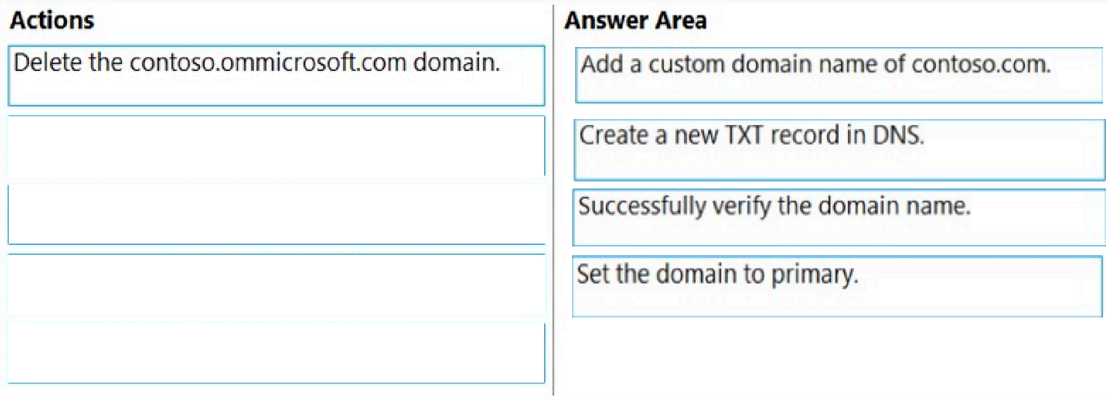


Actions

- Delete the contoso.ommicrosoft.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

Suggested Answer:



Actions

- Delete the contoso.ommicrosoft.com domain.

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, 8 months ago

Correct!!!

upvoted 25 times

oenyabine Most Recent 3 weeks, 2 days ago

correct

upvoted 1 times

EmnCours 11 months, 2 weeks ago

Correct!!!

upvoted 2 times

EmnCours 10 months, 4 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

dule27 1 year, 1 month 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

ANDRESCB1988 1 year, 8 months ago

correct

upvoted 1 times

pete26 1 year, 8 months ago

The answer given is correct!

upvoted 1 times

TJ001 2 years, 5 months ago

Correct !!

upvoted 1 times

Iamjudeicon 2 years, 6 months ago

CORRECT!!!

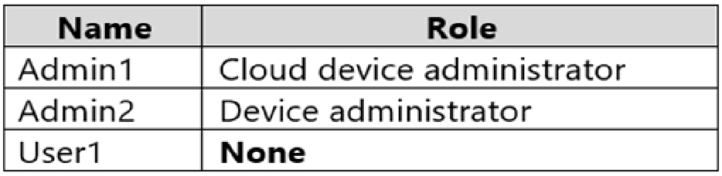
upvoted 2 times

Question #21

Topic 1

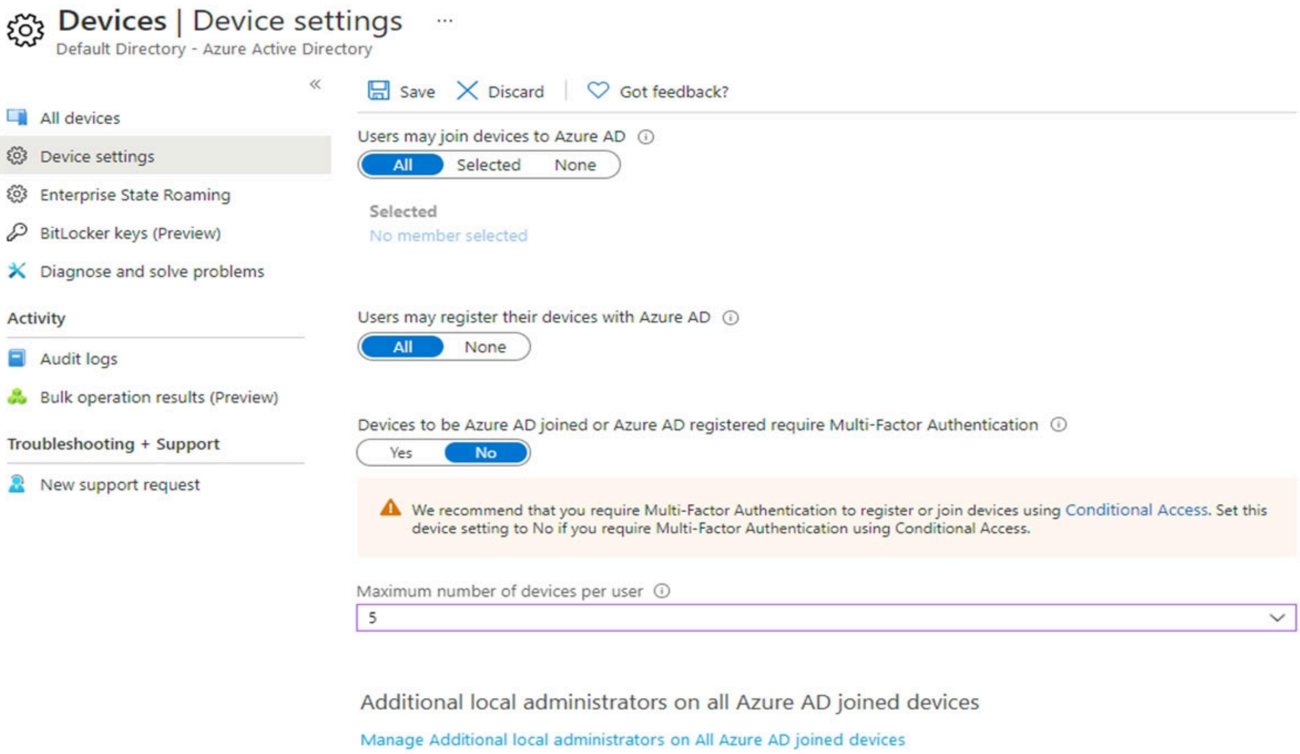
HOTSPOT -

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	**None**

You have the Device Settings shown in the following exhibit.



Devices | Device settings ...

Default Directory - Azure Active Directory

Users may join devices to Azure AD ⓘ

All | Selected | None

Selected

No member selected

Users may register their devices with Azure AD ⓘ

All | None

Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication ⓘ

Yes | **No**

⚠ We recommend that you require Multi-Factor Authentication to register or join devices using Conditional Access. Set this device setting to No if you require Multi-Factor Authentication using Conditional Access.

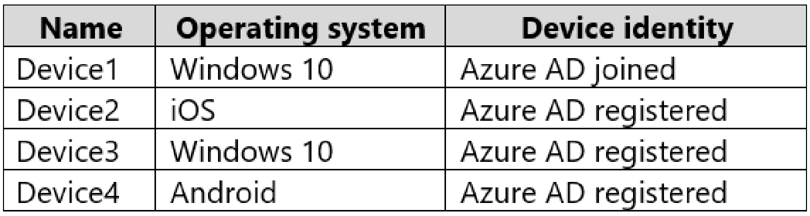
Maximum number of devices per user ⓘ

5

Additional local administrators on all Azure AD joined devices

Manage Additional local administrators on All Azure AD joined devices

User1 has the devices shown in the following table.

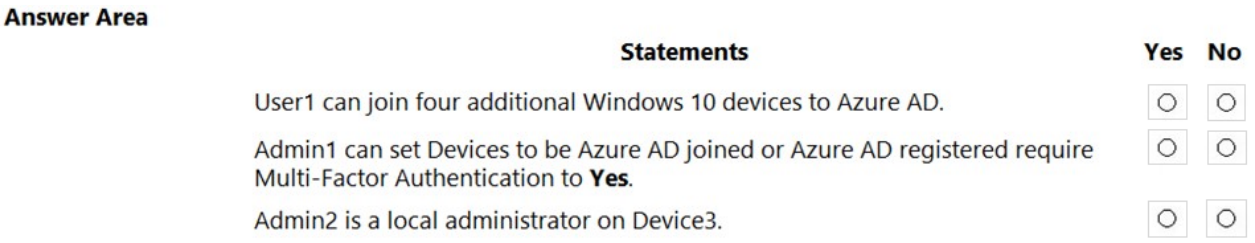


Name	Operating system	Device identity
Device1	Windows 10	Azure AD joined
Device2	iOS	Azure AD registered
Device3	Windows 10	Azure AD registered
Device4	Android	Azure AD registered

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

NOTE: Each correct selection is worth one point.

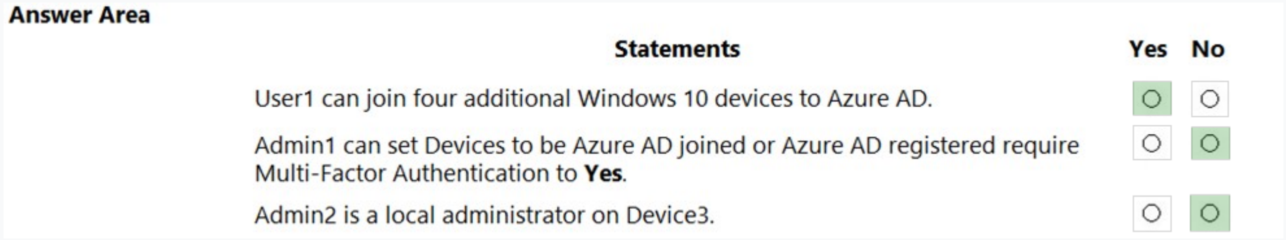
Hot Area:



Answer Area

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.	○	○

Suggested 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.	○	[✓ ○]

Box 1: Yes -

Users may join 5 devices to Azure AD.

Box 2: No -
Cloud device administrator an 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 👍 3 years, 2 months 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

upvoted 86 times

NotanAdmin 7 months, 2 weeks ago

You are correct that : The limit applies to devices that are Microsoft Entra joined or Microsoft Entra registered, with some exceptions.https://learn.mic us/mem/intune/enrollment/device-limit-intune-azure
But this question, unlike the other version of it, says "Users may join 5 devices", so Yes. The other version says something like, "User 1 can join 4 addi SO No, because no matter what devices, he already has 5 joined OR registered.

upvoted 1 times

Menard001 9 months, 1 week ago

it stated there that only 1 is joined and the other 3 is only registered. that's tricky from the question 😂

upvoted 1 times

Alcpt 7 months ago

makes no difference whether joined (work owned) or registered (byod). still adds up to the 5.

upvoted 1 times

Futfuyfyjfj 8 months, 2 weeks ago

Doesn't matter the max devices counts on every device platform, you need to verify the number of devices regardless the OS or join/register type

upvoted 3 times

sergioandreslq 2 years, 6 months ago

100% agreed and tested, these answer are correct:
1) No
2) Yes
3) No

upvoted 15 times

phony 2 years, 10 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/dev device-limit-restriction

upvoted 1 times

phony 2 years, 10 months ago

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

upvoted 11 times

kanew 1 year, 8 months ago

exactly!

upvoted 1 times

xurxosan Highly Voted 👍 2 years, 10 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 26 times

jack987 2 years 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 2 times

enklau Most Recent 2 months, 3 weeks ago
no yes no # i think the first is no because the user has no permissions to
upvoted 3 times

hml_2024 3 months, 2 weeks ago
Given the current settings, User1 can join up to 5 devices to Azure AD. Since User1 already has 1 device Azure AD joined, they can join **4 more devices** to Azure AD. The Azure AD registered devices do not count towards the Azure AD joined device limit.

So, User1 can indeed join another 4 Windows devices to Azure AD.
upvoted 1 times

georgefam 5 months ago
No
No
No
The limit is 5, and the user already have 2 so he can't add 4 more. the limit applies to both Joined and Registered.
"The Maximum number of devices setting applies to devices that are either Microsoft Entra joined or Microsoft Entra registered. This setting doesn't apply to Microsoft Entra hybrid joined devices."
"Cloud Device Administrator:
This is a privileged role. Users in this role can enable, disable, and delete devices in Microsoft Entra ID and read Windows 10 BitLocker keys (if present) in the Azure portal. The role does not grant permissions to manage any other properties on the device."
The Device Admin role, new name Entra Joined Local Administrator, only applied to Entra Joined devices, not Registered devices
upvoted 1 times

07d6037 7 months ago
1) No
2) Yes
3) No

(2)
https://learn.microsoft.com/en-us/entra/identity/devices/manage-device-identities#configure-device-settings
upvoted 1 times

criminal1979 8 months, 3 weeks ago

NO
YES
NO
upvoted 1 times

⊟ **jtlucas99** 9 months ago
Box 2 is YES. - You must be assigned one of the following roles to manage device settings:
Global Administrator
Cloud Device Administrator
upvoted 1 times

⊟ **RahulX** 10 months, 3 weeks ago
Yes
NO
NO

Name: Cloud Device Administrator
Description:
Users in this role can enable, disable, and delete devices in Microsoft Entra ID and read Windows 10 BitLocker keys (if present) in the Azure portal. The role does not grant permissions to manage any other properties on the device.
This role is considered privileged because one or more of its permissions are privileged

Name: Microsoft Entra Joined Device Local Administrator
Description:
Users with this role become local machine administrators on all Windows 10 devices that are joined to Microsoft Entra. They do not have the ability to manage devices objects in Microsoft Entra.
upvoted 2 times

⊟ **Tuvshinjargal** 11 months ago
1) Yes. Not tested. As I understand the user can join additional 4 devices to the Azure AD because the number of devices per user is set to 5. I slightly checked with AI's answer.
2) Yes. I just tested this one. The cloud device administrator can set this setting to Yes.
3) Yes. The user has a device administrator role added to the local administrator on the device.
upvoted 1 times

⊟ **Tuvshinjargal** 11 months ago
By clicking on the link in the local administrator settings directly get into the "Device administrator role" assignment page.
upvoted 1 times

⊟ **Blagojche** 11 months, 4 weeks ago
Azure device limit restriction
Azure device limit restrictions set the maximum number of devices that either Microsoft Entra joins or Microsoft Entra registers. To set the Maximum number of devices per user, go to the Azure portal > Microsoft Entra ID > Devices. For more information, see
https://learn.microsoft.com/en-us/mem/intune/enrollment/device-limit-intune-azure
1.) NO
upvoted 1 times

⊟ **Nyamnyam** 1 year, 1 month ago
I also support the 1.No, 2.Yes, 3.No community here.
upvoted 2 times

⊟ **amurp35** 1 year, 4 months ago
Seems the real correct answer is 1-No, 2-Yes, 3-No, and not what is shown
upvoted 1 times

⊟ **EmnCours** 1 year, 4 months ago
Correction:
NO
YES
NO
upvoted 1 times

⊟ **dule27** 1 year, 7 months ago

NO
NO
NO
upvoted 1 times

⊟ **dule27** 1 year, 6 months ago

Correction:
NO
YES
NO
upvoted 1 times

⊟ **kanew** 1 year, 8 months 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 3 times

⊟ **Holii** 1 year, 6 months 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** 1 year, 8 months 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

Question #21 *Topic 1*

You have a Microsoft 365 subscription.

You need to ensure that when users access the Microsoft 365 portal from Microsoft Edge and have their browser language set to Spanish, they are presented with a Spanish sign-in form.

What should you do in the Microsoft Entra admin center?

A. From Settings for the users, configure the Usage location setting.

B. From Global Secure Access, configure the Session management settings.

C. Configure the Company branding settings.

D. Create a Conditional Access policy.

Suggested Answer: *C*

Community vote distribution

C (100%)

5f2afa7 6 days, 12 hours ago

Selected Answer: C

Entra > User experiences > Company Branding > Add browser language

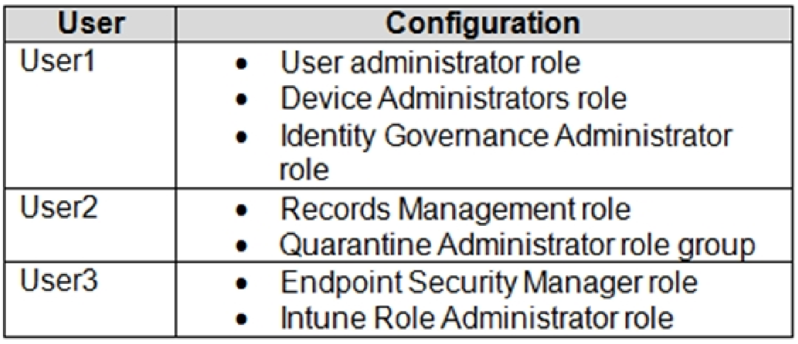
upvoted 2 times

Question #22 *Topic 1*

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.

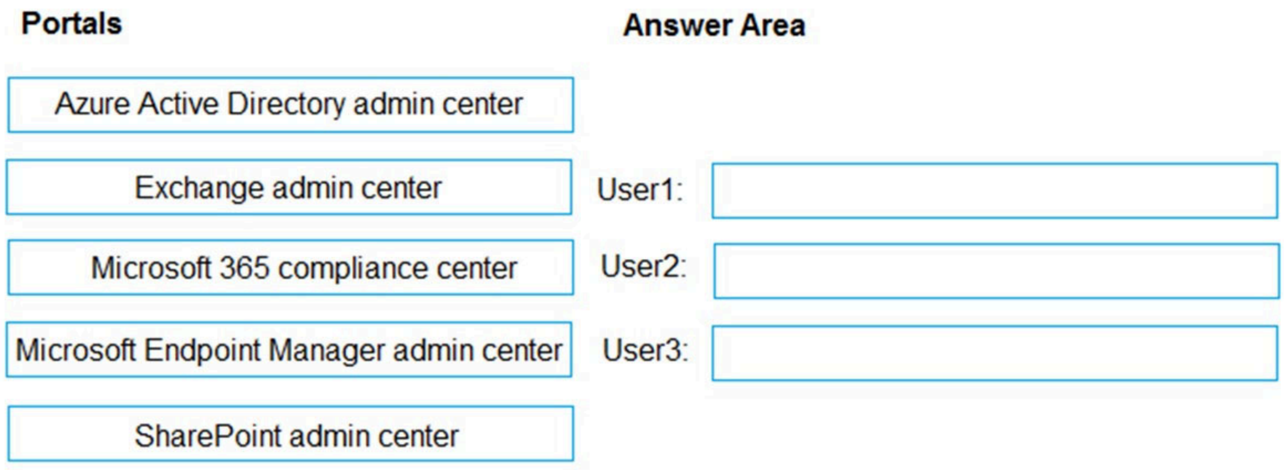


User	Configuration
User1	• User administrator role • Device Administrators role • Identity Governance Administrator role
User2	• Records Management role • Quarantine Administrator role group
User3	• Endpoint Security Manager role • Intune Role Administrator role

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

- Azure Active Directory admin center
- Exchange admin center
- Microsoft 365 compliance center
- Microsoft Endpoint Manager admin center
- SharePoint admin center

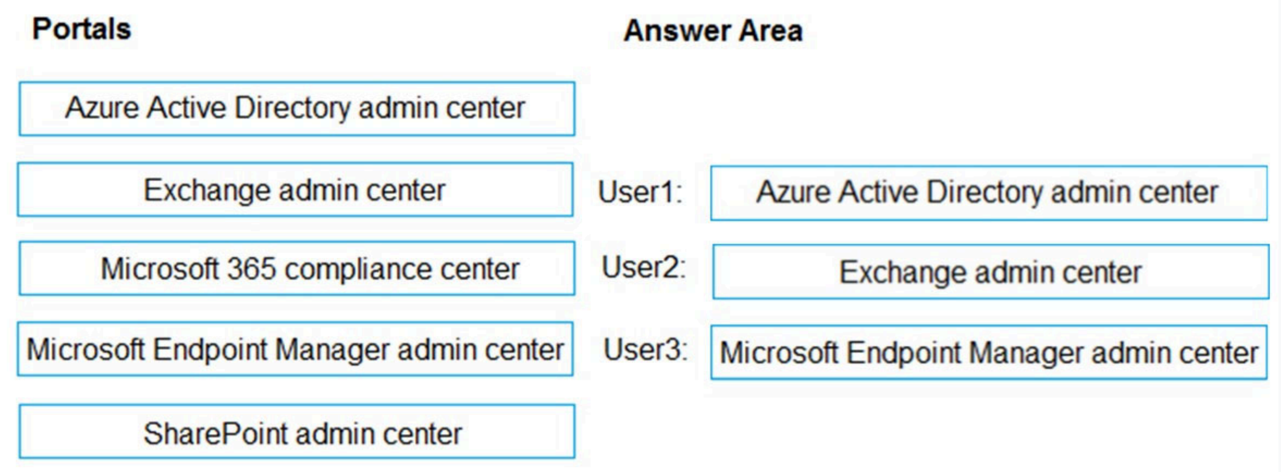
Answer Area

User1:

User2:

User3:

Suggested Answer:



Portals

- Azure Active Directory admin center
- Exchange admin center
- Microsoft 365 compliance center
- Microsoft Endpoint Manager admin center
- SharePoint admin center

Answer Area

User1: Azure Active Directory admin center

User2: Exchange admin center

User3: Microsoft Endpoint Manager admin center

sergioandreslq Highly Voted 1 year, 12 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 37 times

jack987 1 year, 6 months 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 10 times

Nyamnyam 8 months 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

f2bf85a 1 year, 2 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 2 times

dhenrique1555 Highly Voted 2 years, 2 months ago

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

upvoted 13 times

jilly78 2 years, 1 month ago

currently true

upvoted 3 times

Holii 1 year ago

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

upvoted 4 times

RahulX Most Recent 4 months, 3 weeks ago

Azure AD Admin Center (Microsoft Entra ID Admin Center)

* User Administrator Role

* Device Administator Role

* Identity Governance Administrator

Microsoft Purview

Roles & Scopes -> Permissions ->

Role groups for Microsoft Purview solutions

* Quarantine Administrator

* Records Management

Microsoft Intune Admin Center.

Tenant Admin -> Roles -> Endpoint Manager roles

* Endpoint Security Manager

* Intune Role Administrator

upvoted 3 times

mikekrt 9 months, 3 weeks ago

New names:

User 1: Entra ID Admin center

User 2: Microsoft Purview admin center

User 3: Intune admin center

upvoted 5 times

EmnCours 10 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 3 times

EmnCours 11 months, 2 weeks ago
Correct Answer
upvoted 1 times

MatthewMeng 1 year 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 1 year, 1 month ago
User 1: Azure AD Admin Center
User 2: Exchange Admin Center
User 3: Microsoft Endpoint Manager Admin Center
upvoted 2 times

Holii 1 year 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

dule27 12 months ago
User 2: Microsoft Purview Compliance portal
upvoted 1 times

AmplifiedStitches 1 year, 2 months 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 1 year, 5 months ago
Strangely enough, the quarantine administrator role group is in the Exchange Admin Center.
upvoted 1 times

ANDRESCB1988 1 year, 8 months ago
correct
upvoted 1 times

VinciTheTechnic1an 2 years 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 2 years, 1 month 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

slick_orange 1 year, 10 months ago
Or maybe the question was not up to date.
upvoted 2 times

kanew 1 year, 2 months 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

Nilz76 2 years, 2 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

Question #23 Topic 1

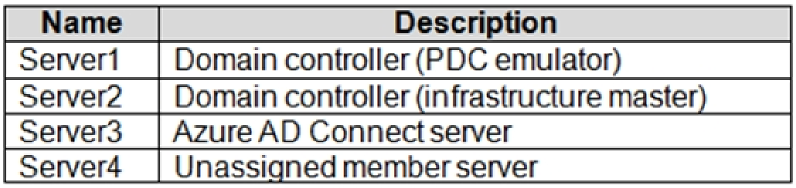
You have an Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant. The tenant uses pass-through authentication.

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

Suggested Answer: *A*

Reference:

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

Community vote distribution

A (88%) 12%

⊟ **Nilz76** Highly Voted 2 years, 2 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 18 times

⊟ **krisbla** Highly Voted 5 months, 1 week ago

On Exam in January 2024!

upvoted 6 times

⊟ **onelove01** Most Recent 6 months, 2 weeks ago

Selected Answer: A

On exam 12/15/2023.

upvoted 2 times

⊟ **EmnCours** 11 months, 2 weeks ago

Selected Answer: A

Answer A.

upvoted 1 times

⊟ **dule27** 1 year, 1 month ago

Selected Answer: A

A: Server 4

upvoted 1 times

⊟ **yakuzasm** 1 year, 4 months ago

server 4 is correct, tested and worked

upvoted 2 times

⊟ **ANDRESCB1988** 1 year, 8 months ago

Server 4 is correct

upvoted 1 times

slick_orange 1 year, 10 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, 11 months ago

Selected Answer: A

Answer A.

upvoted 1 times

Zubairr13 1 year, 11 months ago

On the exam, 7/23/2022.

upvoted 2 times

Tokiki 2 years ago

Agree. A

upvoted 2 times

shine98 2 years ago

On the exam - June 12, 2022

upvoted 1 times

bleedinging 2 years, 1 month 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** 2 years ago
>
> correct...
>
> upvoted 1 times

Davidf 2 years, 1 month ago

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

upvoted 6 times

Nilz76 2 years, 2 months ago

Selected Answer: A

This question was in the exam 28/April/2022

upvoted 3 times

Nilz76 2 years, 2 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 3 times

> **Nilz76** 2 years, 2 months ago
>
> Correction, wrong vote on Selected Answer, Should be Selected Answer A.
>
> upvoted 1 times

Question #24 *Topic 1*

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.

Suggested 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%) Other

⊟ **Jacquesvz** Highly Voted 2 years, 4 months ago
Selected Answer: A
A is the answers, 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 26 times

⊟ **Hot_156** Highly Voted 2 years, 3 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 16 times

⊟ **acsoma** 1 year, 4 months 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 2 times

⊟ **jim85** Most Recent 6 months, 1 week ago
Selected Answer: B
https://learn.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0 only invites the user but won't provide access to any resources. External collaboration settings have to be configured first.
upvoted 1 times

⊟ **Alcpt** 7 months ago
The context of this question is terrible. Does the org already have B2B collaboration setup? If so, then A. But if no collaboration exists as yet, then B is required to setup before sending out invites (A).
grrr.
upvoted 2 times

⊟ **bardock100** 8 months, 1 week ago
Selected Answer: C
https://learn.microsoft.com/pl-pl/training/modules/implement-manage-external-identities/13-configure-identity-providers

Here you have why C is the proper answer:
End-user experience
With SAML/WS-Fed IdP federation, guest users sign in to their Microsoft Entra tenant with their own organizational account. When they access shared resources and are prompted to sign in, users are redirected to their identity provider. Upon successful sign-in, users are returned to their Microsoft Entra ID to access resources. If a Microsoft Entra session expires or becomes invalid, and the federated identity provider has SSO enabled, the user uses SSO. If the federated user's session is valid, the user is not prompted to sign in again. Otherwise, the user will be redirected to their identity provider for sign-in.

upvoted 2 times

haazybanj 1 year, 1 month 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 2 times

EmnCours 1 year, 5 months ago

Selected Answer: A

A. Run the New-AzureADMSInvitation cmdlet.

upvoted 1 times

vietnam 1 year, 5 months ago

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

upvoted 1 times

dule27 1 year, 7 months ago

Selected Answer: A

A. Run the New-AzureADMSInvitation cmdlet.

upvoted 1 times

AMDf 2 years ago

Selected Answer: A

A is correct

upvoted 4 times

pikapin 2 years, 3 months ago

In exam 29/Sep

upvoted 1 times

DeepMoon 2 years, 3 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 1 year, 6 months 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 2 years, 5 months ago

Selected Answer: B

Question is asking the prerequisition of A, so I'll go for B.

upvoted 3 times

⊟ **kangtamo** 2 years, 5 months ago

Selected Answer: A

I would go with A.

upvoted 1 times

⊟ **Tokiki** 2 years, 6 months ago

A is answer

upvoted 1 times

⊟ **Mike8899** 2 years, 6 months ago

B:

By default all users can invite guest users.

Too access to App1. Add applications to the self-service sign-up user flow under configure external collaboration settings.

upvoted 2 times

⊟ **kanew** 1 year, 8 months 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** 2 years, 6 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

Question #25 *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 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

Suggested 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 Highly Voted 2 years, 7 months ago
The Set-MsolUserLicense cmdlet is deprecated. You'd use Set-MgUserLicense now.
upvoted 15 times

sapien45 2 years, 6 months ago
Not yet deprectated

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 6 times

JimboJones99 Highly Voted 1 year, 2 months 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 6 times

klaytech 8 months, 3 weeks ago
Set-MgUserLicense
upvoted 2 times

AlexBrazil Most Recent 2 months ago
Selected Answer: D
According to https://learn.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0, the Set-MsolUserLicense option is the correct one.
upvoted 1 times

dmwelly 4 months, 3 weeks ago

Question in Aug 2024

upvoted 2 times

jtlucas99 7 months, 3 weeks ago

Assigning Licenses:

1. Sign in to the Microsoft Entra admin center as at least a License Administrator.
2. Browse to Identity > Billing > Licenses.
3. Select the name of the license plan you want to assign to the user.
4. After you select the license plan, select Assign.
5. On the Assign page, select Users and groups, and then search for and select the user you're assigning the license.

Select Assignment options, make sure you have the appropriate license options turned on, and then select OK

Removing Licenses:

5. On the Assign page, select Users and groups, and then search for and select the user you're removing the license from.

Select Assignment options, make sure you have the appropriate license options turned off, and then select Ok

upvoted 1 times

sherifhamed 1 year, 3 months ago

But isn't it true thatو

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 1 year, 4 months ago

Selected Answer: D

D. the Set-MsolUserLicense cmdlet

upvoted 2 times

dule27 1 year, 6 months ago

Selected Answer: D

D. the Set-MsolUserLicense cmdlet

upvoted 2 times

ShoaibPKDXB 1 year, 7 months ago

Selected Answer: D

D: Set-MsolUserLicense

upvoted 3 times

[Removed] 2 years ago

Selected Answer: D

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

upvoted 1 times

giver 2 years, 5 months ago

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

upvoted 1 times

> **martinods** 2 years, 3 months ago
>
> in the question 4 "us 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 3 times
>
> **Dimonchik** 2 years ago
>
> For 2500 users? Well... the community like a million of flies- they can't make a mistake.
>
> upvoted 1 times

rachee 2 years, 5 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 2 years, 6 months ago

D is correct

upvoted 1 times

Benkyoujin 2 years, 7 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

Question #26 *Topic 1*

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:

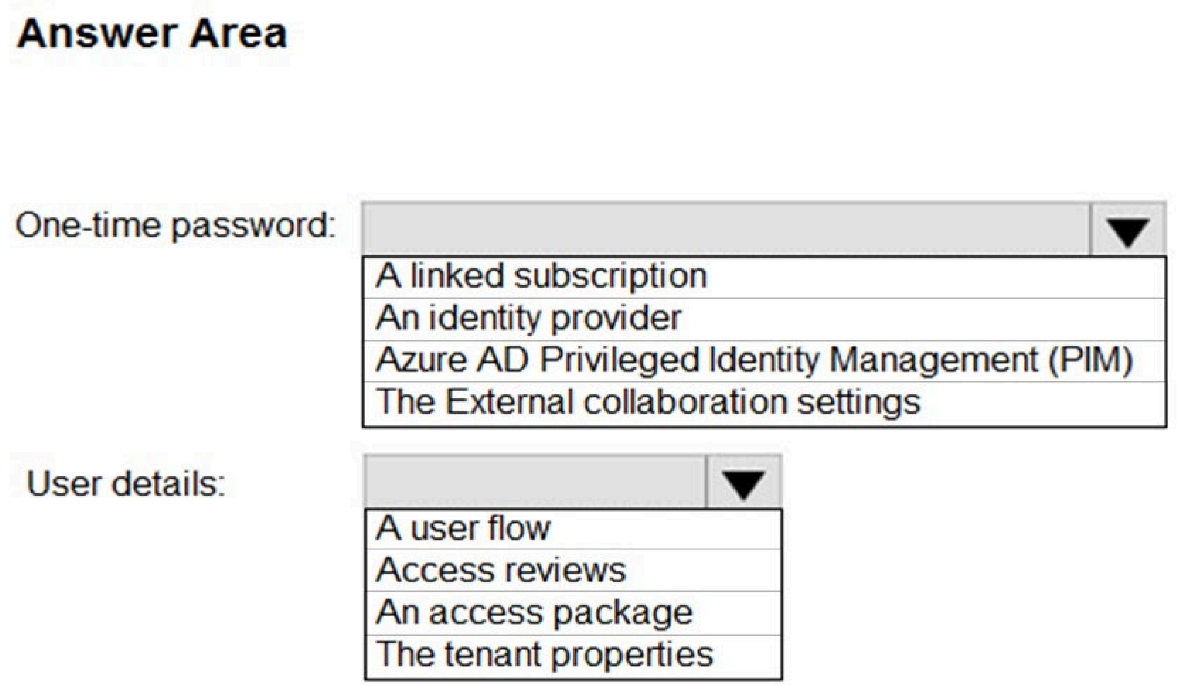
✑ Guest users must be able to sign up by using a one-time password.

✑ 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:

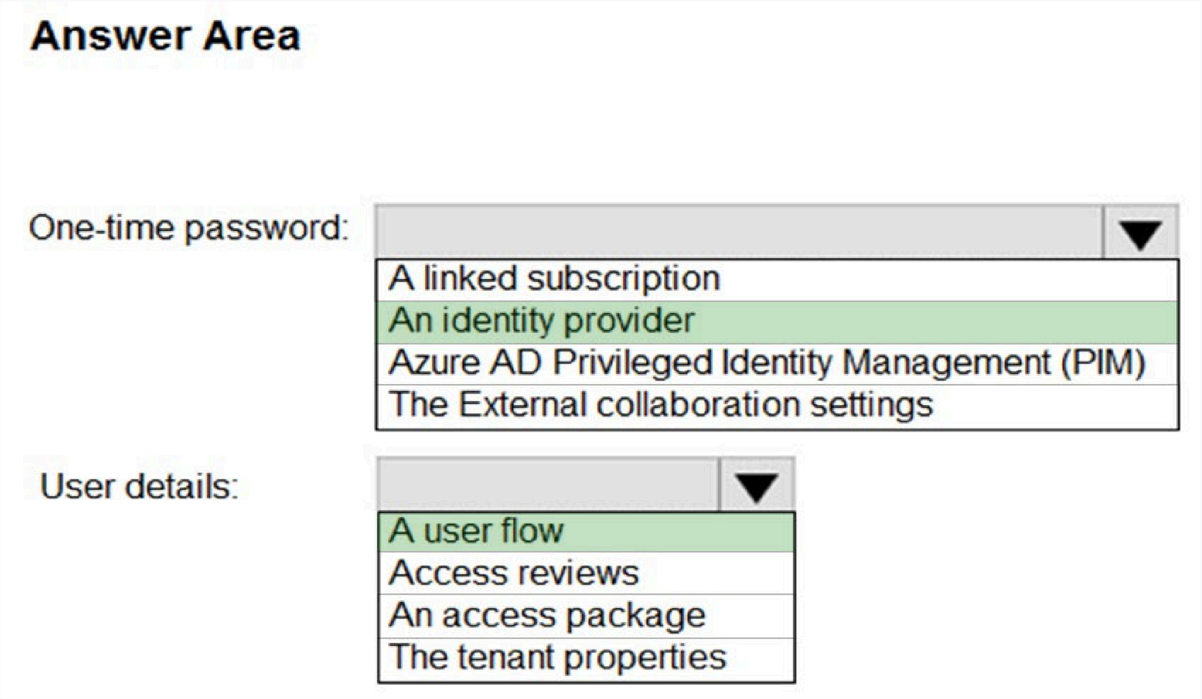


Answer Area

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

Suggested 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

OK2020 Highly Voted 1 year ago

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 32 times

Waris_khan8623 Most Recent 4 months, 1 week ago
B2C identity provider and user flow under B2c Tenant. The answer is correct.
upvoted 2 times

RahulX 4 months, 3 weeks ago
One-time Password: An Identity Provider
Configured identity providers-> Email one-time passcode

User details: A User flow
Enable guest self-service sign up via user flows

https://learn.microsoft.com/en-us/entra/external-id/self-service-sign-up-user-flow#create-the-user-flow-for-self-service-sign-up
upvoted 3 times

EmnCours 11 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 10 months, 3 weeks ago
One-Time Password: an Identity Provider
User Details: a user flow
upvoted 3 times

venumurki 1 year 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 1 year ago
One-Time Password: an Identity Provider
User Details: a user flow
upvoted 2 times

ShoaibPKDXB 1 year, 1 month ago
Correct. An Identity provider and User flow
upvoted 1 times

f2bf85a 1 year, 2 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 4 times

Holii 1 year 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 3 times

Holii 1 year 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

klayytech 2 months, 2 weeks ago

Sign in to the Microsoft Entra admin center as at least a Security Administrator.

Browse to Identity > External Identities > All identity providers.

In the Configured identity providers list, select Email one-time passcode.

Under Email one-time passcode for guests, select one of the following:
upvoted 2 times

ccaitlab 1 year, 7 months 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, 8 months 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, 9 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, 9 months ago

aNSWER IS WRONG. tHE ANSWER IS EXTERNAL COLLABORATION SETTINGS AND USER FLOW
upvoted 1 times

Holii 1 year 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 1 year, 6 months ago

I think guest setting, refer question 3

upvoted 2 times

⊟ **taer** 1 year, 9 months ago

correct

upvoted 1 times

Question #27 *Topic 1*

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

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-add

Community vote distribution
C (100%)

bardock100 Highly Voted 8 months, 1 week ago
This is so old, here you don't have good answer here. I checked right now, bulk create in Entra ID and is: displayName, userPrincipalName, PasswordProfile, accountEnabled.
upvoted 6 times

Nyamnyam Highly Voted 1 year, 1 month 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 5 times

AlexBrazil Most Recent 2 months ago
Selected Answer: C
According to https://learn.microsoft.com/en-us/entra/identity/users/users-bulk-add#to-create-users-in-bulk

"The only required values are Name, User principal name, Initial password and Block sign in (Yes/No)."

The option C is the better.
upvoted 2 times

amurp35 1 year, 4 months 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 3 times

EmnCours 1 year, 5 months ago
Selected Answer: C
Correct Answer: C
upvoted 2 times

dule27 1 year, 6 months ago
Selected Answer: C
C. accountEnabled, displayName, userPrincipalName, and passwordProfile
upvoted 1 times

ShoaibPKDXB 1 year, 7 months ago
Selected Answer: C
Correct. C
upvoted 1 times

kerimnl 2 years, 2 months 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 2 years, 3 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 2 years, 3 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 2 years, 3 months ago

Selected Answer: C

You can see it in the Template

upvoted 2 times

zed026 2 years, 4 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 2 years ago

So basically, none of the provided answers is correct.

upvoted 1 times

ThotSlayer69 1 year, 11 months ago

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

upvoted 2 times

ThotSlayer69 1 year, 11 months ago

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

upvoted 3 times

Question #28 *Topic 1*

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.

Suggested 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 👍 3 years, 2 months 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 21 times

testgm Highly Voted 👍 2 years, 4 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 20 times

AlexBrazil Most Recent 2 months ago
Selected Answer: C
According to https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sso-quick-start,

"You start by adding the following Microsoft Entra URL to all or selected user intranet zone settings through Group Policy in Windows Server AD:
upvoted 2 times

RahulX 10 months, 3 weeks ago
Correct Ans is C
You need to whitelist all the required URL and Endpoint for Azure AD SSO.
https://autologon.microsoftazuread-sso.com
upvoted 2 times

EmnCours 1 year, 5 months ago
Selected Answer: C
Correct Answer: C
upvoted 1 times

dule27 1 year, 6 months ago
Selected Answer: C
C. Modify the Intranet Zone settings.
upvoted 2 times

ShoaibPKDXB 1 year, 7 months ago

Selected Answer: C

Correct: C

upvoted 1 times

Zubairr13 2 years, 5 months ago

On the exam, 7/23/2022.

upvoted 3 times

ali_pin 2 years, 6 months ago

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

upvoted 2 times

shine98 2 years, 6 months ago

On the exam - June 12, 2022

upvoted 3 times

petercorn 2 years, 6 months ago

Selected Answer: C

Answer in Step 3: Roll out the feature

upvoted 1 times

POOUAGA 2 years, 8 months ago

Agree the answer is C

upvoted 1 times

Nilz76 2 years, 8 months ago

This question was in the exam 28/April/2022

upvoted 1 times

Miguelin11 2 years, 9 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 2 years, 9 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 2 years, 9 months ago

On the exam - March 28, 2022

upvoted 1 times

Sh1rub10 2 years, 9 months ago

Selected Answer: C

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

upvoted 1 times

Question #29 *Topic 1*

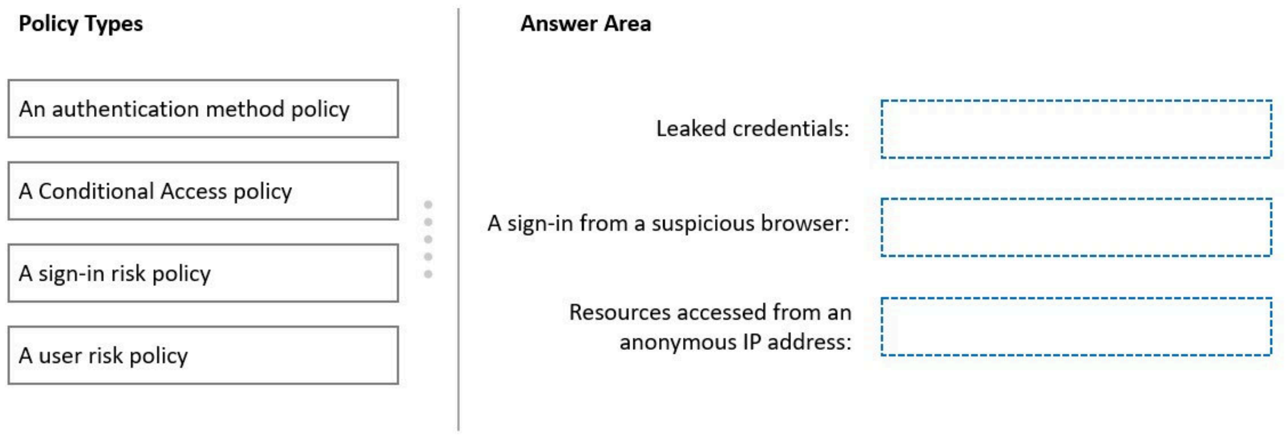
DRAG DROP -

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

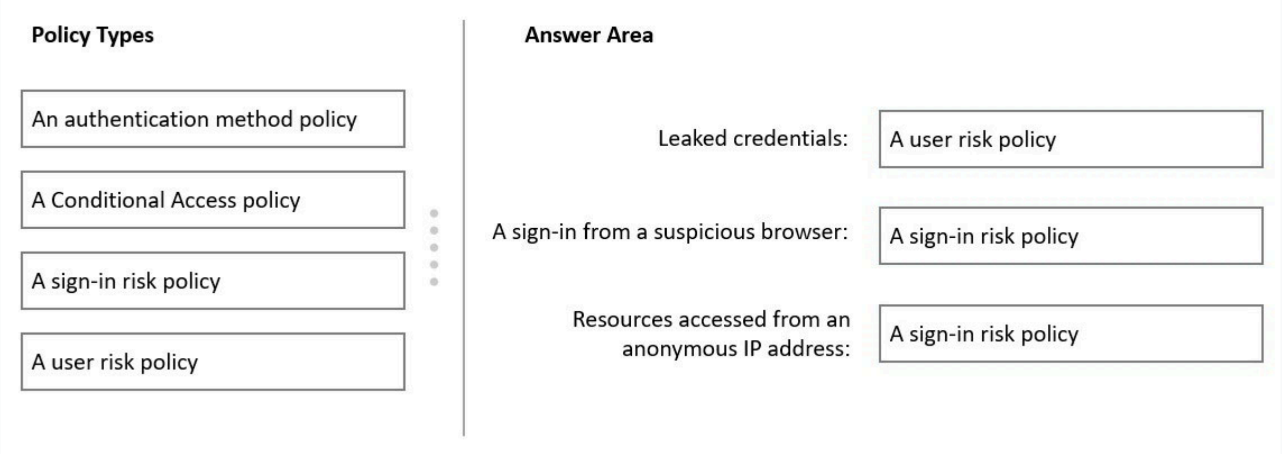
Answer Area

Leaked credentials:

A sign-in from a suspicious browser:

Resources accessed from an anonymous IP address:

Suggested 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, 8 months 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 21 times

⊟ **chikorita** 1 year, 3 months ago

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

upvoted 1 times

⊟ **Holii** 1 year 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

⊟ **chzon** Highly Voted 👍 1 year, 3 months ago

Today I would solve all over Conditional Access.

upvoted 13 times

⊟ **S60** 1 week, 4 days ago

Identity protection console now has a note "We recommend migrating user-risk / Sign-in risk policy to conditional access" so i would say conditional access for all three scenarios.

upvoted 1 times

⊟ **syougun200x** 10 months 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 youre the only one who bothered to go hands on here.

upvoted 2 times

⊟ **RahulX** Most Recent 4 months, 3 weeks ago

1. A user risk policy
2. A sign-in risk policy
3. A sign-in risk policy

upvoted 4 times

⊟ **EmnCours** 10 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** 1 year ago

1. A user risk policy
2. A sign-in risk policy
3. A sign-in risk policy

upvoted 3 times

⊟ **ShoaibPKDXB** 1 year, 1 month ago

Correct

upvoted 1 times

⊟ **den5_pepito83** 1 year, 7 months ago

ON EXAM 14/11/2022

upvoted 4 times

⊟ **Vaerox** 5 months, 4 weeks ago

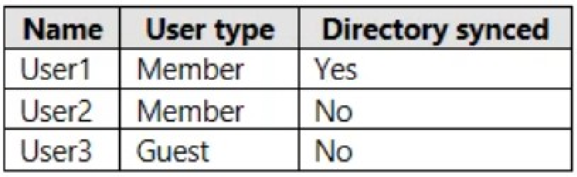
But was it correct?

upvoted 1 times

Question #30 *Topic 1*

HOTSPOT -

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

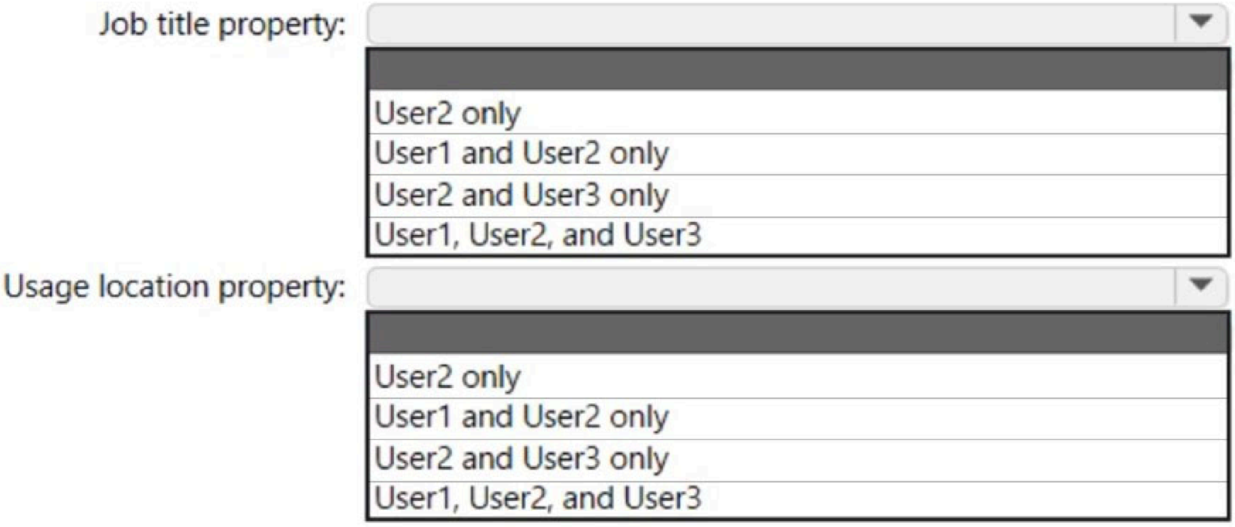


Name	User type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

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:



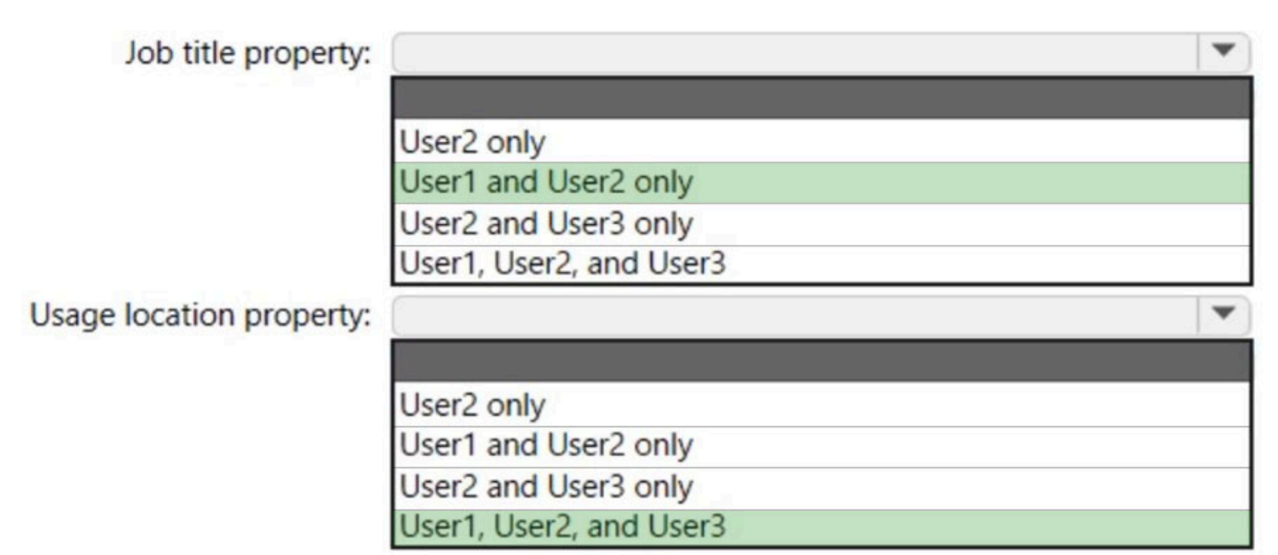
Job title property:

- 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

Suggested 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 2 years, 3 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 86 times

mb0812 9 months, 2 weeks ago
Agree. We canot set job title in Azure for a user synced from on-premise AD
upvoted 3 times

Magis 2 years, 2 months ago
Agree. This answer is correct for sure.
upvoted 5 times

kanew 1 year, 8 months ago
Agree 100% and tested.
upvoted 6 times

Silusha 1 year, 3 months ago
Did you try to change the job title of User3?
upvoted 1 times

sbnpj 1 year, 8 months ago
agree with above answers. you cannot modify directory synced user's properties in azure ad.
upvoted 4 times

referme Highly Voted 2 years, 4 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 20 times

Fcnet 2 years, 2 months ago
Job Title : only user2 & user3
Usage Location can be changed for U1,U2,U3
upvoted 1 times

SvenHorsheim 2 years, 1 month 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 1 year, 6 months 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 2 times

BRZSZCL Most Recent 2 months ago

ANSWER given here is wrong, i have tried in lab environment. usage location can be modified as it is it Azure AD attribute in all 3 scenarios (user 1, user 2, user 3) but job title is attribute set in on-prem AD and synced in Azure AD, so for the user synced in on-prem AD you cannot change his job attribute (only user 3 and user 2 job attribut can be changed)

upvoted 1 times

⊟ **hml_2024** 3 months, 2 weeks ago

Key Points:
- **User1** is a member and is directory-synced.
- **User2** is a member but is not directory-synced.
- **User3** is a guest and not directory-synced.

Configuration of Job Title Property:
The **Job title property** is available for **cloud-only** users (i.e., users who are not directory-synced). Therefore, this property can be configured for **User2** and **User3**.

The correct answer for the **Job title property** is:
- **User2 and User3 only**

Configuration of Usage Location Property:
The **Usage location property** can be set for both cloud-only and directory-synced users, meaning it can be configured for **User1**, **User2**, and **User3**.

The correct answer for the **Usage location property** is:
- **User1, User2, and User3**

upvoted 3 times

⊟ **RahulX** 10 months, 3 weeks ago

Job title property: User2 and User3 (You can't change the Job title from cloud if its a synced user)
Usage location property: User1, User2 and User3.

upvoted 1 times

⊟ **Shuihe** 1 year ago

1. User2 and User3
2. User1, 2, 3

upvoted 1 times

⊟ **JCkD4Ni3L** 1 year, 2 months ago

I do this often,
1. User2/user3 only, you can't modify job title on synced user in Entra ID.
2. User1/user/2/user3

upvoted 4 times

⊟ **Silusha** 1 year, 3 months 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 year, 2 months ago

Correct answer:
- U2 and U3
- U1, U2 and U3

upvoted 1 times

⊟ **StarMe** 1 year, 4 months 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** 1 year, 4 months ago

1. User2 and User3 only

2. User1, User2 and User3

upvoted 1 times

⊟ **Heshan** 1 year, 5 months ago

On the exam, 09/07/2023

upvoted 3 times

⊟ **Sango** 1 year, 6 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** 1 year, 6 months ago

Job Title : User2 and User3 only

Usage Location: User1,User2 and User3

upvoted 1 times

⊟ **ShoaibPKDXB** 1 year, 7 months ago

Correct: 1. User2 and User3 only

2. User1, User2 and user3

upvoted 1 times

⊟ **ShoaibPKDXB** 1 year, 7 months ago

1. User and User 3 only

2. User1, User2 and User3

upvoted 1 times

⊟ **ShoaibPKDXB** 1 year, 7 months ago

Correct

upvoted 1 times

⊟ **rajbne** 1 year, 8 months ago

Please update the final answer as per discussion ?

upvoted 1 times

Question #31 *Topic 1*

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 add1 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.

Suggested 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 (96%) 4%

⊟ **Hot_156** Highly Voted 2 years, 3 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 20 times

⊟ **RahulX** 10 months, 3 weeks ago
The User Administrator role is no longer allowed to manage catalogs and access packages in Microsoft Entra Entitlement Management. Please transition to the Identity Governance Administrator role to continue managing access without disruption, or go to the Entitlement Management settings
upvoted 3 times

⊟ **syougun200x** 1 year, 3 months ago
Thank you. As of today, the same sentence can be seen in the setting section.
upvoted 1 times

⊟ **referme** Highly Voted 2 years, 4 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

⊟ **ColdCut** Most Recent 1 month, 3 weeks ago
The correct answer is:

C. From the Identity Governance blade, modify the Entitlement management settings.

Explanation:
In Azure AD, catalog management permissions are primarily handled through Entitlement Management within the Identity Governance blade. By modifying Entitlement Management settings, you can allow specific users, like User1, to create catalogs and manage resources in the catalogs they own.

Entitlement Management is designed to streamline and secure resource access across different catalogs, including setting policies on who can create or manage catalogs.
The Roles and administrators blade is generally for managing roles that control administrative permissions across Azure AD but doesn't provide catalog creation permissions directly.
Option C aligns with the goal of enabling catalog creation and resource management for User1.
upvoted 1 times

⊟ **mohamedbenamor** 2 months ago

Selected Answer: D

Answer is D : Identity Governance -> Catalogs > Roles & admins
upvoted 2 times

⊟ **EmnCours** 1 year, 5 months ago

Selected Answer: C

https://portal.azure.com/#view/Microsoft_AAD_ERM/DashboardBlade/~/elmSetting

Correct. C
upvoted 1 times

⊟ **dule27** 1 year, 6 months ago

Selected Answer: C

C. From the Identity Governance blade, modify the Entitlement management settings.
upvoted 1 times

⊟ **ShoaibPKDXB** 1 year, 7 months ago

Selected Answer: C

Correct. C
upvoted 1 times

⊟ **eleazarrd** 1 year, 8 months 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** 1 year, 9 months 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]** 2 years ago

Selected Answer: C

Correct answer is C.
upvoted 1 times

⊟ **Imee** 2 years, 3 months ago

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

upvoted 3 times

⊟ **Hot_156** 2 years, 3 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** 2 years, 3 months ago

The Answer is D my Friend

upvoted 1 times

⊟ **Hot_156** 2 years, 3 months ago

test it and then come back and tell us what was the result :)

upvoted 3 times

⊟ **Ltf** 2 years, 3 months ago

Seems it's D

upvoted 3 times

Question #32 | *Topic 1*

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.

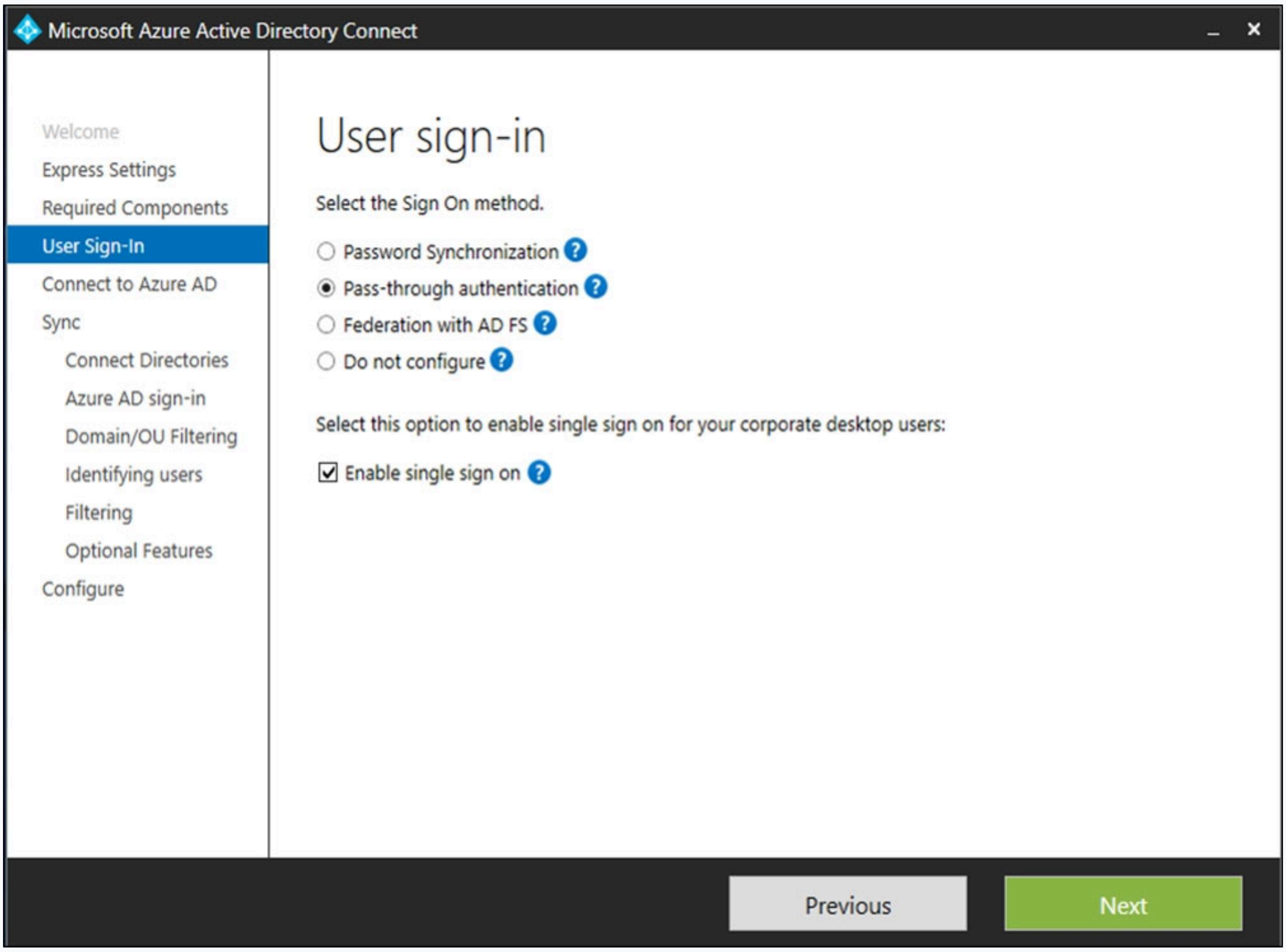
C. Modify the Local intranet Zone settings.

D. Install the Azure AD Connect Authentication Agent.

Suggested Answer: *A*

Enable Seamless SSO through Azure AD Connect.

At the User sign-in page, select the Enable single sign on option.



User sign-in

Select the Sign On method.

○ Password Synchronization

● Pass-through authentication

○ Federation with AD FS

○ Do not configure

Select this option to enable single sign on for your corporate desktop users:

☑ Enable single sign on

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%)

ShinoIgarashi Highly Voted 2 years, 4 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 28 times

jack987 2 years ago

I agree, the correct answer is C.

upvoted 2 times

Taigr 1 year, 10 months 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 1 year, 10 months 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

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

The correct answer is:

C. Modify the Local intranet Zone settings.

Explanation:
To configure Windows 10 computers for Azure AD Seamless Single Sign-On (Seamless SSO), you need to ensure that users' credentials are automatically passed from their Windows session to Azure AD when accessing cloud resources. This is achieved by configuring the Local intranet zone settings in Internet Explorer or Edge.

Azure AD Seamless SSO works by authenticating users seamlessly without prompting for credentials when they access resources in Azure AD. However, for it to work, the Azure AD URLs (like https://autologon.microsoftazuread-sso.com) must be trusted by the browsers on the Windows 10 machines. This is achieved by adding the URLs to the Local intranet zone.
Option A (Configuring Sign-in options) and Option B (Enabling Enterprise State Roaming) are not related to enabling Seamless SSO.
Option D (Installing the Azure AD Connect Authentication Agent) is also incorrect, as the Authentication Agent is used for Pass-through Authentication (PTA) rather than Seamless SSO.
Therefore, Option C is the correct choice to ensure Azure AD Seamless SSO works on Windows 10 computers.

upvoted 1 times

emartiy 9 months, 1 week ago

Selected Answer: C

A for implementing Single Sign-on... Question asks what you need to configure on client side.. so, intranet zone links is the only option for this question..

upvoted 1 times

emartiy 9 months, 1 week ago

Selected Answer: C

Seamless SSO > ıntranet Zone settings... read more.

upvoted 1 times

Er_01 11 months, 2 weeks ago

I would agree with A being answer as it is the only option but moves the process along but configuring Azure AD option does not "configure the windows 10 client to support SSO".
It configures the Azure AD connect server to enable the option on the server, not the windows 10 client. Typical MS question.

upvoted 1 times

maneeshs 1 year, 2 months ago

Answer is C

upvoted 1 times

BenLam 1 year, 2 months 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 year, 2 months ago

Selected Answer: C

As in the previous page, answer is C.

upvoted 2 times

sherifhamed 1 year, 3 months 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 2 times

sherifhamed 1 year, 3 months 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 3 times

> **jtlucas99** 8 months, 3 weeks ago
>
> Copilot says: 1. Ensure Prerequisites are Met: Your environment must meet certain prerequisites, which typically include:
> ○ Azure AD Connect must be installed and configured.
> ○ The computers must be part of an Active Directory domain.
> ○ The Azure AD tenant must be configured for Seamless SSO.
> 2. Enable Seamless SSO: This is done through Azure AD Connect. During the setup, there's an option to enable Seamless SSO. You need to whitelist all the required URL and Endpoints for Azure AD SSO.
> 3. Configure Intranet Zone Settings: You need to add the Azure AD URL to the intranet zone in Internet Explorer/Edge settings to allow for automatic sign-in. This can be done via Group Policy.
> 4. Roll Out the Feature: Gradually roll out Seamless SSO to your users using Group Policy and test it thoroughly.
>
> upvoted 2 times

amurp35 1 year, 4 months ago

Selected Answer: C

Answer is C

upvoted 1 times

EmnCours 1 year, 5 months ago

Selected Answer: C

I agree, the correct answer is C.

upvoted 1 times

dule27 1 year, 6 months ago

Selected Answer: C

C. Modify the Local intranet Zone settings.

upvoted 1 times

ShoaibPKDXB 1 year, 7 months ago

Selected Answer: C

C is correct

upvoted 1 times

DCT 1 year, 10 months ago

walao, answer is C la, sohai

upvoted 1 times

mayleni 1 year, 11 months ago

Selected Answer: C

C is correct also a similar question has the similar answer. Local intranet zone

upvoted 2 times

⊟ **Halwagy** 1 year, 11 months ago

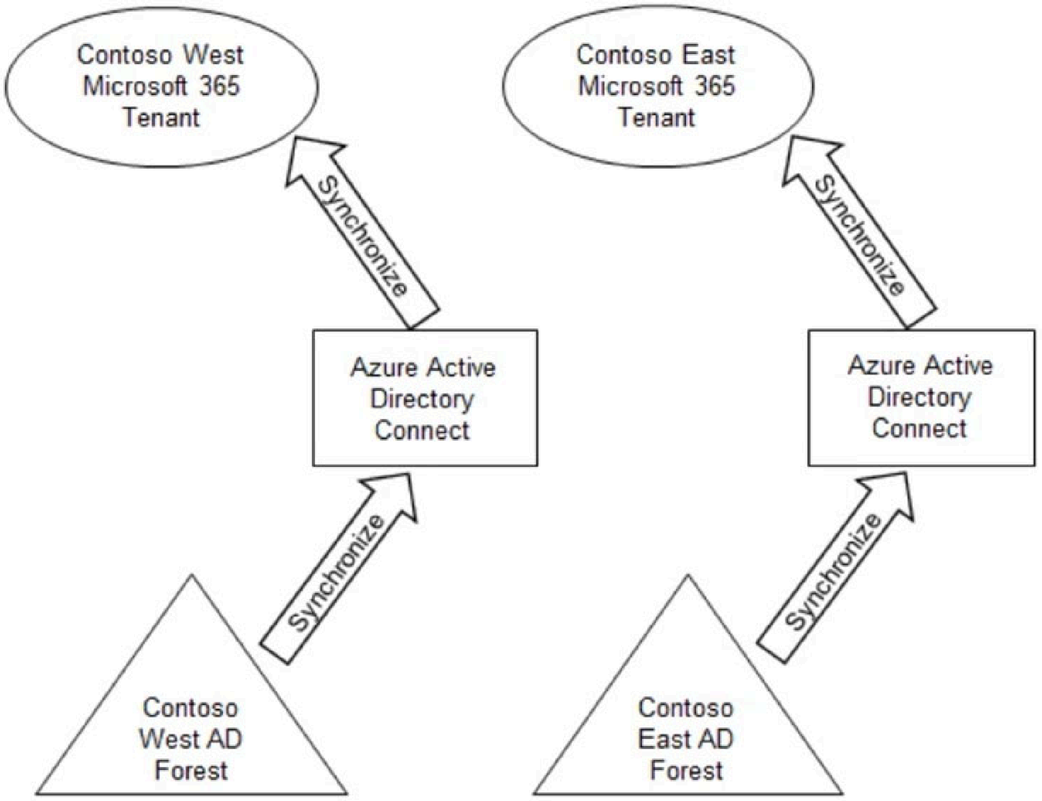
Selected Answer: C

Modify the Local intranet Zone settings. as the question asking what you should do over Windows 10 device

upvoted 2 times

Question #33 Topic 1

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.


Contoso West Microsoft 365 Tenant
Contoso East Microsoft 365 Tenant
Synchronize
Synchronize
Azure Active Directory Connect
Azure Active Directory Connect
Synchronize
Synchronize
Contoso West AD Forest
Contoso East AD Forest

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.

Suggested 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 2 years, 1 month ago
it should be stated as answer: configure cross-tenant access settings
upvoted 7 times

⊟ **Holii** 1 year, 6 months 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

taer Highly Voted 👍 2 years, 3 months ago

Selected Answer: B

Correct Answer: B

upvoted 5 times

ColdCut Most Recent ⏱ 1 month, 3 weeks ago

The correct answer is:

B. Invite the Contoso East users as guests in the Contoso West tenant.

Explanation:
To grant users from Contoso East access to SharePoint Online sites in the Contoso West tenant without requiring additional Microsoft 365 licenses, inviting the Contoso East users as guest users in the Contoso West tenant is the most efficient and cost-effective solution. Here's why:

Guest Access in Microsoft 365: By using Azure AD's B2B collaboration feature, you can invite users from one Azure AD tenant as guests in another tenant. This provides them access to resources like SharePoint Online without the need for extra Microsoft 365 licenses in the Contoso West tenant.
No Need for Additional Synchronization or Infrastructure Changes: Options C and D involve complex configuration changes, like setting up additional Azure AD Connect sync configurations, which are unnecessary for providing basic access.
No Need for Application Proxy: Option A is incorrect because Azure AD Application Proxy is used to provide remote access to on-premises applications, not to share resources between two Azure AD tenants.
Thus, Option B meets the requirement by providing access without additional licensing or complex configurations.

upvoted 3 times

RahulX 10 months, 3 weeks ago

B. Invite the Contoso East users as guests in the Contoso West tenant.

upvoted 2 times

EmnCours 1 year, 5 months ago

Correct Answer: B

upvoted 1 times

dule27 1 year, 6 months ago

Selected Answer: B

B. Invite the Contoso East users as guests in the Contoso West tenant.

upvoted 1 times

haskelatchi 1 year, 7 months ago

B for Bob

upvoted 1 times

ShoaibPKDXB 1 year, 7 months ago

Selected Answer: B

B is correct

upvoted 1 times

[Removed] 2 years 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

Question #34 *Topic 1*

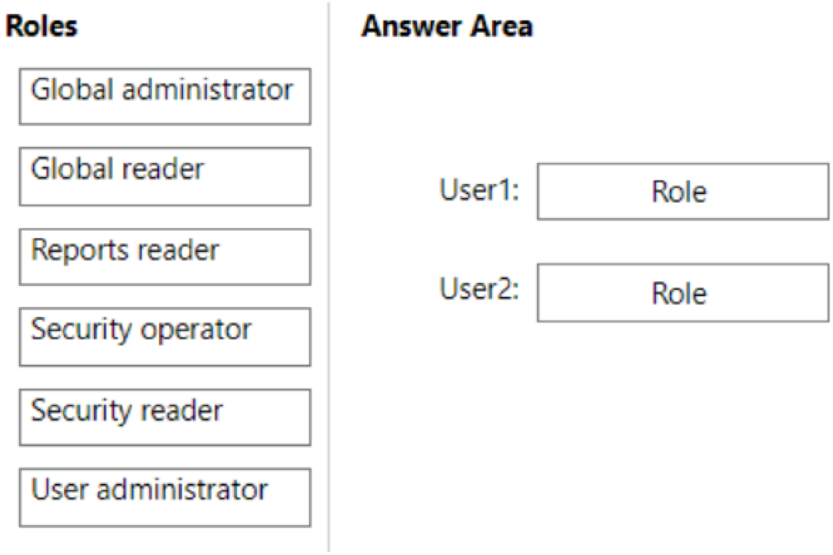
DRAG DROP
-

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

Global administrator

Global reader

Reports reader

Security operator

Security reader

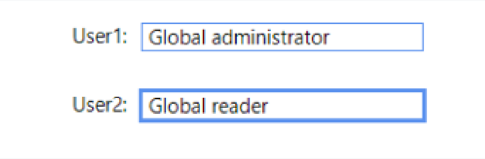
User administrator

Answer Area

User1: Role

User2: Role

Suggested Answer:



User1: Global administrator

User2: Global reader

⊟ **Halwagy** Highly Voted 1 year, 11 months ago

User 1 : User Administrator

User 2 : Security Reader

upvoted 50 times

⊟ **klayytech** 8 months, 2 weeks ago

https://learn.microsoft.com/en-us/entra/id-governance/deploy-access-reviews#who-will-create-and-manage-access-reviews

Global Admin

Global Reader

security reader does not have permission to read the history for Azure resource roles

upvoted 4 times

⊟ **klayytech** 9 months, 1 week ago

Read access review of a group or of an app

Least privileged role = Security Reader

Additional roles= Security Administrator

User Administrator

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-by-task#enterprise-applications

upvoted 4 times

⊟ **HaubeRR89** 3 weeks, 1 day ago

User 1 : User Administrator

User 2 : Global Reader

Global Administrator, Identity Governance Administrator, and Global Reader can see history reports for all access reviews. All other users are only allowed to see reports on access reviews that they generate.

https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-downloadable-review-history

upvoted 1 times

⊟ **oscarpopi** 1 year, 11 months ago

Correct

upvoted 3 times

⊟ **doch** Highly Voted 1 year, 11 months ago

User Admin

Security Reader

Ref: https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task

upvoted 25 times

⊟ **oscarpopi** 1 year, 11 months ago

Correct, that's a nice article, I'll bookmark it

upvoted 3 times

⊟ **Frank9020** Most Recent 2 weeks, 3 days ago

User1: User administrator: Allows managing users, groups, and access reviews, but does not provide global admin rights.

User2: Reports reader: Allows access to reports and analytics without administrative permissions, aligning with least privilege.

upvoted 1 times

⊟ **ColdCut** 1 month, 3 weeks ago

The correct answer is:

User1: User administrator

User2: Global reader

Explanation:

User1 needs to create access reviews for groups. To create access reviews, the User administrator role is appropriate. The User administrator can manage user settings, including group memberships and access reviews.

User2 needs to review the history report for all completed access reviews. The Global reader role allows users to view reports and other information across Microsoft 365 without granting them permissions to make any changes. This role aligns with the requirement for reviewing access review history, as it provides read-only access.

Resource Links:

For more details about roles and permissions:

User Administrator role

Global Reader role

upvoted 1 times

⊟ **AlexBrazil** 2 months ago

According to https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-by-task,

User1: User Administrator

"Create, update, or delete access review of a group or of an app"

User2: Security Reader

"Read access review of a Microsoft Entra role"

upvoted 1 times

⊟ **BRZSZCL** 2 months, 1 week ago

To ensure the least privilege principle is followed for each user:

User1 needs to create access reviews for groups. The appropriate role for this task is User Access Administrator because it allows users to create and manage access reviews in Azure AD.

User2 needs to review the history report for all completed access reviews. The role required for this is Reports Reader, which allows viewing reports without granting the ability to create or manage the reviews themselves.

Summary:
User1: User Access Administrator
User2: Reports Reader
upvoted 3 times

⊟ **hml_2024** 3 months, 2 weeks ago
To meet the requirements while adhering to the principle of least privilege, you should assign the following roles:

- **User1**: Assign the **User Administrator** role. This role allows User1 to create access reviews for groups¹.
- **User2**: Assign the **Global Reader** role. This role allows User2 to review the history report for all completed access reviews without granting any additional administrative permissions².
upvoted 1 times

⊟ **cluocal** 4 months ago
User1: User Admin (Create, update, or delete access review of a group or of an app)
User 2: Security Reader (Read access review of a group or of an app)

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-by-task
upvoted 3 times

⊟ **srysgbvjumozmail** 4 months, 4 weeks ago
User 1 : User Administrator
User 2 : Security Reader

https://learn.microsoft.com/en-us/entra/id-governance/deploy-access-reviews#who-will-create-and-manage-access-reviews
upvoted 2 times

⊟ **klayytech** 8 months, 2 weeks ago
https://learn.microsoft.com/en-us/entra/id-governance/deploy-access-reviews#who-will-create-and-manage-access-reviews
Global Admin
Global Reader
security reader does not have permission to read the history for Azure resource roles
upvoted 1 times

⊟ **Discuss4certi** 6 months ago
Neither can a global reader. You need to be assigned the permissions for that resource. Therefore since it's not stated go for user admin for the creation of access review and security reader for the reports.
upvoted 1 times

⊟ **ItzVerified** 8 months, 2 weeks ago
User 1 : User Administrator
User 2 : Security Reader
upvoted 3 times

⊟ **jtlucas99** 8 months, 3 weeks ago
Per Copilot: In Azure Active Directory (Azure AD), you can assign different roles to users to manage access reviews.

For User1, you should assign the Access Review Contributor role. This role allows the user to create and manage access reviews, but it doesn't allow them to make decisions on behalf of reviewers.
For User2, you should assign the Access Review Reader role. This role allows the user to read access reviews and their decisions, but they can't create, update, or delete access reviews.
These roles follow the principle of least privilege, granting only the necessary permissions to each user for their specific tasks.
upvoted 1 times

⊟ **klayytech** 9 months, 1 week ago
Read access review of a group or of an app
Least privileged role = Security Reader
Additional roles= Security Administrator
User Administrator

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-by-task#enterprise-applications

upvoted 2 times

emartiy 9 months, 1 week ago

User1: User Admin

User 2: security Reader

upvoted 2 times

RahulX 10 months, 3 weeks ago

Create, update, or delete access review of a group or of an app (User Administrator)

Read access review of a group or of an app (Security Reader).

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

upvoted 1 times

Er_01 1 year ago

The question states least privilege as a requirement so GA/GR is does fit this.

User 1 : User Administrator

User 2 : Security Reader

upvoted 1 times

poesklap 1 year, 1 month ago

https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-downloadable-review-history

Global Admin

Global Reader

upvoted 3 times

curtmcgirt 1 year ago

no. that article is about __history reports__ for access reviews, rather than about access reviews themselves. the specific sentence you read is poorly written, and should probably read "Global Administrator and Global Reader can see --history reports of -- all access reviews."

upvoted 2 times

Question #35 *Topic 1*

HOTSPOT
-

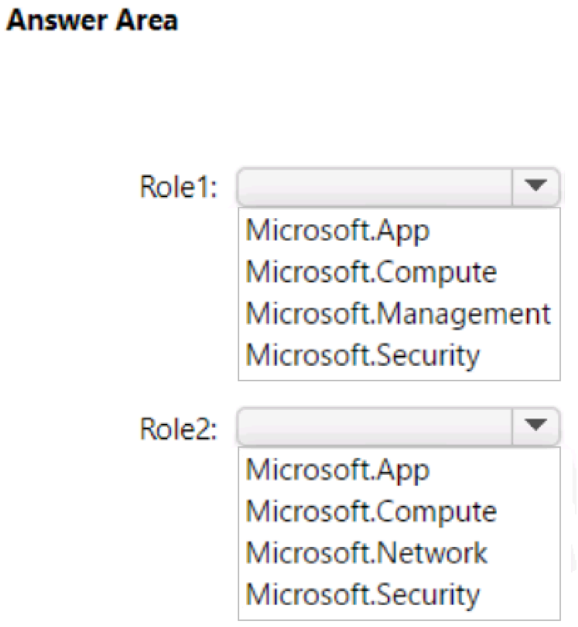
You have an Azure subscription.

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.

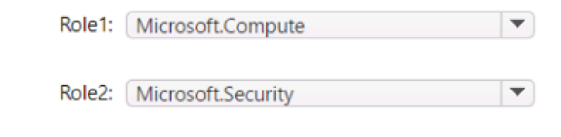


Answer Area

Role1:
- Microsoft.App
- Microsoft.Compute
- Microsoft.Management
- Microsoft.Security

Role2:
- Microsoft.App
- Microsoft.Compute
- Microsoft.Network
- Microsoft.Security

Suggested Answer:



Role1: Microsoft.Compute

Role2: Microsoft.Security

⊟ **dejo** Highly Voted 1 year, 11 months 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 27 times

⊟ **ThotSlayer69** Highly Voted 1 year, 11 months 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 9 times

ColdCut Most Recent 1 month, 3 weeks ago

The correct answer is:

Role1: Microsoft.App
Role2: Microsoft.Security
Explanation:
Role1 requires permissions to create or delete instances of Azure Container Apps. The relevant resource provider for Azure Container Apps is Microsoft.App. This provider includes the necessary permissions to manage container app instances.
Role2 needs to enforce adaptive network hardening rules, which are part of Azure Security Center's capabilities. The Microsoft.Security resource provider contains the permissions required to enforce adaptive network hardening and other security-related configurations.
Resource Links:
For more details on Azure resource providers and roles:

Microsoft.App resource provider
Microsoft.Security resource provider

upvoted 2 times

Labelfree 1 month, 3 weeks ago

The answer here is wrong. It is Role 1: Microsoft.App, not compute -

Given these options, here are the appropriate resource provider permissions for each role:

Role1 (Create or delete instances of Azure Container Apps):

Microsoft.App/containerApps/write: Allows creating or updating Azure Container Apps.
Microsoft.App/containerApps/delete: Allows deleting Azure Container Apps.
Role2 (Enforce adaptive network hardening rules):

Microsoft.Security/adaptiveNetworkHardenings/write: Allows enforcing adaptive network hardening rules.
Microsoft.Security/adaptiveNetworkHardenings/read: Allows reading adaptive network hardening rules.
These permissions ensure that users assigned to Role1 can manage Azure Container Apps, while users assigned to Role2 can enforce network security rules effectively.

upvoted 2 times

BRZSZCL 2 months, 1 week ago

To create custom roles that meet the specified requirements, you need to ensure the correct permissions are applied for each role.

Role1: Create or delete instances of Azure Container Apps
For Role1, users need permissions related to managing Azure Container Apps. The correct resource provider and permission are:

Microsoft.App/containerApps/write: This permission allows users to create and delete Azure Container Apps instances. It provides the necessary capability for Role1.
Role2: Enforce adaptive network hardening rules
For Role2, users need permissions related to adaptive network hardening, which is part of Microsoft Defender for Cloud. The correct resource provider and permission are:

Microsoft.Security/adaptiveNetworkHardenings/write: This permission allows users to enforce adaptive network hardening rules. It fits the requirement for Role2, providing users with the ability to manage these security rules.
Summary:
Role1: Microsoft.App/containerApps/write
Role2: Microsoft.Security/adaptiveNetworkHardenings/write

upvoted 2 times

hml_2024 3 months, 2 weeks ago

To meet the requirements for creating the custom roles, you need to assign the following resource provider permissions:

Role1: Create or delete instances of Azure Container Apps

Microsoft.App: This resource provider includes the necessary permissions to manage Azure Container Apps1.

Role2: Enforce adaptive network hardening rules

Microsoft.Security: This resource provider includes the necessary permissions to manage and enforce adaptive network hardening rules2.

upvoted 2 times

RahulX 10 months, 3 weeks ago

Role1: Microsoft.App (for containers).

Role2: Microsoft.Security.

upvoted 2 times

Siraf 1 year ago

- Role 1: Microsoft.App
- Role 2: Microsoft.Security.

Deploy container app using the Azure portal:

Make sure to have the Resource Provider "Microsoft.App" registered. https://learn.microsoft.com/en-us/azure/container-apps/quickstart-portal#prerequisites.

Adaptive Network Hardening --> Microsoft.Security/adaptiveNetworkHardenings/read

resource provider is Microsoft.Security:

https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftsecurity

upvoted 3 times

marcoby 1 year, 3 months 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 3 times

StarMe 1 year, 4 months 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 1 year, 5 months ago

Role 1: Microsoft.App

Role 2 : Microsoft.Security

upvoted 3 times

dule27 1 year, 6 months ago

Role 1: Microsoft.App

Role 2 : Microsoft.Security

upvoted 2 times

ShoaibPKDXB 1 year, 7 months ago

Correct: 1. Microsoft.Apps

2. Microsoft.Security

upvoted 3 times

kanew 1 year, 8 months ago

Role 1: Microsoft.App microsoft.app/containerapps/delete microsoft.app/containerapps/write

Role 2: Microsoft.Secuirty Microsoft.Security/adaptiveNetworkHardenings/enforce/action

upvoted 4 times

sbnpj 1 year, 8 months 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** 1 year, 9 months ago

ChatGPT says its:

Role 1: Compute

Role 2: Network

upvoted 1 times

⊟ **thadeus** 1 year, 9 months ago

Seriously? Because it told me ".App" for Role1 and ".Network" for Role2.

upvoted 1 times

⊟ **Holii** 1 year, 6 months 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

⊟ **Arjanussie** 1 year, 10 months ago

It is Microsoft.compute.......ask chatgpt what is in graph microsoft.compute and what is in graph microsoft.app

upvoted 1 times

⊟ **Holii** 1 year, 6 months 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 Create or update a Container App

microsoft.app/containerapps/delete Delete a Container App

upvoted 1 times

Question #36 Topic 1

HOTSPOT

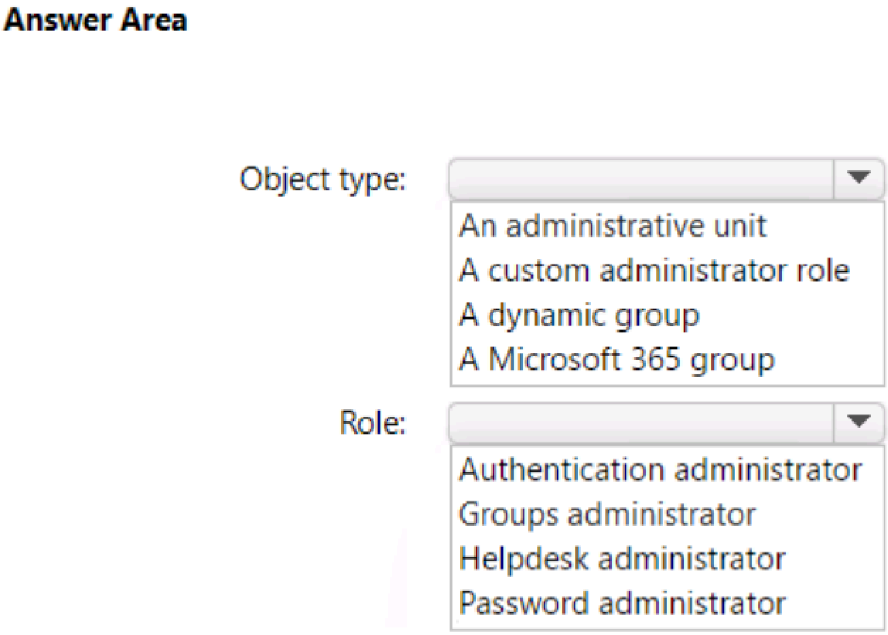
-

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.

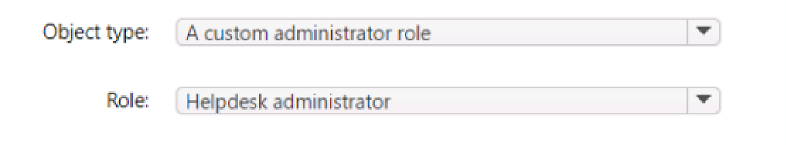


Answer Area

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

Suggested Answer:



Object type: A custom administrator role

Role: Helpdesk administrator

⊟ **Halwagy** Highly Voted 1 year, 11 months ago

Correct Answer:

Object Type: Administrative Unit

Role: Authentication administrator

upvoted 72 times

⊟ **skbudhram** Highly Voted 1 year, 10 months ago

Sheesh this site has a lot of wrong answers, what's the point even ..

upvoted 29 times

⊟ **Davito** Most Recent 2 months ago

The key part of this question is the requirement that these settings be changed or managed for ONLY the executives. From the who can reset passwords page (https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-assign-roles#roles-that-can-be-assigned-with-administrative-unit-scope) it notes that additional restrictions apply to roles scoped to administrative units.

Once you create an AU there is then a smaller selection of eligible roles that can be assigned, and the further restrictions page (https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-assign-roles#roles-that-can-be-assigned-with-administrative-unit-scope) states that the Authentication Administrator "Has access to view, set, and reset authentication method information for any non-admin user in the assigned administrative unit ONLY." This accomplishes our goal of ensuring the administrator permissions would only extend to members of of the AU (executives).

Therefore the answer is: Administrative Unit & Authentication Administrator

upvoted 4 times

BRZSZCL 2 months, 1 week ago

To meet the requirement of allowing the support team to reset passwords and manage MFA settings for only the executives while adhering to the principle of least privilege, you can follow this approach:

Object Type: Azure AD Group

You should use an Azure AD group to define the executives as a specific set of users. Create a group that contains only the 100 executives, which will limit the scope of operations to this group.

Azure AD Role: Authentication Administrator

Assign the Authentication Administrator role to the support team for this specific group. This role allows resetting passwords, managing multi-factor authentication (MFA) settings, and configuring authentication policies, but only for the users within the assigned scope (in this case, the executives group).

Summary:

Object Type: Azure AD Group

Azure AD Role: Authentication Administrator

upvoted 2 times

josemariamr 1 month ago

Copilot: To ensure that the support team can reset passwords and manage multi-factor authentication (MFA) settings for only the executives while adhering to the principle of least privilege, you should use the following:

Object Type: Create a group in Azure AD that includes only the executives.

Azure AD Role: Assign the Authentication Administrator role to the support team members. This role allows them to reset passwords and manage MFA settings, but only for users who are assigned to specific roles or groups.

By creating a group for the executives and assigning the Authentication Administrator role to the support team, you ensure that the support team has the necessary permissions to manage only the executives' accounts without having broader access

upvoted 1 times

hml_2024 3 months, 2 weeks ago

To ensure that the support team can reset passwords and manage multi-factor authentication (MFA) settings for only the executives while adhering to the principle of least privilege, you should use:

Object Type: 1. An Administrative Unit

Role: 1. Authentication Administrator

upvoted 2 times

MISCOLO 7 months ago

no such thing as a custom admin role

upvoted 2 times

SamuelPerezMartin 5 months, 3 weeks ago

Microsoft Entra allows you to create custom admin roles.

upvoted 3 times

HartMS 8 months, 3 weeks ago

AU

Authentication Administrator

upvoted 3 times

b0tag 1 year, 4 months 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 5 times

DasChi_cken 1 year, 2 months 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 Passworts and regarding least privileg this IS the best role

upvoted 5 times

EmnCours 1 year, 5 months ago

Object Type: Administrative Unit
Role: Authentication administrator

upvoted 3 times

dule27 1 year, 6 months ago

Object Type: An Administrative Unit
Role: Authentication Administrator

upvoted 3 times

b233f0a 1 year, 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 2 times

dule27 1 year, 6 months ago

Object Type: An administrative unit
Role: Authentication administrator

upvoted 5 times

ShoaibPKDXB 1 year, 7 months ago

Correct: Object Type: An Administrative Unit
Role: Authentication Administrator

upvoted 1 times

rajbne 1 year, 8 months ago

Please update final answer

upvoted 2 times

Remus999 1 year, 8 months 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 2 times

Akakentavr 1 year, 11 months 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 1 year, 11 months ago

Object Type: Administrative Unit
Role: Authentication administrator

upvoted 1 times

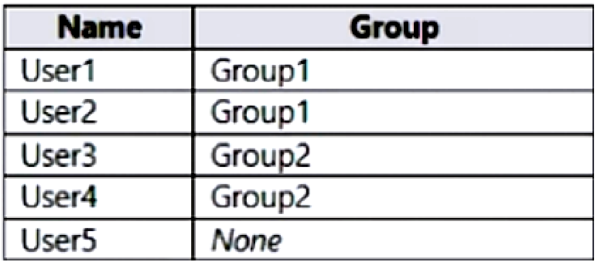
ExamStudy68 1 year, 8 months ago

Maybe it's by design to force discussion and make you think about it or look it up... Not sure really.

upvoted 1 times

Question #37 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

Halwagy Highly Voted 1 year, 11 months 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 37 times

CloudRat Highly Voted 1 year, 11 months 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 5 times

Labelfree Most Recent 1 month, 3 weeks ago

Funny, Co-pilot got this wrong until you copy community notes from here and ask, so is everyone wrong here? it then Agrees with D suddenly. Prior to that it answers A is correct. Here's what it originally output that is 'incorrect' - In Azure Active Directory (Azure AD), a User administrator assigned to an administrative unit (AU) can manage users within that AU. Given the details:

AU1 includes Group1, User2, and User3.

User5 is the User administrator for AU1.

User5 can reset passwords for:

User2 (direct member of AU1)

User3 (direct member of AU1)

User1 (indirect member via Group1, which is part of AU1)

User5 cannot reset passwords for User4 and User5, as they are not part of AU1.

upvoted 2 times

PrismaConsultores 2 months ago

Selected Answer: D

Respuesta correcta D

upvoted 1 times

Futfuyfyjfj 7 months, 2 weeks ago

Selected Answer: D

Assigning groups to an Administrative Unit only assigns/gives permissions to those groups, not to the members of those groups

upvoted 2 times

cyberchef192 10 months ago

Obvious, you cant change password of a group only users, duuuuh!

upvoted 3 times

haazybanj 1 year, 2 months ago

Why is User1 not included?

upvoted 2 times

> **Nyamnyam** 1 year, 1 month ago
>
> Because of what Halwagy has quoted and referenced above ;)
>
> upvoted 2 times

EmnCours 1 year, 4 months ago

Selected Answer: D

User2 and User3 only

upvoted 2 times

Husterix 1 year, 6 months ago

Selected Answer: D

D is the correct answer: the admin role only works on directly added members to the AU.

upvoted 5 times

dule27 1 year, 6 months ago

Selected Answer: D

User2 and User3 only

upvoted 2 times

ShoaibPKDXB 1 year, 7 months ago

Selected Answer: D

D is correct

upvoted 1 times

oscarpopi 1 year, 11 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#operator-precedence

upvoted 1 times

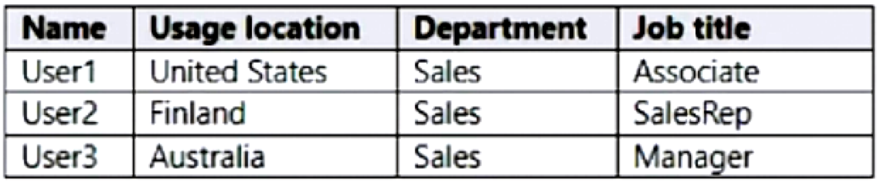
divyakanth 1 year, 11 months ago

can i say that AU is alos a Group and since addidng 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 n ot be added and the other users were directly added and so the admin can act on them

upvoted 1 times

Question #38 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (78%) A (22%)

ydecac Highly Voted 1 year, 11 months 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 30 times

[Removed] 1 year, 8 months 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 18 times

Nyamnyam 1 year, 1 month 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 3 times

Er_01 11 months ago

Based on my current repro of it, user 1 and 2 are correct. Hinges on the separation of the and not not and or operators. However, you have to manually edit the expression to even come up with this gotcha question. Using the UI it fails. You have to add the brackets in part 1 and the not operator, which is bad syntax. In short it was a badly designed question using double negative in part 3. Should have used -ne. Typical MS worthless gotcha question.

upvoted 3 times

Justin0020 8 months, 4 weeks ago

You have to think about it to realise that the OR statement adds User2 as well. User 1 and 2, option D is right.

upvoted 4 times

⊟ **meself7** Highly Voted 👍 1 year, 11 months ago

Selected Answer: D

D is correct

always resolve acording 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 22 times

⊟ **BRoald** 1 year, 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 15 times

⊟ **Holii** 1 year, 6 months 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 4 times

⊟ **Labelfree** 1 month, 3 weeks ago

This is what Copilot says | The OR flag, basically negates the need to be included under the usage location. if there was no OR flag, they would need to be in US or Australia, but since there's a condition "OR Job Title: SalesRep" that's all that is needed to include them.

upvoted 1 times

⊟ **Frank9020** Most Recent 🕘 2 weeks, 3 days ago

Selected Answer: A

A. User1 only:
user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager") –or (user.jobTitle -eq "SalesRep")

This rule includes users who:
Have a usage location in “US” or “AU”.
Are in the Sales department.
Are not Managers.
Or have the job title “SalesRep”:
User1: Located in the United States, department is Sales, job title is Associate.
Meets the location (US) and department (Sales) criteria, and is not a Manager.
User2: Located in Finland, department is Sales, job title is SalesRep.
Does not meet the location criteria (Finland), but meets the job title “SalesRep”.
User3: Located in Australia, department is Sales, job title is Manager.
Meets the location (AU) and department (Sales) criteria, but is excluded because HE is a Manager..

upvoted 2 times

⊟ **Labelfree** 4 weeks, 1 day ago

Selected Answer: D

Tested D is correct. Have to replace dashes with hyphen's for code to work properly.

(user.usageLocation -in ["US", "AU"]) -and

(user.department -eq "Sales") -and
-not (user.jobTitle -eq "Manager") -or
(user.jobTitle -eq "SalesRep")

upvoted 1 times

Labelfree 4 weeks, 1 day ago

Selected Answer: A

None of them are right, but if you enter the Dyn group code in proper format it only pulls User1. Tested, I get an error invalid character using code the provided. After reformatting
to "(user.usageLocation -in ["US","AU"]) -and
(user.department -eq "Sales") -and
((user.jobTitle -ne "Manager") -or (user.jobTitle -eq "SalesRep"))" it only pulls User1

upvoted 2 times

TweedleMB 1 month ago

Selected Answer: D

-and without brackets men's that only one condition is taken to -and

upvoted 1 times

PrismaConsultores 2 months ago

Selected Answer: D

Desglosemos la regla:

user.usageLocation -in ["US", "AU"]: El usuario debe estar en Estados Unidos (US) o Australia (AU).
-and (user.department -eq "Sales"): El usuario debe pertenecer al departamento de ventas (Sales).
-and -not (user.jobTitle -eq "Manager"): El usuario no debe tener el título de trabajo "Manager".
–or (user.jobTitle -eq "SalesRep"): O el usuario debe tener el título de trabajo "SalesRep".

upvoted 1 times

fortunaXI 2 months, 3 weeks ago

D (User1 and user2) is the correct answer. Confirmed in a Test Lab.

upvoted 1 times

Chiragtrapasiya 6 months ago

Selected Answer: D

User1 from user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager")
User2 from or (user. jobTitle -eq "SalesRep")

upvoted 2 times

jsca 8 months ago

Tested this day :
Answer D

upvoted 1 times

vladi72 8 months, 1 week ago

What confusing here is OR statement. To make it simple: OR is not part of NOT it's separate statement. If you read this way answer D is correct.

upvoted 1 times

mkendell 9 months ago

Selected Answer: D

user.usageLocation -in ["US","AU"]: This part checks if the usage location of the user is either in the United States ("US") or Australia ("AU").

-and (user.department -eq "Sales"): It checks if the user's department is "Sales".

-and -not (user.jobTitle -eq "Manager"): This part ensures that the user's job title is not "Manager".

-or (user.jobTitle -eq "SalesRep"): This part checks if the user's job title is "SalesRep".

Putting it all together:

The command checks if the user's usage location is either in the US or Australia, their department is "Sales", and they are not a "Manager". If all these conditions are met, the user is included.

Additionally, if the user's job title is "SalesRep", regardless of the previous conditions, they are also included.

upvoted 2 times

cac91e6 10 months, 3 weeks ago

when you put the command as is in to azure you will get an error ,The actual syntax should be "user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager") or (user.jobTitle -eq "SalesRep")" and this gives us a user1 and user2 i tried it out myself , Poorly designed question

upvoted 2 times

curtmcgirt 1 year ago

Selected Answer: D

((user's location is US or AU) AND (their department is SALES) AND (their job title is NOT Manager))

(OR their job title is SalesRep.)

upvoted 2 times

Siraf 1 year ago

Correct Answer is D.

upvoted 1 times

Alscoran 1 year, 1 month ago

Selected Answer: D

Because of the Or statement

upvoted 1 times

BenLam 1 year, 2 months 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** 1 year, 1 month 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

Question #39 Topic 1

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

Suggested Answer: *D*

Community vote distribution

D (100%)

BRZSZCL Highly Voted 👍 2 months, 1 week ago

D. User Administrator

Reasoning:

The User Administrator role allows users to:

Reset passwords for non-administrators.

Manage licenses (assign and remove licenses).

Create and manage users and groups.

This role combines the capabilities required to manage license assignments and reset user passwords, aligning with the given requirements.

Incorrect Options:

A. Helpdesk Administrator: This role only allows resetting user passwords but not managing licenses.

B. Billing Administrator: This role deals with subscription and billing management, not user licenses or password resets.

C. License Administrator: This role allows managing license assignments but does not permit resetting passwords.

Correct Answer: D. User Administrator

upvoted 5 times

jsca Most Recent 8 months ago

Correct Answer: D

upvoted 2 times

EmnCours 1 year, 5 months ago

Correct Answer: D

upvoted 1 times

dule27 1 year, 6 months ago

Selected Answer: D

D. User administrator

upvoted 1 times

JN_311 1 year, 7 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#user-administrator

upvoted 3 times

SwitchKat 1 year, 7 months 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 4 times

Holii 1 year, 6 months 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 1 year, 6 months ago

Answer is still D. though, because we can't select multiple.

upvoted 1 times

ShoaibPKDXB 1 year, 7 months ago

Selected Answer: D

correct D

upvoted 1 times

itismadu 1 year, 8 months ago

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#helpdesk-administrator

upvoted 1 times

chikorita 1 year, 9 months ago

correct cuz only User Access Admin fits in both the requirement : manage license assignments and reset user passwords.

upvoted 2 times

Aquintero 1 year, 11 months ago

Administrador de Usuarios

upvoted 3 times

jojoseph 1 year, 11 months ago

Selected Answer: D

User Administrator

upvoted 2 times

Halwagy 1 year, 11 months ago

Selected Answer: D

User Administrator

upvoted 3 times

CloudRat 1 year, 11 months ago

D. Is Correct - Neither of the other Roles have permissions to handle all of the statements.

upvoted 3 times

Question #40 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 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

Suggested Answer: *D*

Community vote distribution

A (88%) 13%

mohamedbenamor Highly Voted 2 months ago

Selected Answer: A

now it's : Set-MgUserLicense

https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users.actions/set-mguserlicense?view=graph-powershell-1.0

upvoted 6 times

shuhaidawahab Highly Voted 1 year, 2 months 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 5 times

BRZSZCL Most Recent 2 months, 1 week ago

A. the Set-MsolUserLicense cmdlet

This cmdlet is part of the Microsoft Online Services Module for PowerShell and is specifically designed for managing user licenses in Microsoft 365. With this cmdlet, you can efficiently remove the Office 365 Enterprise E3 licenses from the users.

How it works:

You can use Set-MsolUserLicense to update the licensing for users, including removing or modifying license assignments.

You can script the removal of the E3 licenses from multiple users in bulk.

Other Options:

B. the Set-AzureADGroup cmdlet: This cmdlet is used to manage group properties in Azure AD but is not used for managing licenses.

C. the Set-WindowsProductKey cmdlet: This cmdlet is used for setting Windows product keys and is unrelated to Microsoft 365 licensing.

D. the Administrative units blade in the Azure Active Directory admin center: While administrative units allow you to delegate administrative tasks, they are not directly used for license removal or assignments in bulk.

Correct Answer: A. the Set-MsolUserLicense cmdlet

upvoted 1 times

SynnerG 3 months, 2 weeks ago

what the hell is going on with these answers?

upvoted 3 times

criminal1979 9 months ago

Selected Answer: A

Set-MsolUserLicense is the only way between the proposed answers

upvoted 2 times

Nyamnyam 1 year, 1 month ago

Selected Answer: A

A. is the correct answer

upvoted 2 times

Sandipmcr 1 year, 2 months ago

Selected Answer: A

Set-MsolUserLicense is the only way between the proposed answers

upvoted 2 times

morit2578 1 year, 4 months ago

Selected Answer: A

Set-MsolUserLicense is the only way between the proposed answers

upvoted 2 times

amurp35 1 year, 4 months 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 1 year, 4 months ago

Please update your answer to 'A' the Set-MsolUserLicense cmdlet.
The Administrative Unit is for restriction, setting boundary.

upvoted 2 times

EmnCours 1 year, 4 months ago

Selected Answer: B

A. the Set-MsolUserLicense cmdlet

upvoted 2 times

mali1969 1 year, 6 months 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 1 year, 6 months 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 1 year, 6 months ago

Selected Answer: A

A. the Set-MsolUserLicense cmdlet

upvoted 1 times

H0TDOGG 1 year, 7 months 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** 1 year, 7 months 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 1 year, 7 months ago

Selected Answer: A

Set-MsolUserLicense

upvoted 3 times

Aquintero 1 year, 11 months ago

Selected Answer: A

A. el cmdlet Set-MsolUserLicense

upvoted 1 times

Question #41 *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 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

Suggested Answer: *B*

Community vote distribution

D (100%)

SynnerG 3 months, 2 weeks ago

Selected Answer: D

in no way is the Identity Governance blade in the Azure Active Directory admin center even close to being the right answer. What is going on with these answers?

upvoted 1 times

SynnerG 3 months, 2 weeks ago

in no way is the Identity Governance blade in the Azure Active Directory admin center even close to being the right answer. What is going on with these answers?

upvoted 2 times

07d6037 7 months ago

Selected Answer: D

Opcion D

upvoted 1 times

jsca 8 months ago

D. the Set-MsolUserLicense cmdlet

upvoted 2 times

jtlucas99 8 months, 2 weeks ago

*Add

Set-MsolUserlicenses cmdlt is depricated. Go to: Connect-MgGraph -Scopes

- Set-MgUserLicense <UserID or UPN> Addlicenses @ {<SKUId = "xxxx"} RemoveLicenses @ ()

*Remove

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

upvoted 4 times

Nyamnyam 1 year, 1 month ago

Selected Answer: D

Oh, come on, contributors - Identity Governance blade is about Entitlement Management and Access Reviews. No licensing management there.

upvoted 3 times

shuhaidawahab 1 year, 2 months 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 1 year, 3 months ago

Selected Answer: D

Plz check these questions: Q25, Q40,Q41,Q43.and Q53
upvoted 3 times

sherifhamed 1 year, 3 months 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 4 times

dule27 1 year, 6 months ago

Selected Answer: D

D. the Set-MsolUserLicense cmdlet
upvoted 2 times

ShoaibPKDXB 1 year, 7 months ago

Selected Answer: D

D is correct
upvoted 2 times

AmplifiedStitches 1 year, 8 months 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 1 year, 8 months ago

If Set-MsolUseLicense 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 2 times

AAsif098 1 year, 10 months 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** 1 year, 10 months 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** 1 year, 11 months ago

Selected Answer: D

D. el cmdlet Set-MsolUserLicense

upvoted 2 times

⊟ **mayleni** 1 year, 11 months ago

Selected Answer: D

the same question again! Is D

upvoted 2 times

Question #42 Topic 1

HOTSPOT

-

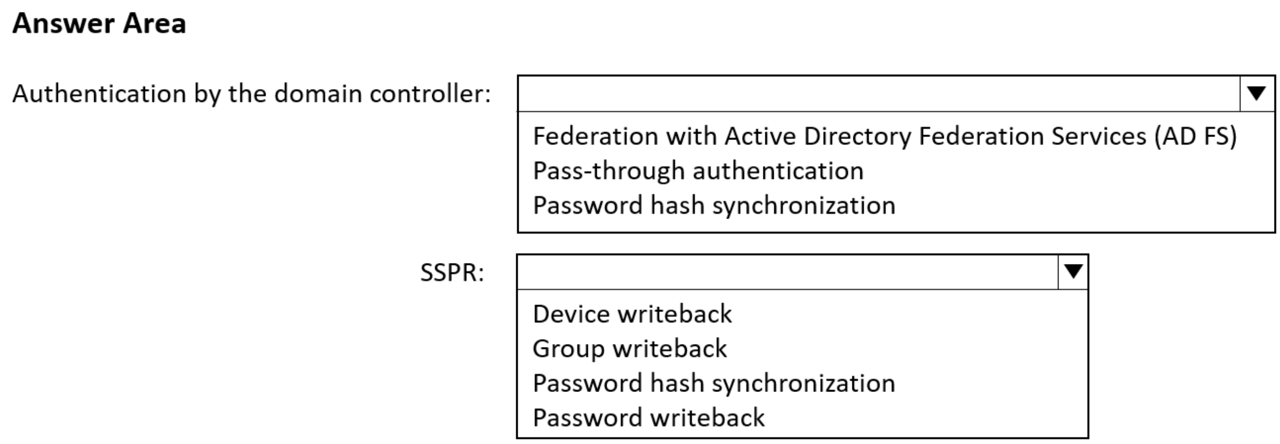
Your on-premises network contains an Active Directory domain that uses Azure AD Connect to sync with an Azure AD tenant.

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.

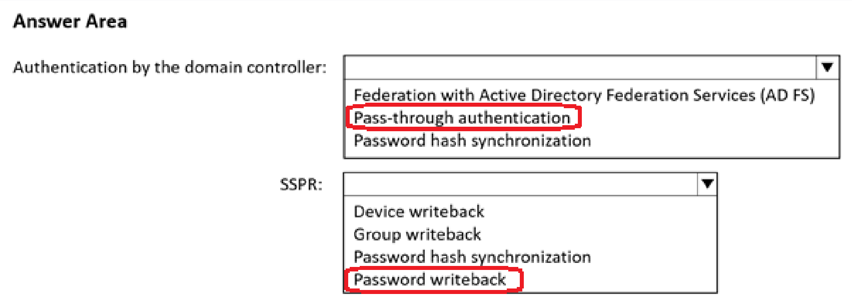


Answer Area

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

Suggested Answer:



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]

jojoseph Highly Voted 11 months, 2 weeks ago

pass- through auth

password write back

upvoted 21 times

naveenbio Most Recent 3 weeks, 6 days ago

1. Authentication by the domain controller:

· Pass-through authentication: This method ensures that user sign-ins to Azure AD are authenticated by an on-premises Active Directory domain controller.

2. SSPR (Self-Service Password Reset):

· Password writeback: This feature allows users to reset their passwords in Azure AD and have those changes written back to the on-premises Active Directory.

upvoted 1 times

EmnCours 4 months, 3 weeks ago

pass- through auth

password write back

upvoted 4 times

⊟ **AMZ** 6 months, 1 week ago

Question valid - 06/23

upvoted 4 times

⊟ **mali1969** 6 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** 4 months, 2 weeks ago

For 2nd requirement, it should be password write back. PHS doesn't help with SSPR

upvoted 2 times

⊟ **dule27** 6 months, 4 weeks ago

1. Pass- through authentication

2. Password writeback

upvoted 2 times

⊟ **DoMing** 9 months ago

PTA and Password hash synchronization

upvoted 1 times

⊟ **kmk_01** 8 months, 3 weeks ago

How does PHS help with SSPR for On-premises AD accounts?

It's password write back for the second question.

upvoted 5 times

⊟ **Aquintero** 11 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** 11 months, 3 weeks ago

The Answer is Correct

upvoted 4 times

Question #43 *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 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

Suggested Answer: *D*

Community vote distribution

D (100%)

Martyss Highly Voted 👍 1 year, 6 months ago

At least they got it right on the 4th try lol

upvoted 29 times

babadook13 12 months ago

:) good one

upvoted 1 times

Labelfree 1 month, 3 weeks ago

lol, pretty bad if we get this one wrong on the exam after going through it 4x, but then again... they've changed it recently too with Microsoft Graph

upvoted 1 times

haskelatchi Highly Voted 👍 1 year, 7 months 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 12 times

krisbla Most Recent 🕒 1 month, 3 weeks ago

If only this question could be asked 50 times during the real Exam.. I'd probably still get 700/1000 □

upvoted 1 times

Labelfree 1 month, 3 weeks ago

lol, how many times is this question going to be asked?

upvoted 3 times

sojorow324 4 months ago

my guess is the answers in the other questions are correct but the question itself is wrong. It is rare to see the same question 4 times.

upvoted 1 times

mohamedbenamor 5 months, 1 week ago

lol , how many times we have to answer it

upvoted 2 times

rajatn 6 months, 3 weeks ago

Same question is having different answer which is correct

upvoted 1 times

jtlucas99 8 months, 2 weeks ago

Set-MgGroupLicense cmdlet

upvoted 1 times

⊟ **shuhaidawahab** 1 year, 2 months ago

same as question before

upvoted 1 times

⊟ **Firefarter** 1 year, 5 months ago

Set-MsolUserLicense would be correct but it is deprecated

upvoted 1 times

⊟ **dule27** 1 year, 6 months ago

Selected Answer: D

D. the Set-MsolUserLicense cmdlet

upvoted 1 times

⊟ **ShoaibPKDXB** 1 year, 7 months ago

Selected Answer: D

D is correct

upvoted 1 times

Question #44 *Topic 1*

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

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

You have 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

Suggested Answer: *B*

Community vote distribution

B (100%)

shuhaidawahab 2 months, 3 weeks ago

same as question before

upvoted 1 times

EmnCours 4 months, 3 weeks ago

Selected Answer: B

B. No is correct answer

upvoted 1 times

mali1969 6 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, 4 weeks ago

Selected Answer: B

B. No is correct answer

upvoted 1 times

haskelatchi 7 months, 3 weeks ago

Another repeat question. The answer is obviously C

upvoted 1 times

kanew 8 months ago

B) https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/users-revoke-access

upvoted 3 times

Question #45 *Topic 1*

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

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

You have a Microsoft 365 E5 subscription.

You create 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

Suggested Answer: *A*

Community vote distribution

A (86%) 14%

AMZ Highly Voted 9 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 17 times

kmk_01 8 months, 3 weeks ago

Thanks for the link.

upvoted 2 times

mali1969 Highly Voted 6 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 5 times

Frank9020 Most Recent 2 weeks, 3 days ago

Selected Answer: B

The two roles that allow you to make changes and directly interact with Identity Secure Score are:

Global Administrator

Security Administrator

upvoted 1 times

RoelvD 1 month, 2 weeks 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 4 times

⊟ **shuhaidawahab** 2 months, 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 3 times

⊟ **EmnCours** 5 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 2 times

⊟ **mali1969** 6 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 3 times

⊟ **Rynol** 6 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, 4 weeks ago

Selected Answer: A

A. Yes is the correct answer

upvoted 1 times

⊟ **ShoaibPKDXB** 7 months, 4 weeks ago

Selected Answer: A

correct

upvoted 1 times

⊟ **ShoaibPKDXB** 7 months, 4 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

⊟ **LeonLau** 7 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

Question #46 *Topic 1*

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

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

You have a Microsoft 365 E5 subscription.

You create 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

Suggested Answer: *B*

Community vote distribution

B (100%)

Labelfree 4 weeks, 1 day ago

Selected Answer: B

Seems counterintuitive that Exchange Admin is included, and User Admin is not, but False is correct here.

upvoted 1 times

AlexBrazil 2 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-identity-secure-score#read-and-write-roles

With read and write access, you can make changes and directly interact with identity secure score:

- Security Administrator
- Exchange Administrator
- SharePoint Administrator

upvoted 1 times

a6792d4 7 months, 2 weeks ago

Read and write roles

With read and write access, you can make changes and directly interact with identity secure score.

Security Administrator

Exchange Administrator

SharePoint Administrator

upvoted 4 times

EmnCours 1 year, 5 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#read-and-write-roles

upvoted 2 times

dule27 1 year, 6 months ago

Selected Answer: B

B. NO is the correct answer

upvoted 1 times

⊟ **m4rv1n** 1 year, 7 months 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 3 times

⊟ **ShoaibPKDXB** 1 year, 7 months ago

Selected Answer: B

Correct B

upvoted 1 times

⊟ **boapaulo** 1 year, 9 months ago

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#read-and-write-roles

upvoted 1 times

Question #47 *Topic 1*

HOTSPOT

-

Case Study

-

Overview

-

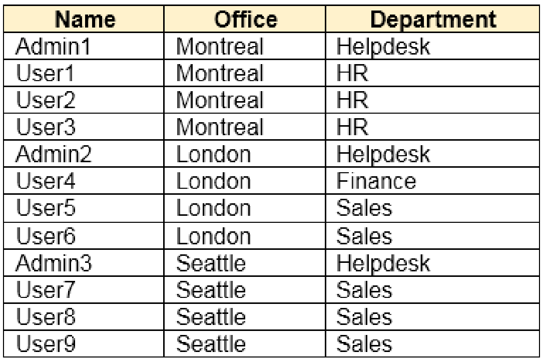
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.

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

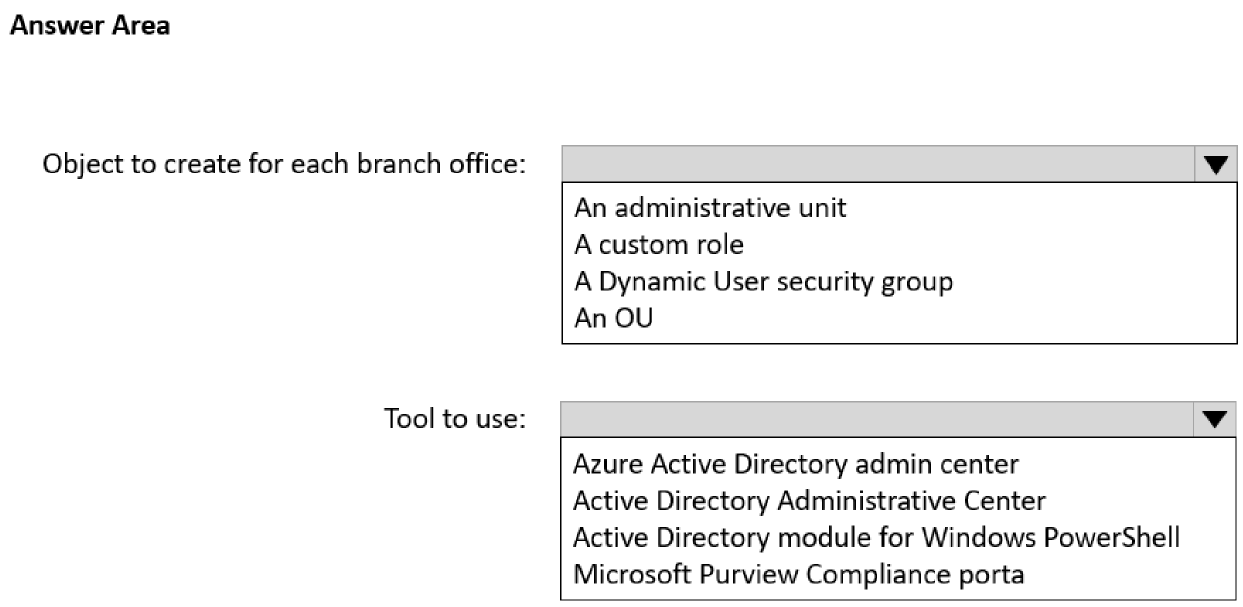
Contoso identifies the following technical requirements:

• 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

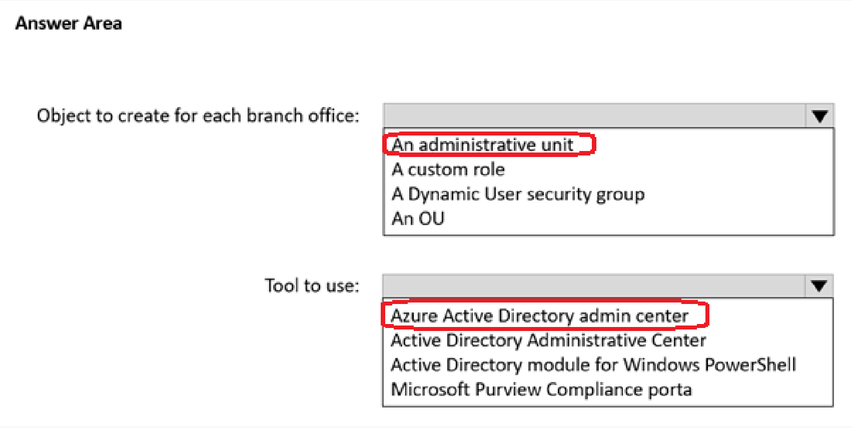
Object to create for each branch office: ▼

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 porta

Suggested Answer:



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 porta

⊟ **kijken** Highly Voted 1 year, 1 month 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 14 times

⊟ **mikekrt** Highly Voted 1 year, 3 months ago

correct

upvoted 9 times

⊟ **dann_S** Most Recent 3 months ago

Are we all sure about this one? I was going based off of "All users must be synced from AD DS to the contoso.com Azure AD tenant."

This would indicate that user passwords need to be reset from the Server AD infrastructure which then flow to Entra ID (Azure) via Azure AD Connect. This would mean they would need an OU (for their respective site), and then password reset via use of the Server AD Admin Center via delegation (old school yes, but that's what I see if going based-upon the presen ted use case). Otherwise I would have definitely agreed with an AU and Entra (Azure) admin center.

Box 4 = an OU
Box 2 = Active Driectory Administrative Center

upvoted 3 times

⊟ **Sunth65** 6 days, 22 hours ago

Correct answer

upvoted 1 times

jsca 8 months ago

answer is correct

upvoted 2 times

haazybanj 1 year, 2 months ago

box1= Dynamic group

box = Azure admin center

upvoted 2 times

> **kijken** 1 year, 1 month ago
>
> first is administrative unit, please read what that is
>
> upvoted 3 times
>
> > **haazybanj** 1 year, 1 month ago
> >
> > You're right
> >
> > upvoted 3 times
>
> **haazybanj** 1 year, 1 month ago
>
> Box1= Administrative unit
>
> upvoted 1 times

hw121693 1 year, 5 months 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** 1 year, 5 months 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** 1 year, 5 months ago
> >
> > you cannot apply a role to a dynamic security group - tested
> >
> > upvoted 4 times

Question #48 Topic 1

Case Study -

Overview -

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

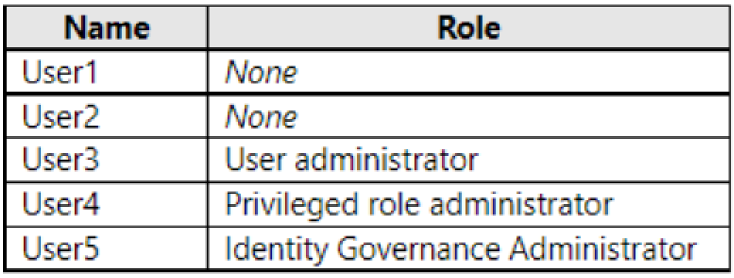
Existing Environment. ADatum Environment

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.

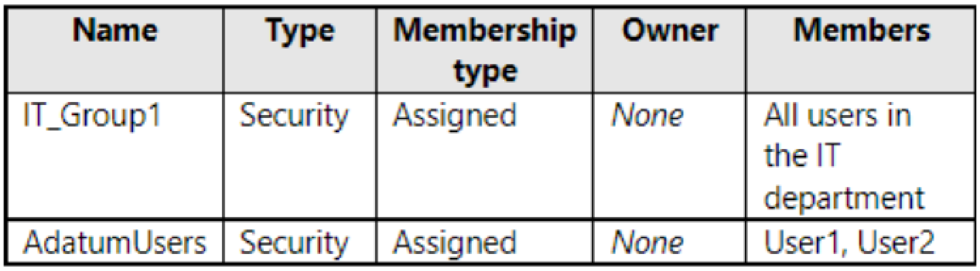
ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

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 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

Suggested Answer: *A*

Community vote distribution

A (100%)

penatuna Highly Voted 4 months, 1 week ago

Selected Answer: A

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."

Requirements. Planned Changes:
Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

Within Device settings, you can increase maximum number of devices a user can join/register to Azure AD.

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 6 times

penatuna 4 months, 1 week ago

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.

Note!
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-us/azure/active-directory/devices/manage-device-identities#configure-device-settings

upvoted 3 times

ELQUMS Most Recent 4 months, 1 week ago

Selected Answer: A

Answer A

upvoted 2 times

Siraf 6 months, 2 weeks ago

Answer is A
From Azure portal > Microsoft Entra ID > Devices > Device Settings > Maximum number of devices per user

upvoted 3 times

marsot 11 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 11 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

Question #49 *Topic 1*

Case Study -

Overview -

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

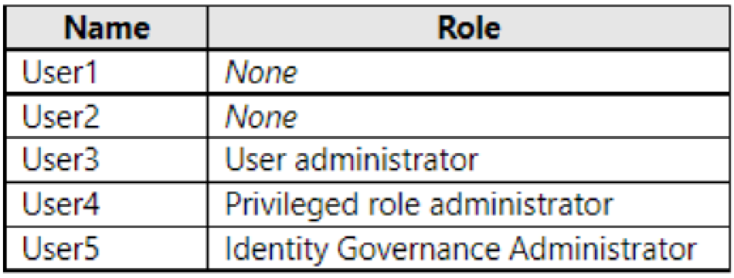
Existing Environment. ADatum Environment

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.

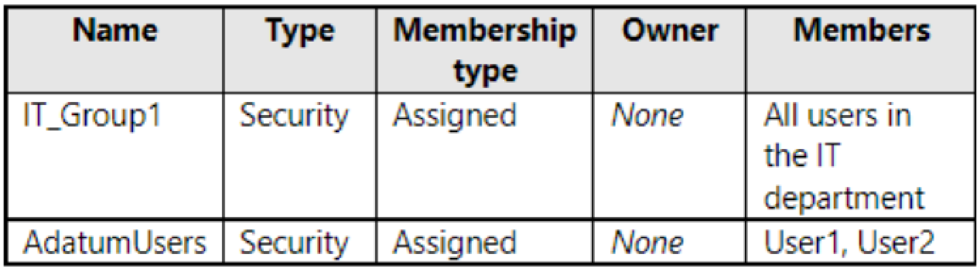
ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

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.

Suggested Answer: *B*

Community vote distribution

B (100%)

razmus Highly Voted 1 year, 5 months ago

And when recreating, set isAssignableToRole. https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept

upvoted 15 times

AlexBrazil Most Recent 2 months ago

Selected Answer: B

Only groups that have the isAssignableToRole property set to true at creation time can be assigned a role. This property is immutable. Once a group is created with this property set, it can't be changed.

You can't set the property on an existing group.

So, you have to recreate it.

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept#how-are-role-assignable-groups-protected

upvoted 4 times

⊟ **Studytime2023** 1 year, 1 month 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 4 times

⊟ **Studytime2023** 1 year, 1 month 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 3 times

⊟ **Nyamnyam** 1 year, 1 month 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** 1 year, 4 months ago

Selected Answer: B

recreate group, set isAssignableToRole

upvoted 3 times

⊟ **mali1969** 1 year, 4 months ago

Correct answer is "Add an owner to IT_Group1"

upvoted 1 times

⊟ **mali1969** 1 year, 4 months ago

and also answer A is corrected

A. Change Membership type of IT_Group1 to Dynamic User

upvoted 1 times

Question #50 *Topic 1*

Case Study -

Overview -

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

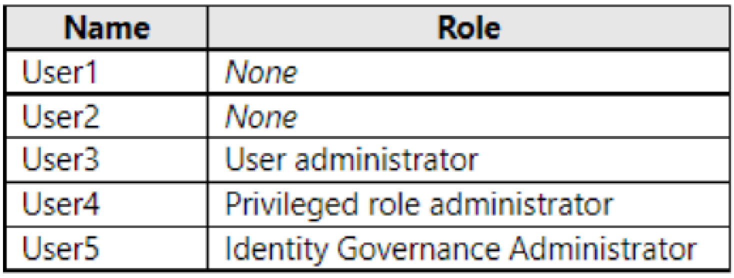
Existing Environment. ADatum Environment

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.

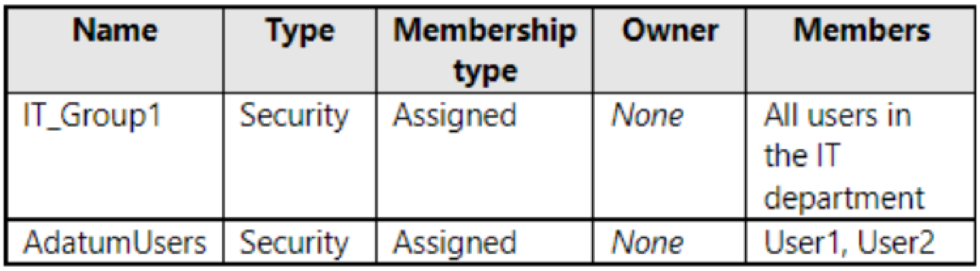
ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

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 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

Suggested Answer: *B*

Community vote distribution

A (100%)

penatuna Highly Voted 1 year, 3 months 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 14 times

Alcpt 7 months, 2 weeks ago

i had to do some research but its definitely A as per MS video at 1:45.
https://youtu.be/9T6lKEloq0Q

upvoted 2 times

0byte **Highly Voted** 1 year, 3 months 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/hybrid/cloud-sync/plan-cloud-sync-topologies#multi-forest-single-microsoft-entra-tenant

upvoted 8 times

AlexBrazil **Most Recent** 2 months ago

Selected Answer: A

"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."

https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/what-is-cloud-sync

upvoted 1 times

baz 11 months, 2 weeks ago

Answer = B. Some of the excluded options in cloud sync prevent the solution – pass thru auth required for SSPR
https://practical365.com/how-to-decide-between-azure-ad-connect-and-azure-ad-connect-cloud-sync/

upvoted 5 times

Waiuku2123 1 year ago

Both AADC and Cloud Sync would work, however there is no detail that there is comms links between the two AD forests therefore Cloud Connect is the better option. AADC does not require an AD Trust unless Pass-thru-auth is to be deployed. PTA is not a requirement

upvoted 4 times

Kipper_2022 1 year, 3 months ago

Selected Answer: A

No trust = Cloud sync

upvoted 5 times

ServerBrain 1 year, 4 months ago

Selected Answer: A

"Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains."

upvoted 3 times

KrissB 1 year, 4 months 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 1 year, 5 months 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 5 times

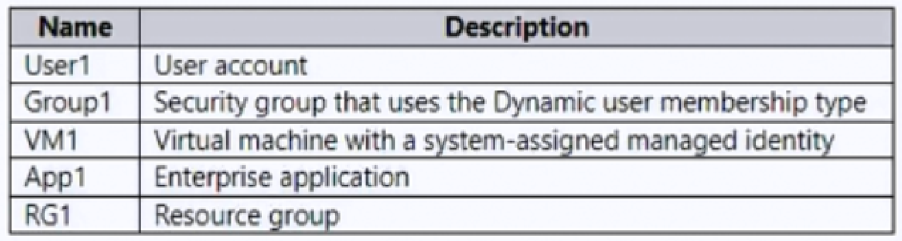
katvik001 1 year, 5 months ago

B is correct, litware.com should be included in AADC.

upvoted 4 times

Question #51 Topic 1

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

Suggested Answer: *E*

Community vote distribution

E (60%) D (29%) 11%

pokrz26 Highly Voted 1 year ago

Selected Answer: D

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept#how-are-role-assignable-groups-protected

The membership type for role-assignable groups must be Assigned and can't be a Microsoft Entra dynamic group. Automated population of dynamic groups could lead to an unwanted account being added to the group and thus assigned to the role.

Group1 is dynamic an to those groups you can't assign role. So answer is:

User1, VM1, App1

upvoted 14 times

sabas4 11 months, 3 weeks ago

You can't assign an MS Entra Role (to prevent an administrator elevating their privileges), but you can assign an Azure role. E is correct.

upvoted 8 times

j11v0sud Highly Voted 1 year, 3 months ago

Selected Answer: E

Tested in-lab, fyi user-assigned managed identity works also

upvoted 6 times

ATimTimm Most Recent 3 weeks, 1 day ago

Selected Answer: D

You can't assign role to dynamic group. That's what I studied.

upvoted 1 times

Marius12345 1 month, 2 weeks ago

Selected Answer: D

Answer: D. User1, VM1, and App1 only

Explanation:

In Azure, the Contributor role for a resource group like RG1 can be assigned to the following types of identities:

User accounts (such as User1).
System-assigned managed identities for Azure resources (such as VM1).
Service principals associated with enterprise applications (such as App1).
Here's why each option qualifies or does not qualify:

User1: A user account can be assigned the Contributor role, so User1 is eligible.
VM1: Since VM1 has a system-assigned managed identity, it can be assigned roles like Contributor for RG1.
App1: As an enterprise application (service principal), App1 can also be assigned the Contributor role.
However:

Group1 cannot be assigned the Contributor role because dynamic groups (such as those with the Dynamic user membership type) are not supported for Azure role-based access control (RBAC) assignments. Only static groups or individual users, service principals, and managed identities can be assigned roles.

upvoted 1 times

AlexBrazil 2 months ago

Selected Answer: D

A security principal is an object that represents a user, group, service principal, or managed identity that is requesting access to Azure resources. You can assign a role to any of these security principals.
So, you can assign a role to
- User
- Group (Assigned)
- Service Principal
- Managed Identity
https://learn.microsoft.com/en-us/azure/role-based-access-control/overview

However, it says in another doc:
The membership type for role-assignable groups must be Assigned and CAN'T be a Microsoft Entra dynamic group.
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept#how-are-role-assignable-groups-protected

upvoted 1 times

mohamedbenamor 5 months, 1 week ago

User, group and appllication (Service principal) with no doubt : https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps#step-1-determine-who-needs-access

VM (system assigned) : https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/tutorial-windows-vm-access?pivots=windows-vm-access-wvm

so E is correct

upvoted 2 times

jtlucas99 7 months, 2 weeks ago

Copilot
In Azure, you can assign the Contributor role for a resource group (RG1 in this case) to the following identities:

User Accounts: You can assign the role to individual user accounts, such as user1 in your table.
Security Groups: You can also assign the role to security groups, such as group1. All members of the group, including those dynamically added due to the group's dynamic membership rules, will inherit the role.
Managed Identities: Managed identities for Azure resources, such as the system-assigned managed identity for VM1, can also be assigned the role. This allows the VM to manage resources in the resource group.
Enterprise Applications: Enterprise applications, such as app1, can be assigned the role if they have an associated service principal. This allows the application to manage resources in the resource group.
Remember, the Contributor role allows the assigned identity to create and manage all types of Azure resources, but it does not allow them to grant access to other users. For that, you would need the Owner role or User Access Administrator role.

upvoted 2 times

JuanZ 8 months, 1 week ago

Selected Answer: D

The membership type for role-assignable groups must be Assigned and can't be a Microsoft Entra dynamic group. Automated population of dynamic groups could lead to an unwanted account being added to the group and thus assigned to the role.

upvoted 1 times

RoelvD 1 year, 1 month 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 4 times

Nyamnyam 1 year, 1 month 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 4 times

ACSC 1 year, 3 months ago

Selected Answer: E

You can assign RBAC roles to any of the options, user, group, MI and apps.

upvoted 5 times

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

E looks correct. https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps

upvoted 2 times

Kyumogi 1 year, 4 months 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** 1 year, 4 months 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 5 times

⊟ **einkaufacs** 1 year, 3 months 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 2 times

Question #52 *Topic 1*

HOTSPOT

-

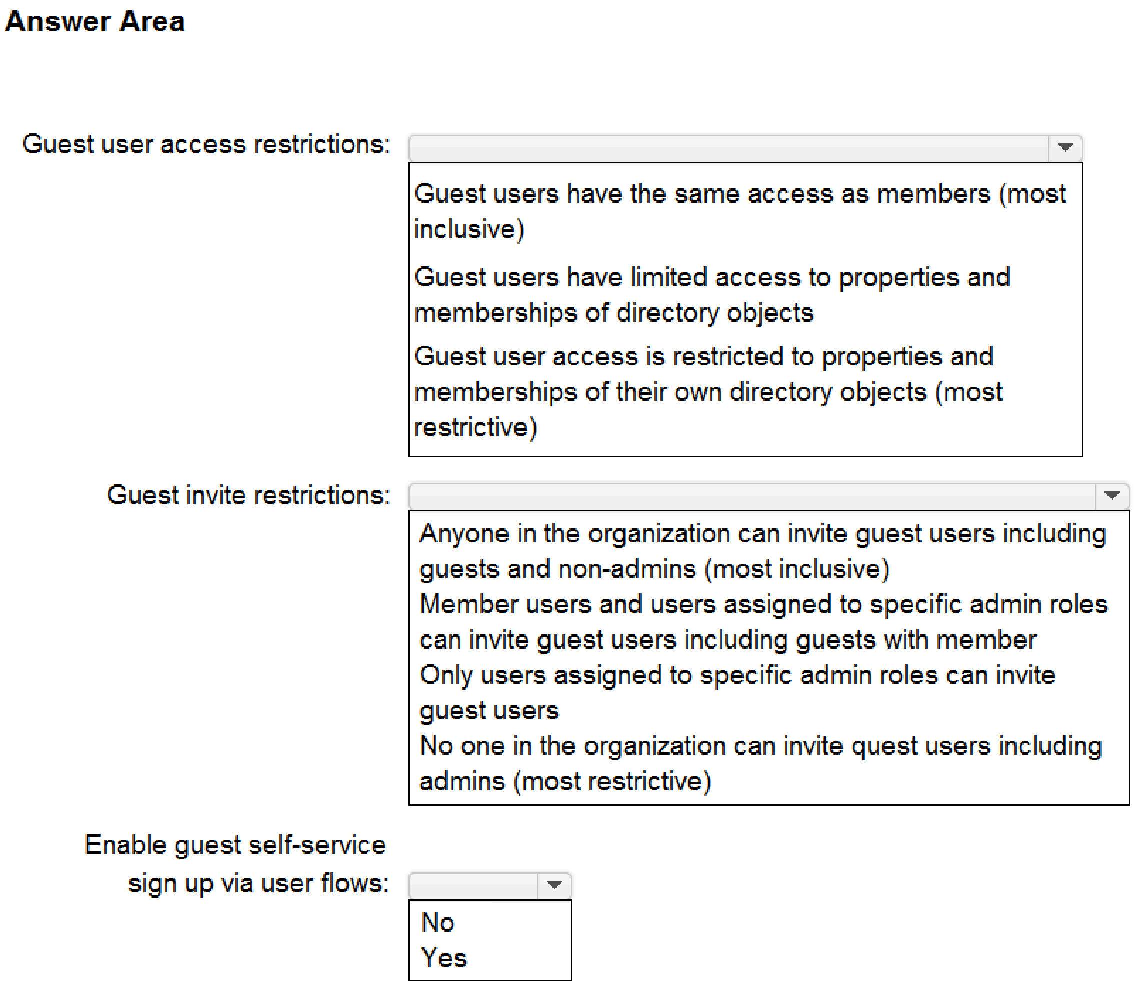
You have an Azure AD tenant that contains a user named User1. User1 is assigned the User Administrator role.

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)

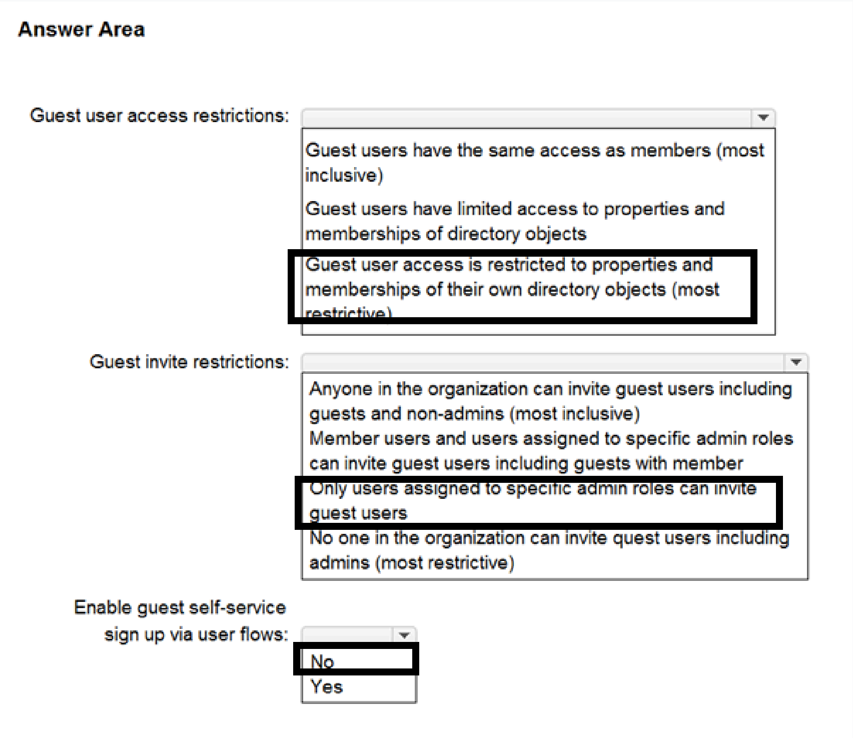
Guest invite restrictions:

- 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 quest users including admins (most restrictive)

Enable guest self-service sign up via user flows:

- No
- Yes

Suggested Answer:



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

RoelvD 1 month, 2 weeks 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 3 times

Nyamnyam 1 month, 3 weeks ago

Correct

upvoted 3 times

sehlohomoletsane 3 months, 3 weeks ago

tested in lab

the answer is correct

upvoted 4 times

ServerBrain 4 months, 1 week ago

100% correct

upvoted 3 times

EmnCours 4 months, 3 weeks ago

Correct

upvoted 2 times

Question #53 *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 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

Suggested Answer: *D*

Community vote distribution

D (60%) B (40%)

ServerBrain Highly Voted 1 year, 4 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 5 times

throwaway10188 11 months, 4 weeks ago

https://learn.microsoft.com/en-us/powershell/module/azuread/set-azureaduserlicense?view=azureadps-2.0

The Set-AzureADUserLicense 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

josemariamr Most Recent 4 weeks, 1 day ago

Selected Answer: D

No, you cannot delete user licenses with the Set-AzureAdUser cmdlet. To manage licenses, you must use the Set-AzureADUserLicense or Set-MgUserLicens cmdlet.

upvoted 1 times

Davito 2 months ago

As of 2024/11/03 the Licenses blade in Entra explicitly states with a banner:

"Adding, removing, and reprocessing licensing assignments is only available within the M365 Admin Center."

D should not be correct, it might be correct in the future, but seeing as there is like 7 variations of this question with different answers, the intended answer is likely the PowerShell script of Set-MsolUserLicense

upvoted 1 times

mohamedbenamor 5 months, 1 week ago

B is not correct here

https://learn.microsoft.com/nl-nl/powershell/module/azuread/set-azureaduserlicense?view=azureadps-2.0

upvoted 1 times

jtlucas99 7 months, 2 weeks ago

1. Sign in to the Microsoft Entra admin center as at least a License Administrator.

2. Browse to Identity > Billing > Licenses.

upvoted 1 times

KRISTINMERIEANN 8 months, 4 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-us/microsoft-365/enterprise/remove-licenses-from-user-accounts-with-microsoft-365-powershell?view=o365-worldwide

upvoted 2 times

⊟ **Siraf** 1 year ago

With my free P2 license, I can remove license from Group blade or from License blade in Microsoft Entra ID. I don't have Microsoft 365 Enterprise license.

upvoted 1 times

⊟ **mtberdaan** 1 year, 4 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** 1 year, 4 months ago

Agree. it should be powershell script

upvoted 1 times

⊟ **stai** 1 year, 4 months 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 2 times

⊟ **mohamedbenamor** 5 months, 1 week ago

But your docs refers to Microsoft Graph ?

upvoted 1 times

Question #54 *Topic 1*

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

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

You have a Microsoft 365 E5 subscription.

You create 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

Suggested Answer: *B*

Community vote distribution

B (100%)

nils241 Highly Voted 5 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 13 times

sehlohomoletsane Most Recent 3 months, 3 weeks ago

Selected Answer: B

The answer is no
upvoted 1 times

Question #55 Topic 1

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

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

You have a Microsoft 365 E5 subscription.

You create 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

Suggested Answer: *A*

Community vote distribution

A (100%)

⊟ **nils241** Highly Voted 1 year, 5 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 6 times

⊟ **SynnerG** Most Recent 3 months, 2 weeks ago

Selected Answer: B

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
upvoted 1 times

⊟ **EmnCours** 1 year, 4 months ago

Selected Answer: A

A. Yes
upvoted 1 times

⊟ **1c67a2c** 1 year, 5 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 2 times

Question #56 *Topic 1*

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.

Suggested Answer: *D*

Community vote distribution

D (66%) C (33%)

⊟ **hellawaits111** Highly Voted 1 year, 5 months ago

Selected Answer: C

Role explained here:
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#helpdesk-administrator

upvoted 13 times

⊟ **Alcpt** 7 months, 2 weeks ago

nope
The answer is D.
Users with Helpdesk Administrator role can:
change passwords,
Invalidate refresh tokens,
Create and manage support requests with Microsoft for Azure and Microsoft 365 services,
and MONITOR service health.

To CREATE a support request:
You must have the Owner, Contributor, or Support Request Contributor role, or a CUSTOM role with Microsoft.Support/*, at the subscription level.
A Helpdesk Admin CANNOT CREATE and MANAGE support tickets.
You are forced to create a custom role to 1. satisfy all your needs , 2. least admin has no choice here.

upvoted 10 times

⊟ **photon99** 2 weeks, 5 days ago

You are wrong. Helpdesk Admin CAN create Support Tickets:
microsoft.azure.supportTickets/allEntities/allTasks : Create and manage Azure support tickets : https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#helpdesk-administrator

upvoted 1 times

⊟ **Logitech** 1 year, 3 months ago

You need to ensure that Admin1 can perform only the following tasks... Sounds pretty clear that the user should not be able to to more than this 3 things.
With Helpdesk Admin you can do more. Really supid MS Question again....
D should be the answer.

upvoted 8 times

Nyamnyam Highly Voted 👍 1 year, 1 month 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 12 times

Cybersecgirl Most Recent 🕒 2 months, 2 weeks ago

Chatgpt says
You should assign Admin1 the Helpdesk Administrator role.

The Helpdesk Administrator role in Microsoft 365 and Azure allows a user to:

Create and manage service requests (support tickets).
Read and configure service health.
This role meets all the requirements without the need to create and manage a custom role, which minimizes administrative effort. Creating a custom role would add complexity and is unnecessary in this case, as the Helpdesk Administrator role provides the exact permissions needed.

upvoted 1 times

> **Cybersecgirl** 2 months, 2 weeks ago
>
> No, the Helpdesk Administrator role does not grant the ability to create and manage support tickets in the Azure portal. The Helpdesk Administrator role is primarily focused on Microsoft 365 tasks such as:
>
> Creating and managing service requests in the Microsoft 365 admin center.
> Viewing and configuring service health in the Microsoft 365 admin center.
> To allow Admin1 to create and manage support tickets in the Azure portal, you would need to assign the Support Request Contributor role in Azure. This role specifically allows a user to create and manage support tickets in the Azure portal.
>
> upvoted 1 times

penatuna 3 months ago

D. I would say that least privileged is always more important than minimizing administrative effort.

upvoted 1 times

omnomsnom 6 months, 1 week ago

In the real world, the Service Support Administrator role exists for this use case.

upvoted 1 times

bpaccount 8 months, 1 week ago

Selected Answer: C

It's C, a custom role isnt the least administrative effort.

upvoted 1 times

Justin0020 8 months, 3 weeks ago

Selected Answer: C

The best solution is D, de one with the least administrative effort is C so i say C.

upvoted 2 times

emartiy 9 months, 1 week ago

Selected Answer: D

need to ensure that Admin1 can perform only the following tasks means that create a custom role an assign what you want a user can perform as admin :)
D - D - D - D - ::)))

upvoted 3 times

Er_01 11 months ago

Selected Answer: C

Help desk admin - description - role permissions. Here, the 3 items in the question are listed under lines 5,6,8 verbatim.

upvoted 1 times

Er_01 1 year ago

Selected Answer: D

It is for ONLY these items and HD Admin does alot more so a custom role for it fits the bill.

upvoted 4 times

marco_aimi 1 year ago

"minimize administrative effort" using custom role? hum..

upvoted 5 times

RoelvD 1 year ago

Selected Answer: D

"can perform only".. Helpdesk admin can do more then that. So D.

upvoted 4 times

onelove01 1 year ago

Selected Answer: D

Key word here is "ONLY", implying they can't perform any task outside of the three listed. D is the correct answer

upvoted 7 times

Alscoran 1 year, 1 month ago

Selected Answer: D

It doesn't ask for password resets so why would you give such privileges. Has to be D.

upvoted 6 times

kijken 1 year, 1 month ago

Selected Answer: D

Least privileged option is D. C can be, but has too much permissions

upvoted 5 times

MacDanorld 1 year, 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 5 times

Nivos23 1 year, 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 5 times

Question #57 Topic 1

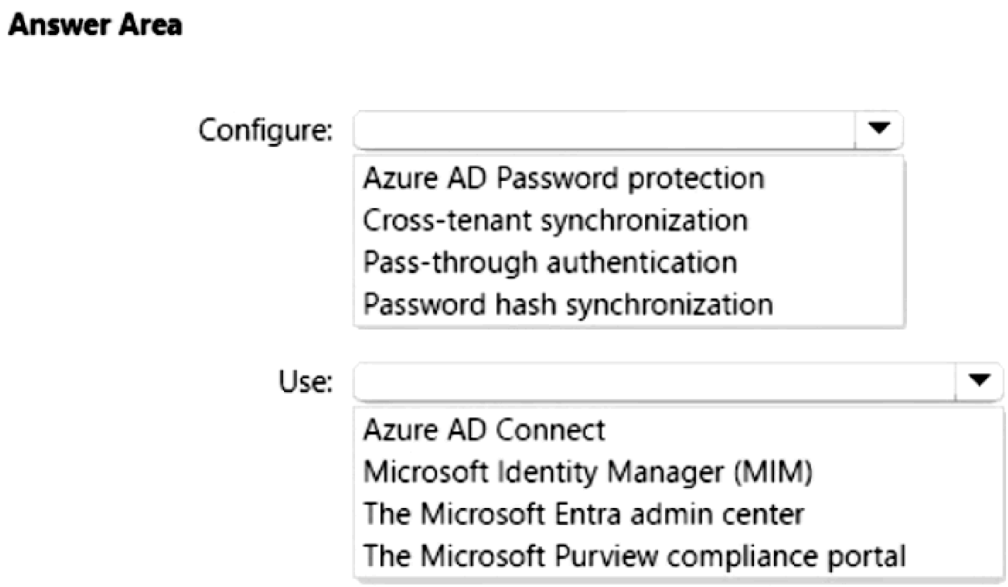
HOTSPOT
-

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.

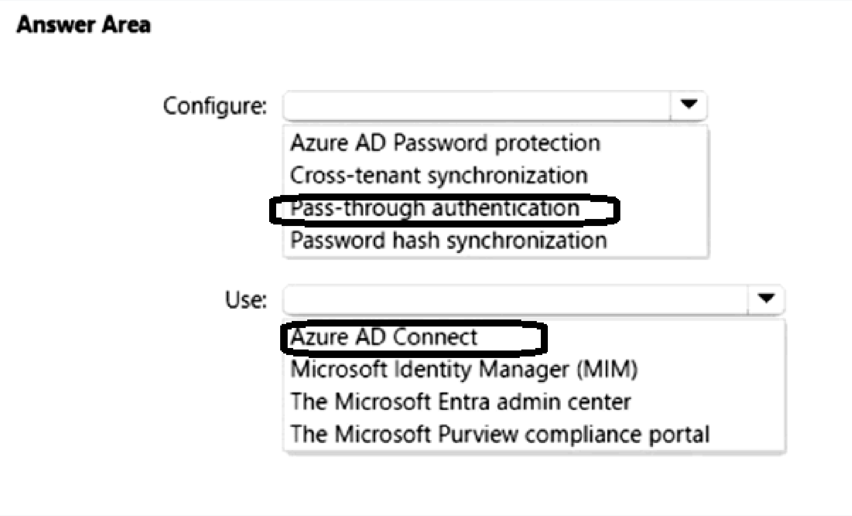


Answer Area

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

Suggested Answer:



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

ServerBrain Highly Voted 10 months, 1 week ago

Correct. PTA using AD Connect

upvoted 9 times

penatuna Most Recent 9 months, 3 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 4 times

Wicke 9 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 2 times

> **Futfuyfyjfj** 2 months, 1 week ago
>
> Wrong answer, wrong link:
>
> https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-password-hash-synchronization?toc=%2Fentra%2Fidentity%2Fdomain-services%2Ftoc.json&bc=%2Fentra%2Fidentity%2Fdomain-services%2Fbreadcrumb%2Ftoc.json#detailed-description-of-how-password-hash-synchronization-works
>
> upvoted 2 times

CoSaWe 10 months, 1 week ago

password hash synchronization: https://learn.microsoft.com/en-us/azure/active-directory-domain-services/synchronization#password-hash-synchronization-and-security-considerations

upvoted 2 times

> **Futfuyfyjfj** 2 months, 1 week ago
>
> Wrong answer, wrong link:
>
> https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-password-hash-synchronization?toc=%2Fentra%2Fidentity%2Fdomain-services%2Ftoc.json&bc=%2Fentra%2Fidentity%2Fdomain-services%2Fbreadcrumb%2Ftoc.json#detailed-description-of-how-password-hash-synchronization-works
>
> upvoted 3 times

EmnCours 10 months, 3 weeks ago

Correct Answer

upvoted 2 times

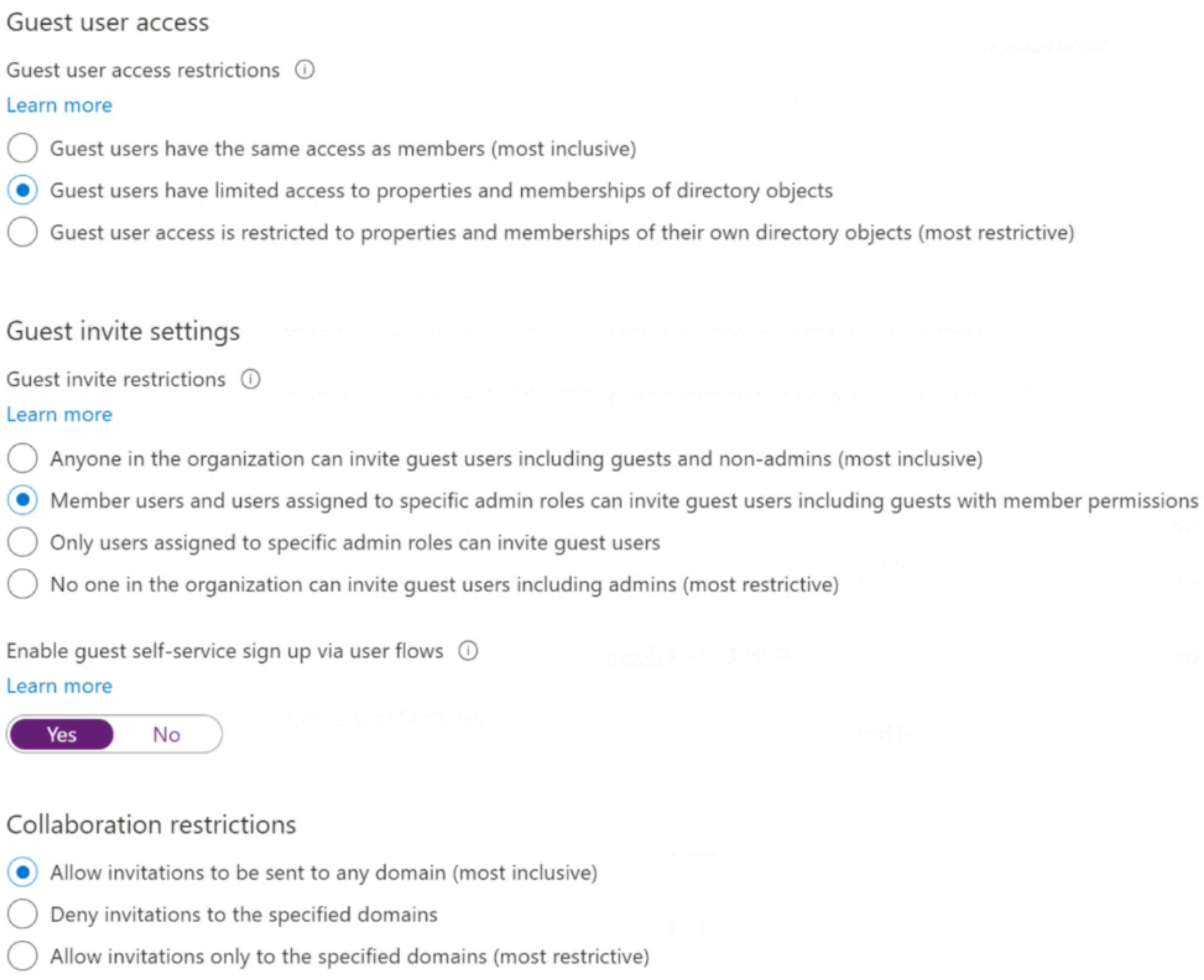
sehlohomoletsane 11 months ago

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises

upvoted 1 times

Question #58 Topic 1

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 ⓘ

Learn more

○ Guest users have the same access as members (most inclusive)

● Guest users have limited access to properties and memberships of directory objects

○ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

Learn more

○ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

● Member users and users assigned to specific admin roles can invite guest users including guests with member permissions

○ Only users assigned to specific admin roles can invite guest users

○ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

Learn more

[✓ Yes] No

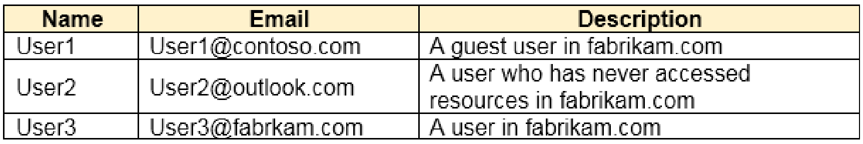
Collaboration restrictions

● 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@fabrkam.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

Suggested Answer: *A*

Community vote distribution

B (51%) A (49%)

Matajare Highly Voted 1 year, 1 month 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 22 times

⊟ **Max_He** Highly Voted 8 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 a Microsoft Entra 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.

Obviously, @outlook.com is a Microsoft account, won't receive a passcode.
upvoted 10 times

⊟ **krisbla** 1 month, 2 weeks ago
are emails using @outlook.com deemed automatically "Microsoft Accounts" ? .. Outlook.com is an online service, you can register a third-party email as a microsoft account but not sign-up for that service. This is how I'm reading it here: https://support.microsoft.com/en-us/office/connecting-a-microsoft-account-with-a-third-party-email-address-to-outlook-55cfbed6-4ce9-4d6f-a66b-8ace77fe9d5a
upvoted 1 times

⊟ **Nail** 2 months, 2 weeks ago
"Obviously, @outlook.com is a Microsoft account, won't receive a passcode." Is it obvious? Why wouldn't Microsoft accounts receive a passcode?
upvoted 1 times

⊟ **Nail** 2 months, 2 weeks ago
My bad, it's right there in your text and I found the documentation for it.
upvoted 1 times

⊟ **josemariamr** Most Recent 4 weeks, 1 day ago
Selected Answer: B
Outlook is Microsoft account and is autheticated by Microsoft itself whithout needing passcodes.
upvoted 2 times

⊟ **Davito** 2 months ago
This is currently in the test bank of questions and has a different option toggled for Guest Invite Settings. Based on the configuration in THIS photo the correct answer is None.

The ability to invite guests is locked to specific users and admin roles, bsmith does not have a specific role or permission in the example, therefore we should assume he cannot.

In the exam bank test questions the Guest Invite settings are set to the first radio option. The question is testing your knowledge of when one time pass codes are sent.
upvoted 3 times

⊟ **AlexBrazil** 2 months ago
Selected Answer: B

User1 authenticates with email one-time passcode
User2@outlook.com authenticates at Microsoft
User3@fabrikam.com authenticates at the own domain

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.
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.

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

diazed 2 months ago

Selected Answer: B

one-time passcode is used for guest that don't have a Microsoft account

upvoted 2 times

N0cturnal 2 months, 2 weeks ago

Just tested this in an environment with the exact same settings as shown in the exhibit and no users need to login with an OTP they all just get the mail of a shared file and then they can open it without reauthenticating. So NO ANSWER is correct

upvoted 2 times

dannyhcool 2 months, 3 weeks ago

Should be A.

upvoted 1 times

maomaopass 9 months ago

I think the answer is "B" because

(1) It doesn't mention one-time passcode is disabled and according to the following article, the one-time passcode is enabled by default.

https://learn.microsoft.com/en-us/entra/external-id/one-time-passcode#:~:text=one%2Dtime%20passcodes-,The%20email%20one%2Dtime%20passcode%20feature%20is%20now%20turned%20on%20by%20default%2
This%20feature%20provides

(2) Outlook.com is already a Microsoft account.

upvoted 1 times

Alcpt 8 months, 1 week ago

It's not B. He is already registered. Why would he get another invite when he already has an invite? Invites never expire.

upvoted 3 times

Jackboss47 11 months ago

Selected Answer: A

point 1: Guest users who redeemed an invitation before email one-time passcode was enabled will continue to use their same authentication method - where "User1" fits here.

Point 2: 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. If you want to update the user's authentication method, you can reset their redemption status. Since the User2 still didn't access the resource and while accessing its prompt for an Email one time passcode

upvoted 2 times

Jackboss47 11 months ago

Selected Answer: A

point 1: Guest users who redeemed an invitation before email one-time passcode was enabled will continue to use their same authentication method - where "User1" fits here.

Point 2: 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. If you want to update the user's authentication method, you can reset their redemption status. Since the User2 still access the environment and while accessing prompts for Email one time passcode

upvoted 1 times

⊟ **siffy** 11 months, 1 week ago

Selected Answer: B

B is correct

upvoted 2 times

⊟ **SFAY** 11 months, 2 weeks ago

Selected Answer: B

Tested using an outlook account and then a non MS account.

B is the correct answer.

upvoted 2 times

⊟ **onelove01** 1 year ago

Selected Answer: B

B is correct. There is no mention in the question that the setting was ever disabled

upvoted 2 times

⊟ **fatilaura** 1 year, 1 month 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

> ⊟ **onelove01** 1 year ago
>
> You are correct except that nothing in the question states that the setting was disabled before. In my opinion B is correct.
>
> upvoted 1 times

⊟ **kijken** 1 year, 1 month ago

B

A is wrong because is @ outlook.com and that is a microsoft account and authenticated by microsoft

upvoted 2 times

⊟ **Nivos23** 1 year, 2 months ago

Selected Answer: A

I think the answer is A. User2 only

upvoted 2 times

Question #59 *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 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

Suggested Answer: *A*

Community vote distribution

B (100%)

throwaway10188 5 months, 3 weeks ago

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 managements APIs from Microsoft Graph.

For the test before January 31st us mgsol command.

upvoted 1 times

BenLam 8 months, 1 week 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 2 times

JimboJones99 8 months, 1 week ago

Selected Answer: B

B as per the other questions

upvoted 3 times

MS_RF 8 months, 2 weeks ago

Selected Answer: B

B of course

upvoted 2 times

JCkD4Ni3L 8 months, 2 weeks ago

Selected Answer: B

B is the correct answer...

upvoted 1 times

shuhaidawahab 8 months, 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** 8 months, 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 2 times

⊟ **Anonymouse1312** 8 months, 4 weeks ago

Selected Answer: B

As with the previous 100 times this question has been asked it is

B. the Set-MsolUserLicense cmdlet

upvoted 3 times

⊟ **MicrosoftMaster2023** 8 months, 4 weeks ago

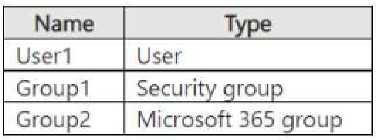
Selected Answer: B

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

Question #59 *Topic 1*

You have two Microsoft Entra tenants named contoso.com and fabrikam.com. Contoso.com contains the identities shown in the following table.



Name	Type
User1	User
Group1	Security group
Group2	Microsoft 365 group

You configure cross-tenant synchronization from contoso.com to fabrikam.com.

Which identities will sync with fabrikam.com?

A. User1 only

B. User1 and Group1 only

C. User1 and Group2 only

D. User1, Group1, and Group2

Suggested Answer: *A*

Community vote distribution

A (100%)

Sunth65 6 days, 15 hours ago

Selected Answer: A

Cross-tenant synchronization limitations and disadvantages

Only one-way sync is supported. ...

The target tenant isn't queried for changes in attributes. ...

No support for cross-cloud sync.

Only Entra ID users can be synchronized (groups, devices and contacts are not supported).

Cross-tenant sync starts every 40 minutes.

upvoted 1 times

mert123 1 week, 1 day ago

Selected Answer: A

correct chatgpt

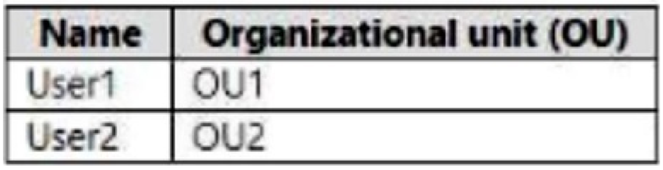
upvoted 1 times

Question #60 *Topic 1*

HOTSPOT

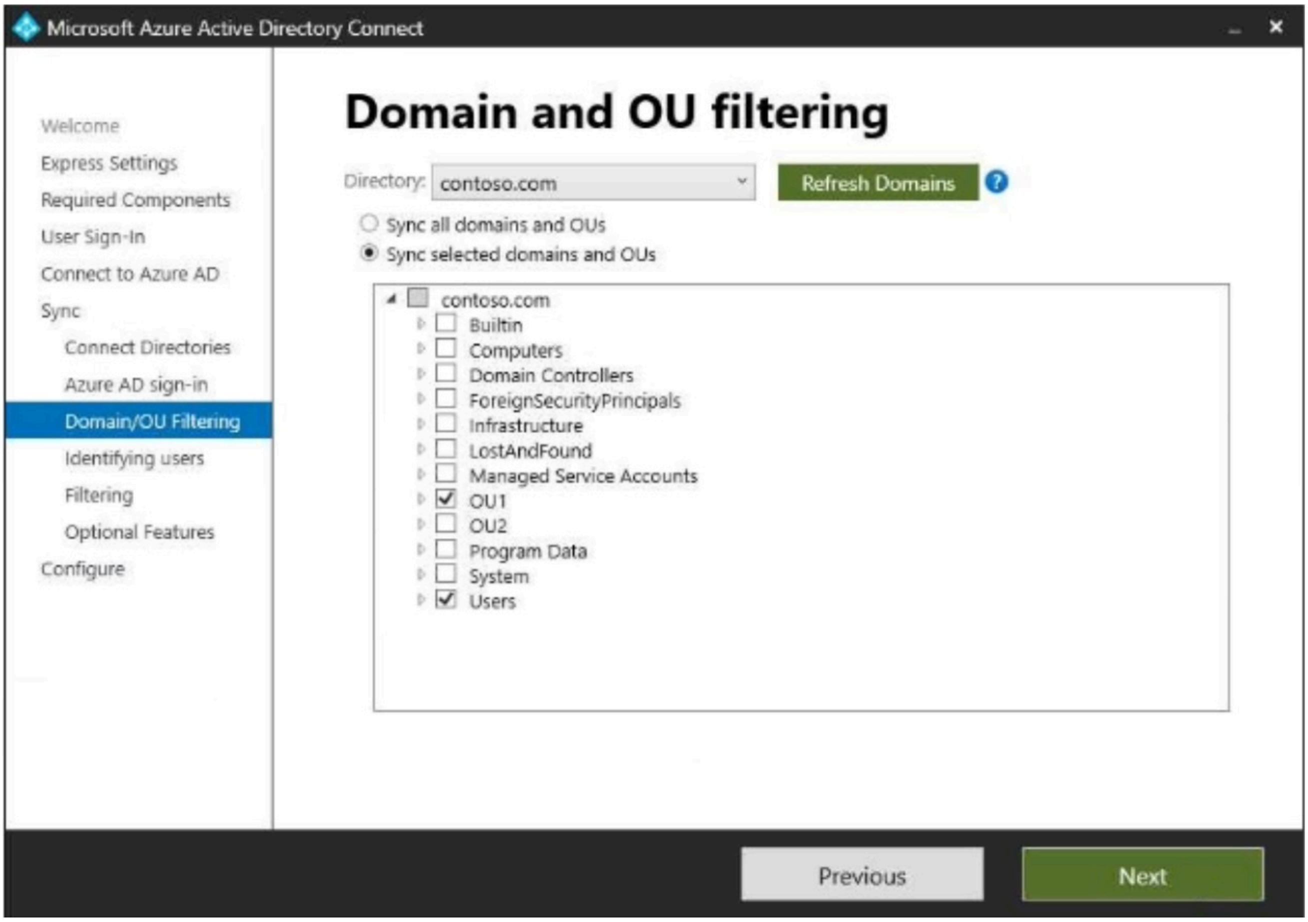
-

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.



Microsoft Azure Active Directory Connect

Domain and OU filtering

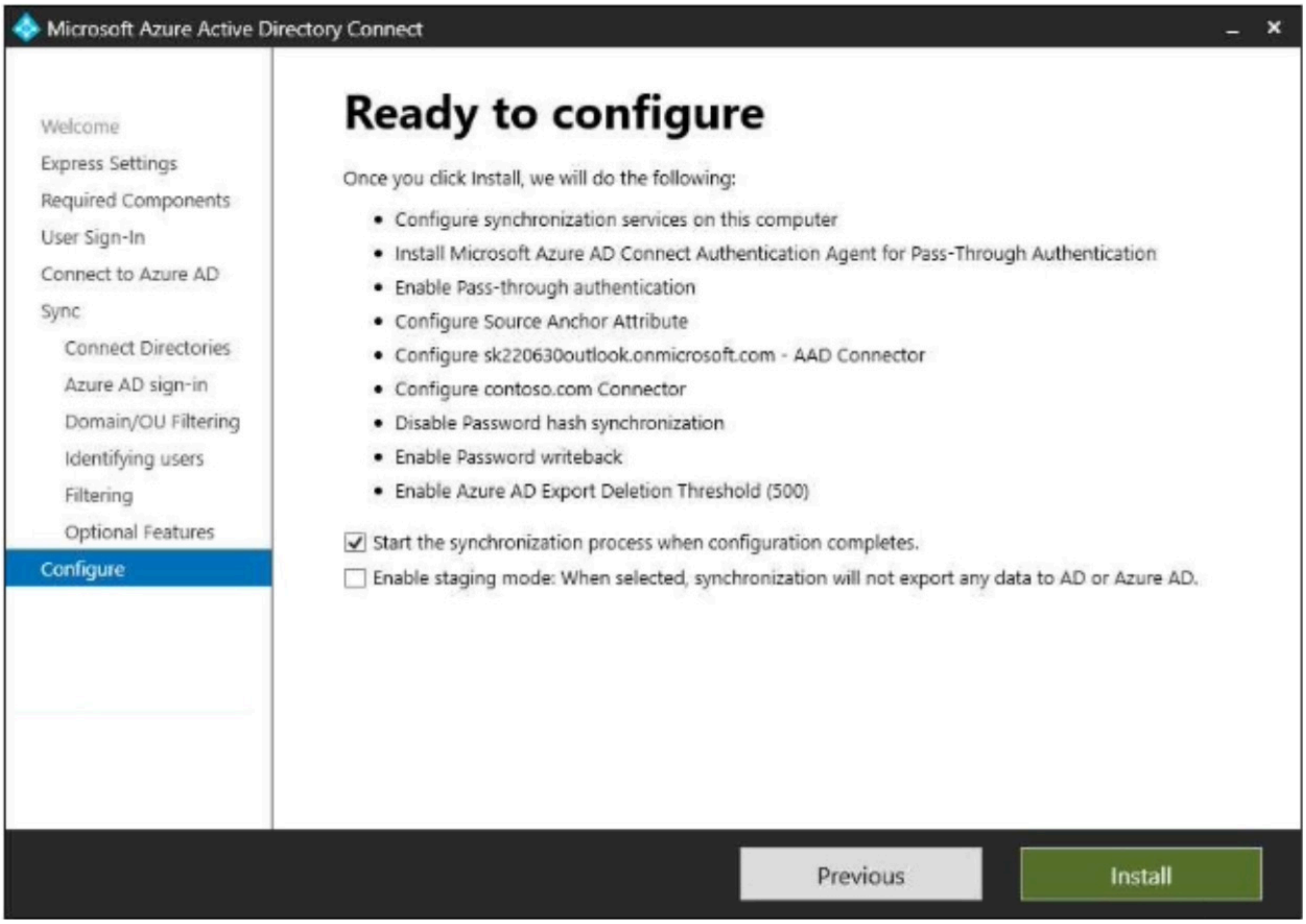
Directory: contoso.com

○ Sync all domains and OUs

● Sync selected domains and OUs

- □ contoso.com
  - □ Builtin
  - □ Computers
  - □ Domain Controllers
  - □ ForeignSecurityPrincipals
  - □ Infrastructure
  - □ LostAndFound
  - □ Managed Service Accounts
  - ☑ OU1
  - □ OU2
  - □ Program Data
  - □ System
  - ☑ Users

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



Ready to configure

Once you click Install, we will do the following:

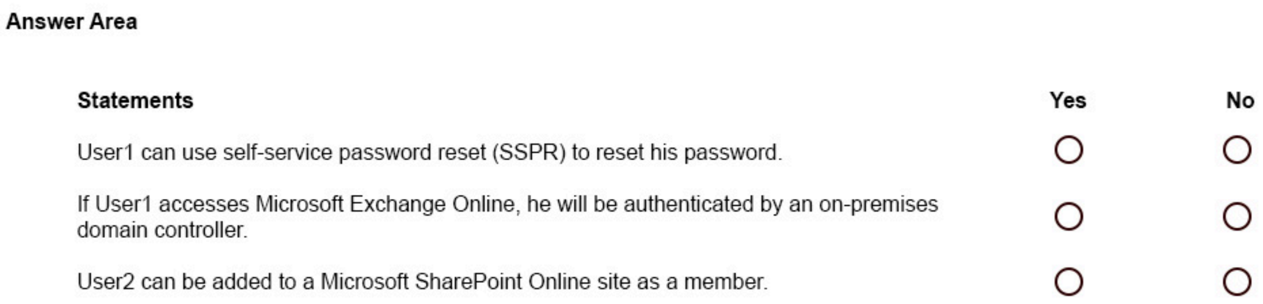
- Configure synchronization services on this computer
- Install Microsoft Azure AD Connect Authentication Agent for Pass-Through Authentication
- Enable Pass-through authentication
- Configure Source Anchor Attribute
- Configure sk220630outlook.onmicrosoft.com - AAD Connector
- Configure contoso.com 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.

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

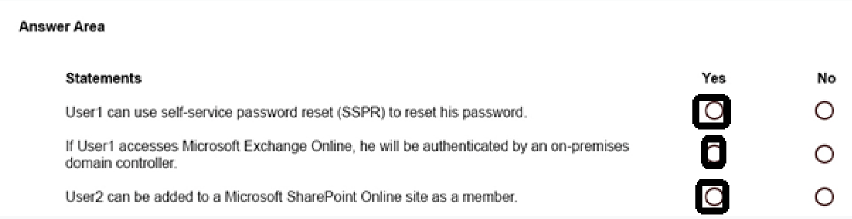
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 can use self-service password reset (SSPR) to reset his password.	○	○
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.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
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.	[✓ ○]	○

niesz1 Highly Voted 1 year, 2 months ago

YES

YES

NO- User 2 is not synced to 365

upvoted 33 times

Das_Duck 2 months, 3 weeks ago

I agree,

YES - Password writeback requires an Entra ID P1 license and by default SSPR is enabled (Always assume default settings in these questions unless given otherwise.)

YES

NO - Since OU filtering is being enable and User 2 is in an OU not being synced they will not be added as a member but can still be added as a GUEST.

upvoted 2 times

Another_one Highly Voted 1 year, 2 months 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 13 times

omnomsnom 6 months, 1 week ago

Agree, plus SSPR and password writeback require Entra ID P1 license as well. Nothing is known about the license status or SSPR service config, so we can't say that User 1 can use SSPR.

upvoted 2 times

OrangeSG 1 year, 1 month ago

Password write-backup are enabled in the last screenshoot.

upvoted 5 times

Siraf Most Recent 1 year ago

It looks like all users are synced according to the check box at the bottom.

So, even if OU2 is not synced, user2 will be synced.

If this is the case, the correct answer will be Yes - Yes - Yes

upvoted 6 times

penatuna 11 months, 3 weeks ago

Even if there is Users selected in Domain and OU filtering, User2 is not selected.

You can test this in ADUC: If you make new user in OU, it does not appear in Users, only in OU.

upvoted 5 times

[Removed] 1 year, 1 month 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 7 times

Kali13 1 year, 1 month ago

NO : password hash synchronization is disabled

YES : PTA is enabled

NO : No Sync to AAD

upvoted 2 times

mohamedbenamor 5 months, 1 week ago

Password Write back requires PTA

upvoted 1 times

Nivos23 1 year, 2 months ago

In my opinion it is

yes

yes

no

upvoted 4 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

Suggested Answer: *B*

Community vote distribution

B (100%)

OrangeSG Highly Voted 👍 7 months, 4 weeks 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 5 times

ralphw Highly Voted 👍 7 months, 1 week ago

I ated the purple berries. And this question is starting to make as much sense.

upvoted 5 times

Waris_khan8623 Most Recent 🕘 3 months, 2 weeks ago

Selected Answer: B

Set-MgUserLicense should be used in Microsoft Graph. Since it is missing so B is correct.

upvoted 1 times

Waris_khan8623 3 months, 2 weeks ago

Set-MgUserLicense should be used in Microsoft Graph. Since it is missing so B is correct.

upvoted 1 times

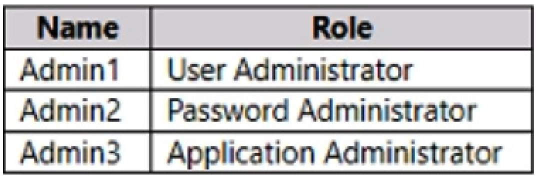
Ed2learn 8 months, 1 week ago

the other right answer.

upvoted 2 times

Question #62 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

B (78%) C (22%)

Julesy Highly Voted 1 year, 3 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/admin-roles-page#compare-roles

upvoted 12 times

Er_01 11 months, 2 weeks ago

Your link compares the role not the user.

upvoted 1 times

Alscoran 1 year, 1 month 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 2 times

strongline 6 months, 3 weeks ago

app admin is listed

upvoted 1 times

vladi72 Most Recent 6 months ago

Selected Answer: C

The answer is C.

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

Microsoft 365 admin center doesn't have Application Administrator role

upvoted 3 times

AlexBrazil 2 months ago

It does have. I've checked.

upvoted 2 times

NotanAdmin 7 months, 2 weeks ago

The correct answer is B. the Microsoft 365 admin center.

The Microsoft 365 admin center provides a centralized location where you can view and manage the role permissions of each user in your Azure AD tenant. This will allow you to easily compare the permissions of Admin1, Admin2, and Admin3, thus minimizing administrative effort. The other options do not provide this specific functionality.

upvoted 2 times

jtlucas99 7 months, 2 weeks ago

If you dont include the answer choices:
You should use the Azure Active Directory (Azure AD) Privileged Identity Management (PIM). Azure AD PIM provides a consolidated view of the role assignments across your organization, and it makes it easy to see who has what permissions.
If you include the answer options given:
B. the Microsoft 365 admin center.

The Microsoft 365 admin center provides a consolidated view of the role assignments across your organization, and it makes it easy to see who has what permissions. This solution minimizes administrative effort as it provides a centralized view and management of role assignments.

Please note that the other options:

A. the Microsoft 365 Defender portal is primarily used for managing security threats.
C. the Microsoft Entra admin center does not exist.
D. the Microsoft Purview compliance portal is used for data governance and compliance, not for managing user roles and permissions.

upvoted 4 times

jsca 8 months ago

Microsoft 365 admin center

upvoted 1 times

JuanZ 8 months, 1 week ago

Selected Answer: B

https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/assign-admin-roles?view=o365-worldwide#compare-roles
You can now compare permissions for up to 3 roles at a time so you can find the least permissive role to assign.

In the admin center

upvoted 4 times

emartiy 9 months, 1 week ago

Selected Answer: B

B is correct answer!

upvoted 1 times

Er_01 11 months ago

Selected Answer: B

So it is B because it actually has a “compare roles” button to compare up to 3 roles with. So the question is not about actually comparing roles, but where the menu option is to do it the MS way. More certification trivia!

upvoted 3 times

baz 11 months, 2 weeks ago

B. Testing we can see all role in both admin centers but 0365 admin has the option to "compare" roles.

upvoted 3 times

> **JanioHSilva** 10 months, 2 weeks ago
>
> I also tested it, it is correct
>
> upvoted 1 times

Er_01 11 months, 2 weeks ago

All 3 accounts are listed with role permissions in both portals. Since Entra is the place for ID management, the MS answer would be C. Also, the m365 portal lists the name of each permission not the actual syntax for each user right. Again, this supports the MS answer.

upvoted 1 times

cpaljchc4 11 months, 2 weeks ago

Selected Answer: B

I think there's a similar question in MS-102 and answer is M365 admin

upvoted 2 times

osi22 1 year ago

Selected Answer: C

Looking at the current state (03.01.24) we have the roles available in both B and C!
MS 365 Admin center - Application Administrator:
Create and manage enterprise application, registrations, and proxy

settings, excluding Microsoft Graph and Azure AD Graph
Consent to delegated permissions and application permissions
MS Entra Admin Center - Application Adminstrator:
Users in this role can add, manage, and configure enterprise
applications, app registrations and manage on-premises like app
proxy.

There's also no difference in the remaining roles, however thinking in the MS world, I still would go for C!

upvoted 2 times

Alscoran 1 year, 1 month ago

Selected Answer: C

Application Administrator not visible on M365 site

upvoted 1 times

klayytech 9 months, 1 week ago

https://admin.microsoft.com/#/rbac/directory

upvoted 1 times

Blagojche 1 year, 1 month ago

Application Administrator is present in M365 Admin Center, check!

upvoted 2 times

Alscoran 1 year, 1 month 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 1 year, 1 month 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 4 times

JaySapkota 1 year, 1 month ago

Selected Answer: C

Entra Admin Center has all the roles

upvoted 1 times

penatuna 1 year, 2 months ago

Selected Answer: B

Just tested with Microsoft 365 admin center, and you can compare all three roles mentioned.

upvoted 3 times

Ed2learn 1 year, 2 months 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 year ago

Eu acredito que você passou despercebido

upvoted 1 times

Question #63 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

B (100%)

⊟ **haazybanj** Highly Voted 1 year, 1 month 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 8 times

⊟ **Labelfree** 4 weeks ago

The Update-MgPolicyPermissionGrantPolicyExclude cmdlet is related to permission grant policies and doesn't apply to self-service sign-up restrictions.

upvoted 1 times

⊟ **Labelfree** Most Recent 4 weeks ago

Selected Answer: A

Correct answer is A. B isn't even a valid command.

upvoted 2 times

⊟ **Mole857** 1 month ago

Selected Answer: A

Isn't the correct answer A?

Update-MgOrganization AllowEmailVerifiedUsers $false would block self-service sign-up to the tenancy?

upvoted 2 times

⊟ **Tony416** 4 months ago

Selected Answer: B

MS Articles:

https://learn.microsoft.com/en-us/microsoft-365/commerce/subscriptions/manage-self-service-signup-subscriptions?view=o365-worldwide#block-users-from-signing-up

or

https://learn.microsoft.com/en-us/entra/identity/users/directory-self-service-signup#how-do-i-control-self-service-settings

upvoted 1 times

⊟ **Labelfree** 4 weeks ago

According to these links Update-MgPolicyAuthorizationPolicy which is not an option here. A is correct.

upvoted 1 times

d3ebc45 6 months, 4 weeks ago

Selected Answer: B

```
Import-Module Microsoft.Graph.Identity.SignIns
connect-MgGraph -Scopes "Policy.ReadWrite.Authorization"
$param = @{
allowedToSignUpEmailBasedSubscriptions=$true
allowEmailVerifiedUsersToJoinOrganization=$false
}
Update-MgPolicyAuthorizationPolicy -BodyParameter $param
```

upvoted 2 times

Panama469 5 months, 3 weeks ago

Yeah I'm not seeing the answer in this list, must be an updated question in the exam.

I used to be Set-MsolCompanySettings but your Graph commands are whats in the article.

upvoted 1 times

jtlucas99 7 months, 2 weeks ago

Per Copilot: C. Update-MgDomain.

The Update-MgDomain cmdlet is used to update the properties of a domain in Azure Active Directory (Azure AD). You can use this cmdlet to disable the ability for users to sign up for Microsoft 365 services using their contoso.com email address.

Please note that the other options:

A. Update-MgOrganization is not related to managing user sign-ups.
B. Update-MgPolicyPermissionGrantPolicyExclude does not exist.
D. Update-MgDomainFederationConfiguration is used to manage federation configurations, not user sign-ups.
Therefore, option C is the most suitable choice for this task.
If you dont give the answer options:
To prevent users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services, you should run the Set-MsolCompanySettings cmdlet with the -UsersPermissionToCreateSelfServiceApplication parameter set to $false.

upvoted 1 times

JuanZ 8 months, 3 weeks ago

la opción A, es la correcta.
https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup

upvoted 1 times

belyo 10 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/microsoft-365/admin/misc/self-service-sign-up?view=o365-worldwide#:~:text=To%20control%20whether%20users%20can%20sign%20up%20for%20self%2Dservice%20subscriptions%2C%20use%20the%20Update%2

however when you go to MG documentation for that CMDlet this parameter is not even listed. Most likely is changed to these
allowedToSignUpEmailBasedSubscriptions=$true
allowEmailVerifiedUsersToJoinOrganization=$false

upvoted 2 times

Shuihe 1 year ago

B
You use the Update-MgPolicyAuthorizationPolicy cmdlet with the AllowAdHocSubscriptions parameter to control whether users can sign up for self-service sign-up subscriptions.

upvoted 1 times

rabicon 1 year ago

Selected Answer: B

I stand for B

upvoted 1 times

Ed2learn 1 year, 2 months 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

Question #64 *Topic 1*

HOTSPOT

-

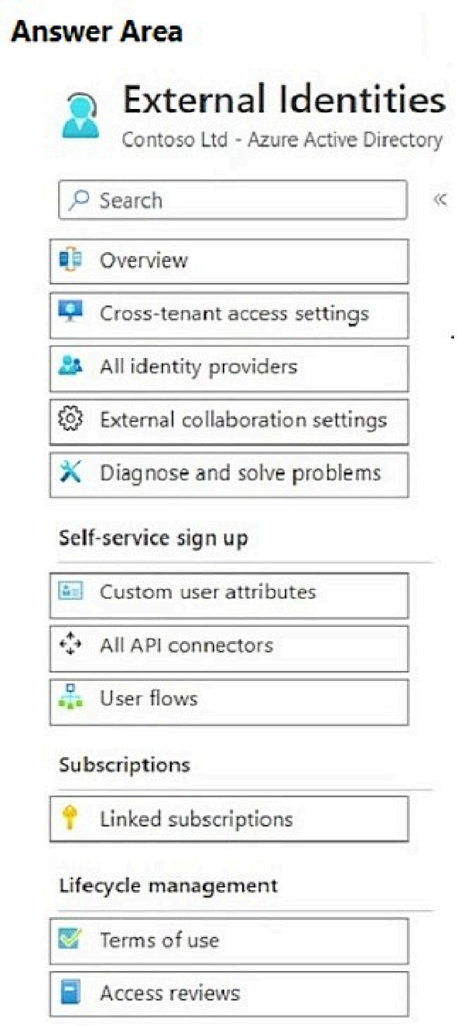
You have an Azure AD tenant.

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.

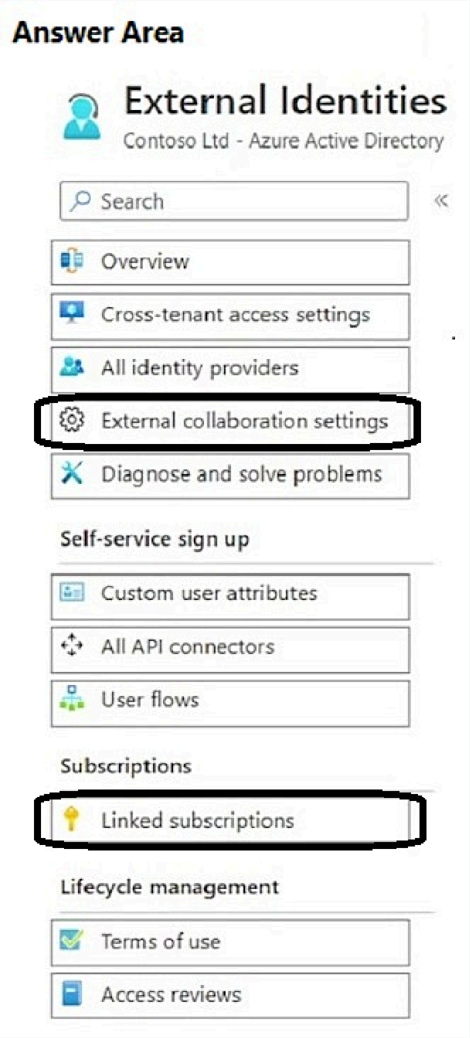


Answer Area

External Identities

Contoso Ltd - Azure Active Directory

Suggested Answer:



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

Nivos23 Highly Voted 1 year, 2 months ago

I think the answer is correct

External Collabration settings

And

Linked Subscriptions

upvoted 7 times

Nail Most Recent 1 month, 4 weeks ago

1st one is definitely Cross-tenant access settings. Go take a look for yourself in Entra. Check out the Default Settings tab and then "edit inbound defaults". It specifically lets you configure "B2B Collaboration".

upvoted 1 times

AlexBrazil 2 months ago

Answers:

Cross-tenant access settings

Linked subscriptions

Because:

External collaboration settings => It defines "Guest user access restrictions", "Guest invite restrictions", "Enable guest self-service sign up via user flows", "External user leave settings" and "Collaboration restrictions".

Cross-tenant access settings => It allows the configuration of external Microsoft Entra tenants not listed on the organizational settings tab. You can configure "Inbound access settings", "Outbound access settings", "Tenant restrictions".

All identity providers => It Configures any of predefined built-in identity providers for users to authenticate and access the resources using their external identities.

Linked subscriptions => It allows configuring the Monthly Active Users (MAU).

upvoted 1 times

⊟ **Justin0020** 8 months, 3 weeks ago

My answer is:

Cross tenant-access settings

Linked Subscriptions

upvoted 3 times

⊟ **penatuna** 1 year, 1 month 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 2 times

⊟ **penatuna** 1 year, 1 month 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 year, 1 month ago

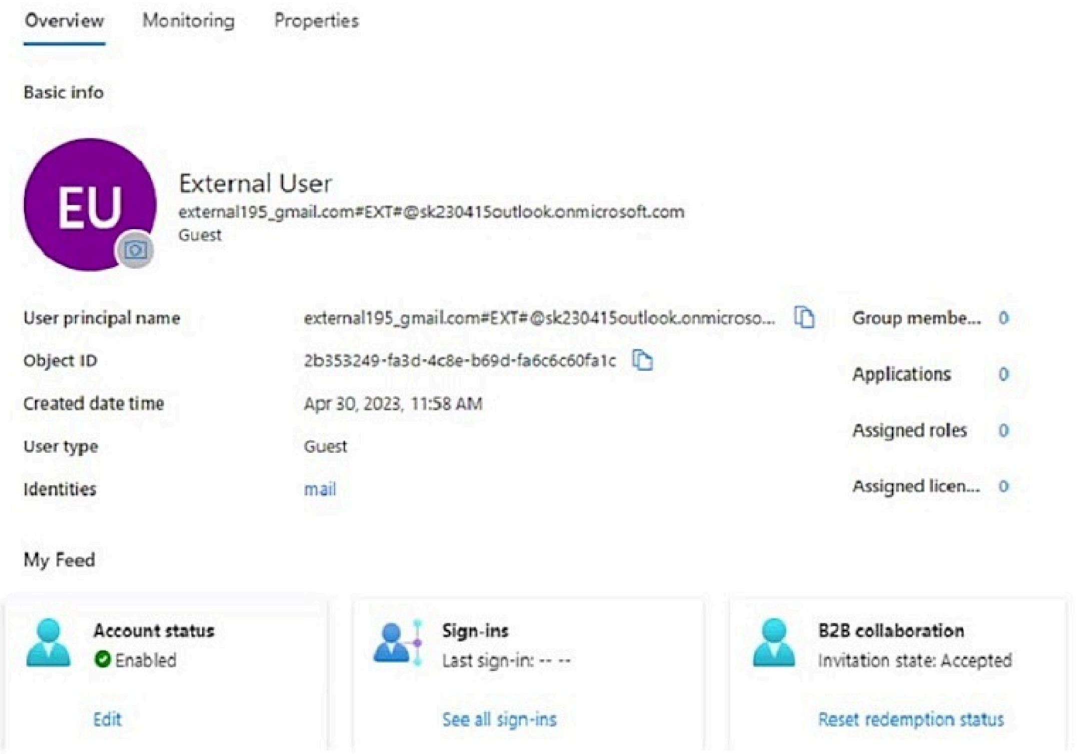
In Entra ID's Cross-tenant access settings it actually says this:

"Use cross-tenant access settings to manage collaboration with external Microsoft Entra tenants. For non-Microsoft Entra tenants, use collaboration settings."

upvoted 2 times

Question #65 *Topic 1*

You have an Azure AD tenant that contains the external user shown in the following exhibit.



External User
external195_gmail.com#EXT#@sk230415outlook.onmicrosoft.com
Guest

User principal name	external195_gmail.com#EXT#@sk230415outlook.onmicroso...	Group membe...	0
Object ID	2b353249-fa3d-4c8e-b69d-fa6c6c60fa1c	Applications	0
Created date time	Apr 30, 2023, 11:58 AM	Assigned roles	0
User type	Guest	Assigned licen...	0
Identities	mail		

My Feed

Account status
Enabled
Edit

Sign-ins
Last sign-in: -- --
See all sign-ins

B2B collaboration
Invitation state: Accepted
Reset redemption status

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.

Suggested Answer: *D*

Community vote distribution

D (100%)

⊟ **OrangeSG** Highly Voted 1 month, 3 weeks 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 11 times

⊟ **kijken** Most Recent 1 month, 3 weeks ago

Cool,
I didnt know this one, I would have recreated the guest user

upvoted 4 times

⊟ **kijken** 1 month, 3 weeks ago

answer is D btw

upvoted 3 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

Suggested Answer: *A*

Community vote distribution

A (100%)

⊟ **haazybanj** Highly Voted 1 year, 1 month 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 8 times

⊟ **Labelfree** Most Recent 4 weeks ago

Selected Answer: A

Untested atm but sounds right.

upvoted 1 times

⊟ **Jackdisuin** 10 months, 1 week ago

Correct. External collaboration settings > collaboration restrictions

upvoted 2 times

Question #67 *Topic 1*

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.

Suggested Answer: *D*

Community vote distribution

B (100%)

haazybanj Highly Voted 👍 1 year, 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 9 times

hml_2024 Most Recent 4 months, 1 week ago

B is correct.Access reviews in Azure AD allow you to schedule regular reviews of group memberships, including guest users. By setting up an access review, User1, as the owner of Group1, can be notified to validate the guest memberships periodically (e.g., every three months).

upvoted 1 times

loukyeexamtopic 5 months, 1 week ago

I would go for B too, but it is actually D people.

Check:https://learn.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-groups-expiration-policy?view=o365-worldwide

upvoted 1 times

penatuna 5 months, 1 week ago

No, it's not. Group expiration policy can help remove inactive groups, not to validate the guest membership of Group.

upvoted 1 times

Nazir97 1 year, 1 month ago

Selected Answer: B

Access review

upvoted 1 times

penatuna 1 year, 1 month 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 2 times

penatuna 1 year, 1 month 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 4 times

⊟ **einkaufacs** 1 year, 2 months ago

Selected Answer: B

Validatating a membership is access review, in my opinion.

upvoted 3 times

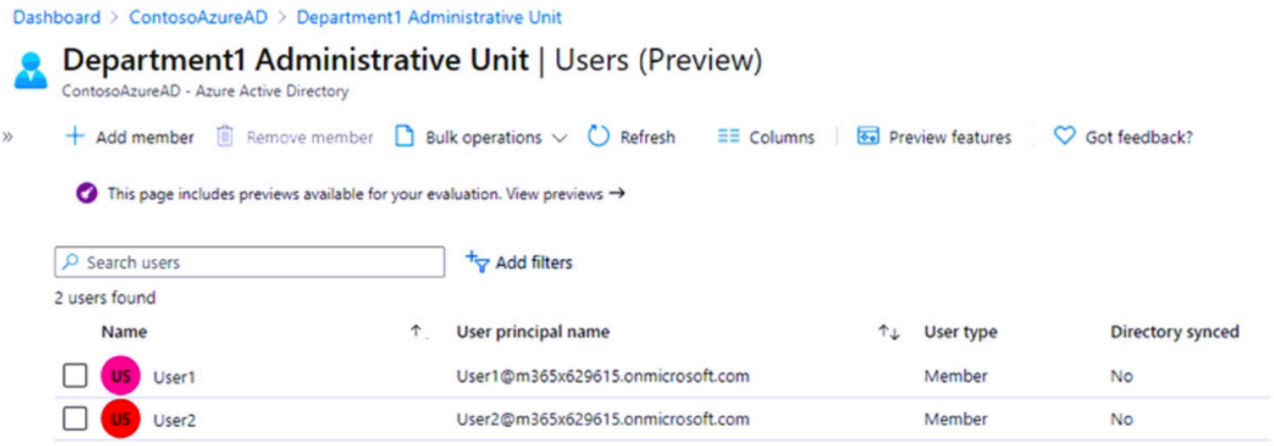
Question #68 *Topic 1*

HOTSPOT

-

You have a Microsoft Entra 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.)



Department1 Administrative Unit | Users (Preview)

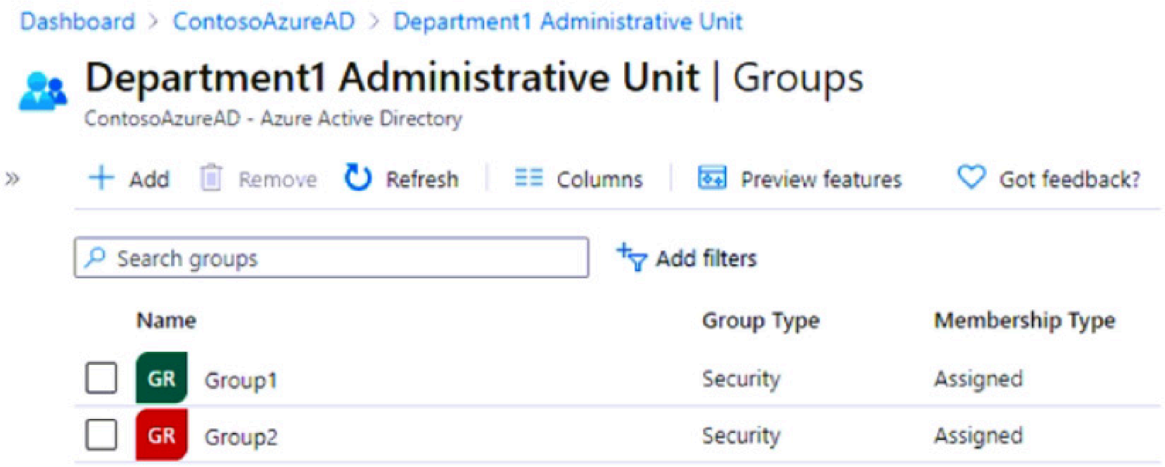
ContosoAzureAD - Azure Active Directory

This page includes previews available for your evaluation. View previews →

2 users found

	Name ↑	User principal name ↑↓	User type	Directory synced
□	User1	User1@m365x629615.onmicrosoft.com	Member	No
□	User2	User2@m365x629615.onmicrosoft.com	Member	No

Department1 has the groups shown in the Groups exhibit. (Click the Groups tab.)

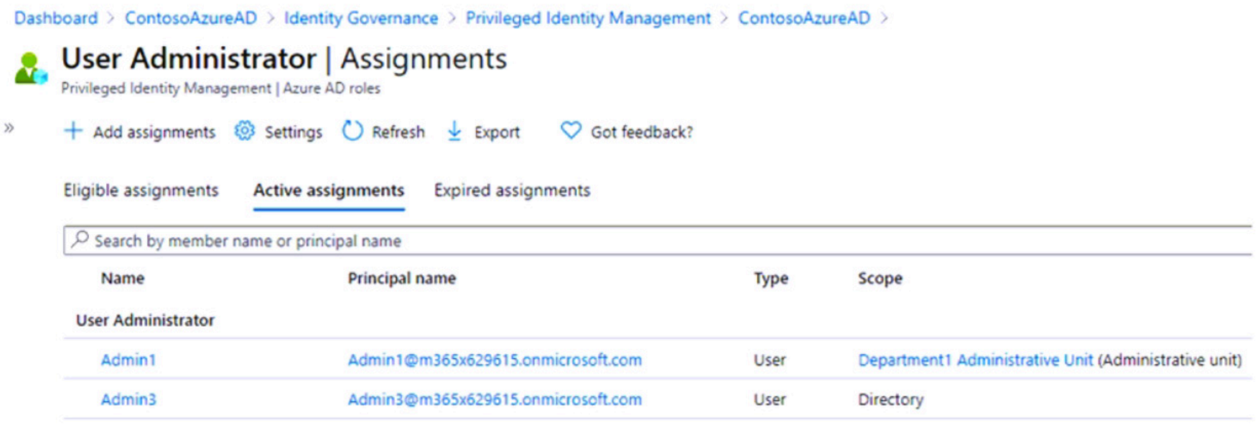


Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

	Name	Group Type	Membership Type
□	Group1	Security	Assigned
□	Group2	Security	Assigned

The User Administrator role assignments are shown in the Assignments exhibit (Click the Assignments tab.)



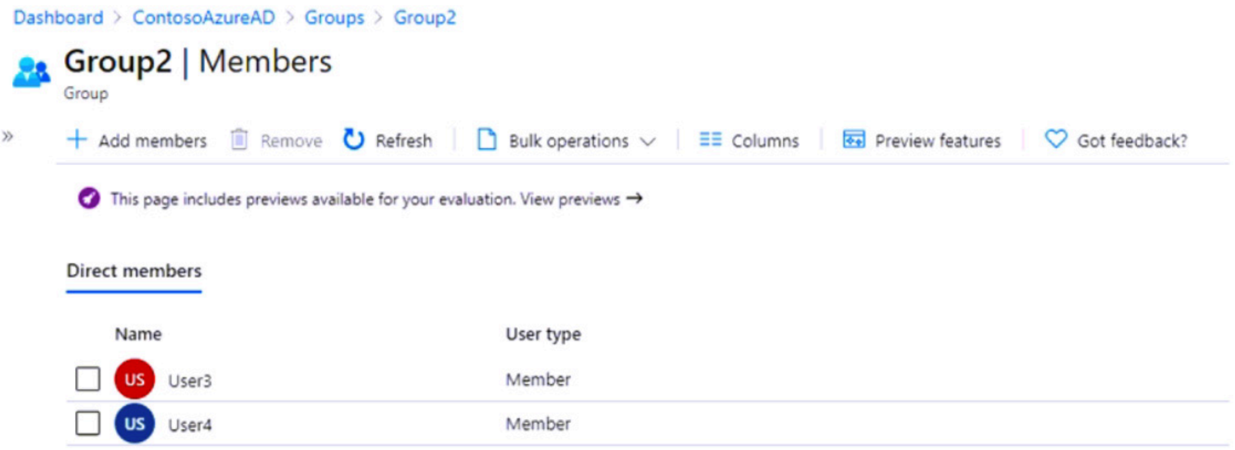
Dashboard > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >
»
+ Add assignments
Settings
Refresh
Export
Got feedback?
Eligible assignments
Active assignments
Expired assignments
Search by member name or principal name

User Administrator | Assignments

Privileged Identity Management | Azure AD roles

Name	Principal name	Type	Scope
User Administrator			
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Department1 Administrative Unit (Administrative unit)
Admin3	Admin3@m365x629615.onmicrosoft.com	User	Directory

The members of Group2 are shown in the Group2 exhibit. (Click the Group2 tab.)


Dashboard > ContosoAzureAD > Groups > Group2
»
+ Add members
Remove
Refresh
Bulk operations
Columns
Preview features
Got feedback?
This page includes previews available for your evaluation. View previews →
Direct members

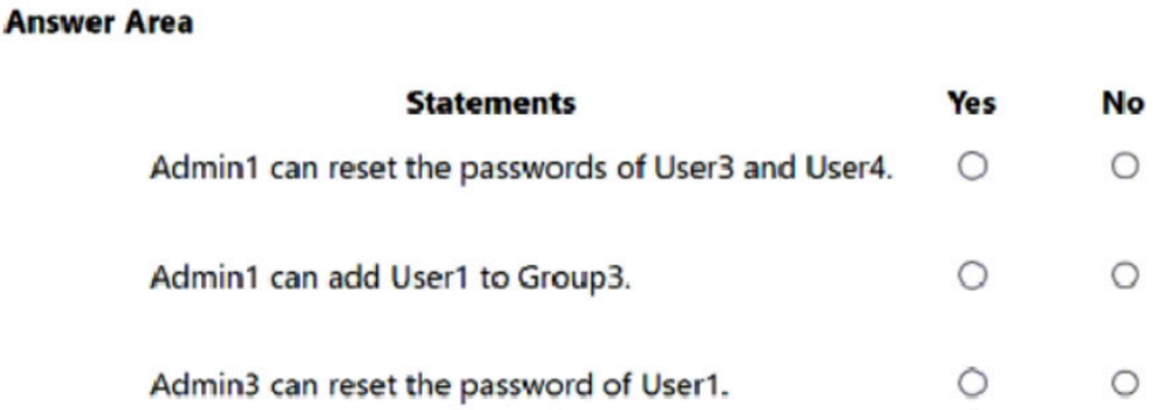
Group2 | Members

Group

	Name	User type
□	US User3	Member
□	US User4	Member

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

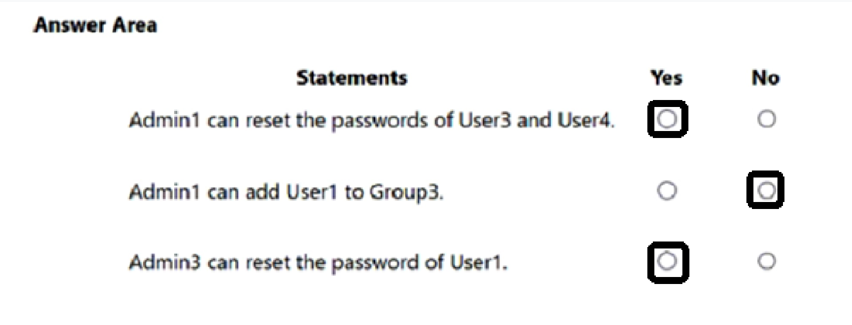
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group3.	○	○
Admin3 can reset the password of User1.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	[✓ ○]	○
Admin1 can add User1 to Group3.	○	[✓ ○]
Admin3 can reset the password of User1.	[✓ ○]	○

⊟ **SFAY** Highly Voted 11 months, 2 weeks ago

No, No, Yes

upvoted 25 times

⊟ **Bossdwarf** Highly Voted 10 months, 3 weeks ago

No

No

Yes

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).

upvoted 13 times

⊟ **Ody** 10 months, 2 weeks ago

Link.

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative-units#groups

upvoted 2 times

⊟ **[Removed]** Most Recent 11 months ago

Isn't the given answer correct? User3 and User4 are both assigned to group2 which is assigned to the Department1 AU (second screenshot), so that would be YNY for the answer? Open to learning if that's correct or not...

upvoted 2 times

⊟ **einkaufacs** 10 months ago

I thought it the same way. But here nesting users in groups does not work. "Adding a group to an administrative unit brings the group itself into the management scope of the administrative unit, but not the members of the group"
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative-units#groups

upvoted 7 times

⊟ **Tim1119** 11 months, 1 week ago

No, No, Yes

Admin1 has a only the permissions on Department1 administrative unit.
User3 and User4 are not assigned to Department1, so Admin1 has no permissions to reset passwords.

Group3 is not assigned to Department1.

Admin3 has permissions for the entire Directory.

upvoted 9 times

⊟ **loukyexamtopic** 5 months, 1 week ago

incorrect, they are actually part of department1 admin unit, check pictures again

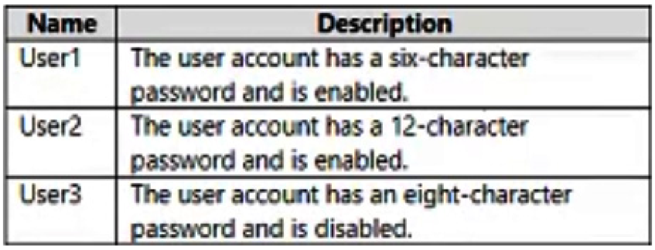
upvoted 1 times

Question #69 *Topic 1*

HOTSPOT

-

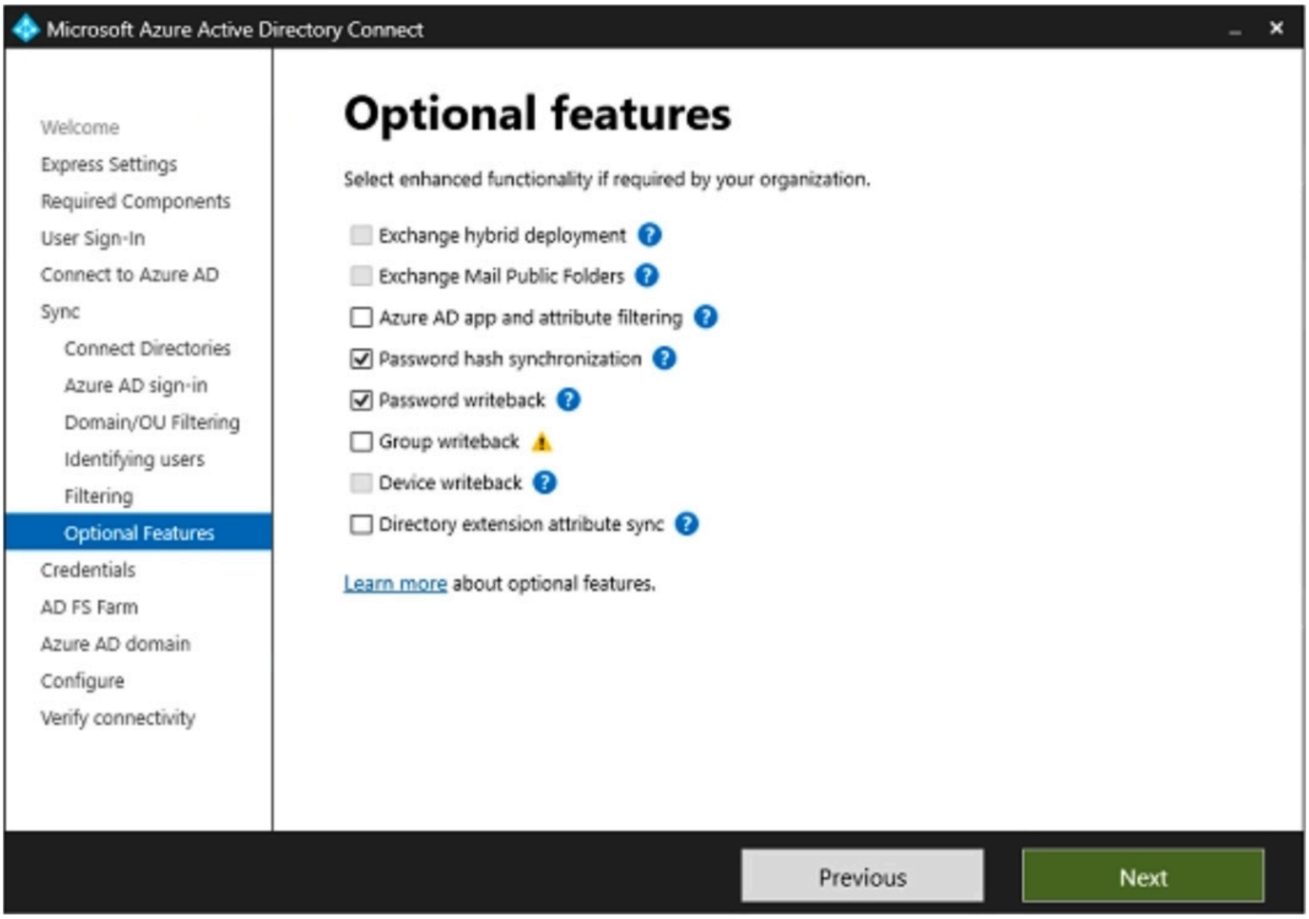
Your network contains an on-premises Active Directory Domain Services (AD DS) domain named fabrikam.com. The domain contains an Active Directory Federation Services (AD FS) instance and a member server named Server1 that runs Windows Server. The domain contains the users shown in the following table.



Name	Description
User1	The user account has a six-character password and is enabled.
User2	The user account has a 12-character password and is enabled.
User3	The user account has an eight-character password and is disabled.

You have a Microsoft Entra tenant named contoso.com that is linked to a Microsoft 365 subscription.

You establish federation between fabrikam.com and contoso.com by using a Microsoft Entra Connect instance that is configured as shown in the following exhibit.



Optional features

Select enhanced functionality if required by your organization.

□ Exchange hybrid deployment

□ Exchange Mail Public Folders

□ Azure AD app and attribute filtering

☑ Password hash synchronization

☑ Password writeback

□ Group writeback

□ Device writeback

□ Directory extension attribute sync

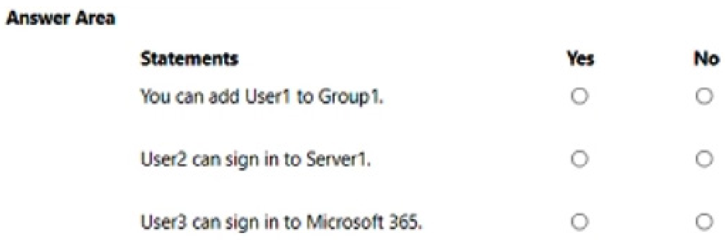
Learn more about optional features.

You perform the following tasks in contoso.com:

- Create a group named Group1.
- Disable User2.
- Enable User3.

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

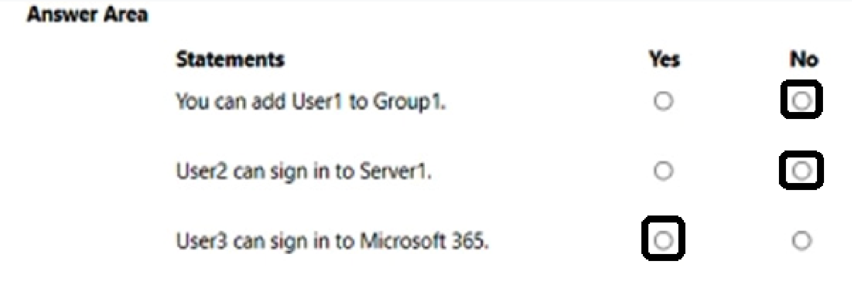
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
You can add User1 to Group1.	○	○
User2 can sign in to Server1.	○	○
User3 can sign in to Microsoft 365.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
You can add User1 to Group1.	○	[✓ ○]
User2 can sign in to Server1.	○	[✓ ○]
User3 can sign in to Microsoft 365.	[✓ ○]	○

MatExam Highly Voted 11 months, 1 week ago

I would say:
Yes: Group1 is created in the entra ID tenant, and the user is synced, so this is possible. It doesn't state that the group should be visible on-prem
Yes: The user is a directory-synced user, so authority lies on-prem. Disabling it from the Entra ID portal will have no effect. The server is also an on-prem server. Disabling should be done in on-prem adds
No: for the same reason as above, you enable the account in the entra id tenant, but the account is directory synced, so authority lies with the on-prem AD, enabling from the portal is not possible...

upvoted 17 times

naveenbio 4 weeks, 1 day ago

It is correct (YES, YES & NO)

upvoted 1 times

krisbla 1 month, 3 weeks ago

Where did it say Group 1 was created in the Entra ID Tenant and synced? I see a yellow triangle with "!" on Group writeback.

upvoted 1 times

ultravincent 9 months, 2 weeks ago

Funny how the correct answers are the exact opposite of what is shown as the solution. 3/3 wrong.

upvoted 5 times

mkendell Highly Voted 7 months, 2 weeks ago

The question states that changes are made in the Contoso (Azure domain not on-prem), Password writeback and hash synchronisation is enabled.

So my answers are:

Yes: Group1 is created in the entra ID tenant, and the user is synced and enabled.

Yes: The user is a directory-synced but even with writeback enabled, Disabling the account from the Entra ID portal will not lock-out the corresponding on-prem account.

No: the account us directory synchronised and will lock again if you try to enable it

upvoted 6 times

rtsh06 Most Recent 1 month, 1 week ago

This is what I feel should be the correct answer. I am open to feedback. please let me know if there is anything wrong.

Box 1: No. Group Writeback is not enabled.
Box 2: No. User 2 can sign in to Server 1. As User2 is disabled, it will not allow him to sign in to Server.
Box 3: Yes, User3 is enabled, so he should be abled to sign in to Microsoft 365.

upvoted 1 times

⊟ **HartMS** 8 months, 3 weeks ago

YYY

In Summary:

The cloud-enabled status benefits User 3 for M365 access, but the disabled on-prem status prevents them from logging into Server1. User 2 can access Server1 with valid credentials because their cloud status isn't relevant for on-prem authentication via ADFS.

upvoted 1 times

⊟ **emartiy** 9 months, 1 week ago

It says, 3 actions performed at contoso.com (isn't it AD DS? instead of Entra ID?)
So, you can add user 1 to Group1 in AD DS.
User2 is disabled, can't sign in to any server.
User3 can sign in to entra since password length is suffient to entra id SSPR etc.
YES - NO - YES would be my selections for this question.

upvoted 3 times

⊟ **einkaufacs** 11 months ago

I am confused. If you have a synced user, you can not enable or disable the user in Azure AD. You do this in the AD DS.

upvoted 3 times

⊟ **Ody** 10 months, 3 weeks ago

It says we have write-back turned on and I haven't tested it, but Entra ID now has a disable option on the User. I also see it on a synched user.

upvoted 2 times

⊟ **Ody** 10 months, 2 weeks ago

This seems to imply that disabling in Azure will only cause Entra ID connect to re-enable it in the tenant.

https://learn.microsoft.com/en-us/answers/questions/1072787/how-do-i-get-actions-such-as-disabling-an-account

upvoted 3 times

⊟ **[Removed]** 11 months, 1 week ago

Why would the first one be no?

upvoted 1 times

⊟ **Ody** 10 months, 3 weeks ago

I was thinking it was due to the 8 character minimum in Entra ID

upvoted 2 times

⊟ **Ody** 10 months, 2 weeks ago

Rethinking this and think the answer should be Yes for User 1.

"The Microsoft Entra password policy doesn't apply to user accounts synchronized from an on-premises AD DS environment using Microsoft Entra Connect, unless you enable EnforceCloudPasswordPolicyForPasswordSyncedUsers."

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy

upvoted 2 times

⊟ **krisbla** 1 month, 2 weeks ago

1 is NO, there is an 8 character limit in Entra, they'll be prompted to change the password to meet the policy but the question is, "Can they log in?" ---> "No."
(check link above)

upvoted 1 times

⊟ **Tim1119** 11 months, 1 week ago

You can add the user to the group, however it is not available on-premise as group writeback is not enabled.

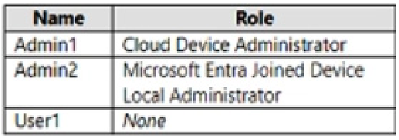
upvoted 1 times

Question #70 Topic 1

HOTSPOT

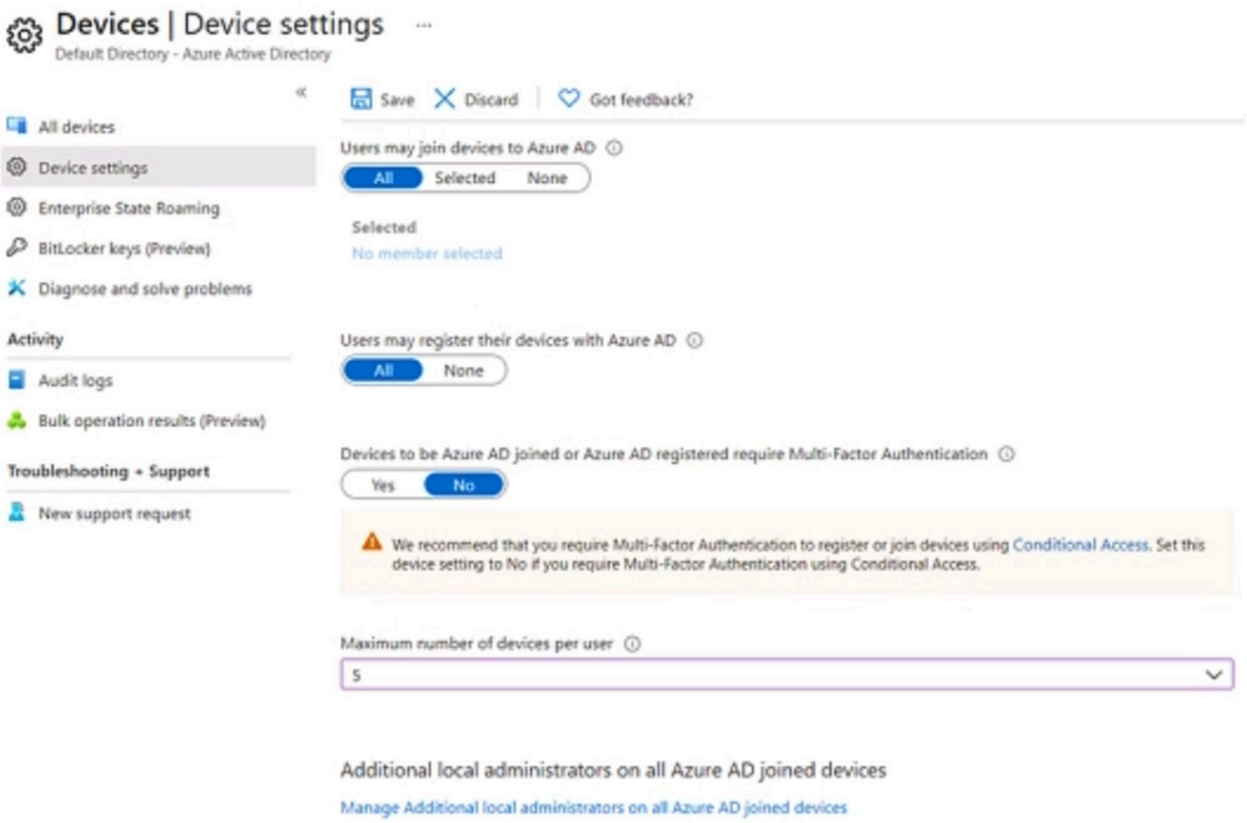
-

You have a Microsoft Entra tenant that has a Microsoft Entra ID P2 service plan. The tenant contains the users shown in the following table.



Name	Role
Admin1	Cloud Device Administrator
Admin2	Microsoft Entra Joined Device Local Administrator
User1	*None*

You have the Device settings shown in the following exhibit.



Devices | Device settings ...
Default Directory - Azure Active Directory
«
All devices
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Diagnose and solve problems
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Save
Discard
Got feedback?

Users may join devices to Azure AD ⓘ

● All ○ Selected ○ None

Selected

No member selected

Users may register their devices with Azure AD ⓘ

● All ○ None

Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication ⓘ

○ Yes ● No

⚠ We recommend that you require Multi-Factor Authentication to register or join devices using Conditional Access. Set this device setting to No if you require Multi-Factor Authentication using Conditional Access.

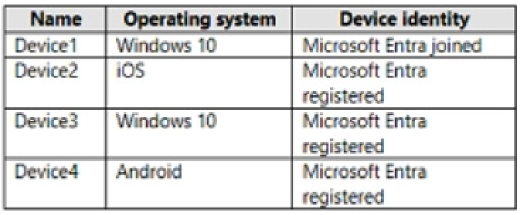
Maximum number of devices per user ⓘ

5

Additional local administrators on all Azure AD joined devices

Manage Additional local administrators on all Azure AD joined devices

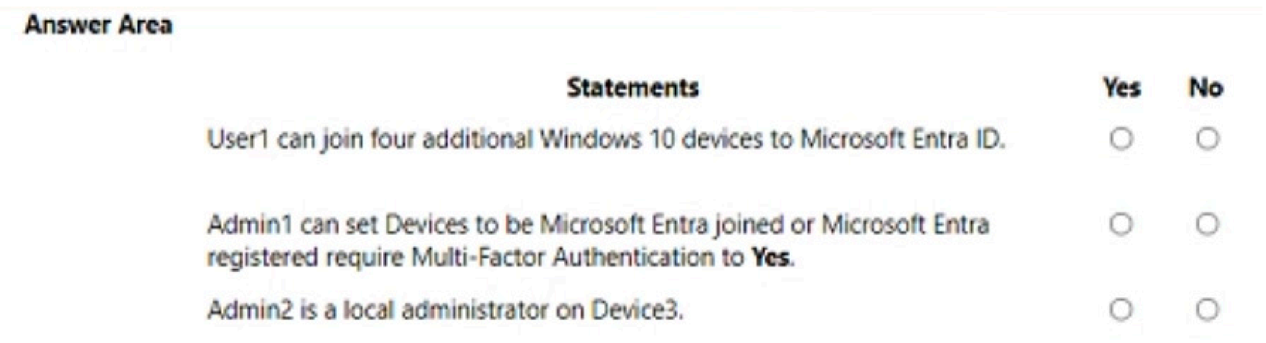
User1 has the devices shown in the following table.



Name	Operating system	Device identity
Device1	Windows 10	Microsoft Entra joined
Device2	iOS	Microsoft Entra registered
Device3	Windows 10	Microsoft Entra registered
Device4	Android	Microsoft Entra registered

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

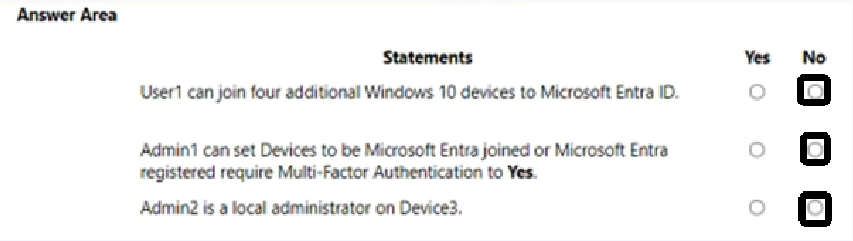
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Microsoft Entra ID.	○	○
Admin1 can set Devices to be Microsoft Entra joined or Microsoft Entra registered require Multi-Factor Authentication to **Yes**.	○	○
Admin2 is a local administrator on Device3.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Microsoft Entra ID.	○	[✓ ○]
Admin1 can set Devices to be Microsoft Entra joined or Microsoft Entra registered require Multi-Factor Authentication to **Yes**.	○	[✓ ○]
Admin2 is a local administrator on Device3.	○	[✓ ○]

Anusha_2000 Highly Voted 11 months, 1 week ago

No
Yes
No

upvoted 24 times

penatuna Highly Voted 10 months, 4 weeks ago

1) NO

Maximum number of devices: This setting enables you to select the maximum number of Microsoft Entra joined or Microsoft Entra registered devices that a user can have in Microsoft Entra ID. 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, Microsoft Entra ID sets it to 100. You can also use Unlimited to enforce no limit other than existing quota limits.

Note! The Maximum number of devices setting applies to devices that are either Microsoft Entra joined or Microsoft Entra registered. This setting doesn't apply to Microsoft Entra hybrid joined devices.

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

upvoted 10 times

penatuna 10 months, 4 weeks ago

2) YES

Admin1 is a Cloud Device Administrator. You must be assigned one of the following roles to manage device settings:

- Global Administrator
- Cloud Device Administrator

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

3) NO

This only applies to Win 10/11 Entra JOINED devices. This device is only registered.

upvoted 12 times

penatuna 10 months, 4 weeks ago

NOTE:

Additional local administrators on Microsoft Entra 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 Microsoft Entra ID. Global Administrators in Microsoft Entra ID and device owners are granted local administrator rights by default. This option is a premium edition capability available through products like Microsoft Entra ID P1 or P2 and Enterprise Mobility + Security.

https://learn.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin
https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register
https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin#manage-administrator-privileges-using-microsoft-entra-

groups-preview
https://learn.microsoft.com/en-us/entra/identity/devices/manage-device-identities
upvoted 8 times

rtsh06 Most Recent 1 month, 1 week ago
This is based on my understanding.

Explanation:
Box 1: No. User1 already has 4 devices registered under his name and there is limit to register max 5 devices. Hence User 1 can register additional 1 device only.

Box 2: Yes. I tested this condition in my test tenant, I was able to change the Require Multi-Factor Authentication from No to Yes.

Box 3: No. Condition 3 is applicable to Win 10/11 Entra Joined devices. The keyword is JOINED. Device 3 is Entra Registered.
upvoted 1 times

MadsB 1 month, 3 weeks ago
No
No
No
upvoted 1 times

BRZSZCL 2 months, 1 week ago
When maximum number of devices limit is set in Azure tenant, it is basically irrelevant of Entra Joint or Entra registered devices? My idea was answer to 1 would be yes, becuase there was only 1 Entra Joined device, but in discussion pannel i have realised it is different.
upvoted 1 times

hml_2024 4 months ago
Check Question 21

Yes
No
No
upvoted 3 times

thetootall 5 months, 2 weeks ago
1) NO
Maximum number of devices: 5
User already has 4 in Entra - they can only add 1 more

2) YES
Admin1 is a Cloud Device Administrator.

3) NO
This only applies to Win 10/11 Entra JOINED devices. This device is only registered.
upvoted 3 times

jarattdavis 5 months, 3 weeks ago
1. NO = Devices already added: 2 (1 Microsoft Entra joined + 1 Microsoft Entra registered). Remaining devices you can add: 5 - 2 = 3. So, you can add 3 additional Windows 10 devices, whether they are Microsoft Entra joined or Microsoft Entra registered.
upvoted 1 times

NotanAdmin 7 months, 2 weeks ago
2) No
Cloud Device Admin - This is a privileged role. Users in this role can enable, disable, and delete devices in Microsoft Entra ID and read Windows 10 BitLocker keys (if present) in the Azure portal. The role does not grant permissions to manage any other properties on the device.
upvoted 3 times

emartiy 9 months, 1 week ago
YES -1 device is joined 1 registered so user can still join 4 device to azure since count is 1/5 (join important, not register)
NO - Cloud Device Asdmins has no privileged to perform this option.
NO - Device is not azure joined. It is only registered. So, this option also not valid.
upvoted 7 times

Futfuyfyjfj 8 months, 1 week ago

The device maximum has nothing to do with the join type, it’s an overall limit regardless join of register so the first one is a NO.

upvoted 4 times

> **Alcpt** 7 months, 1 week ago
>
> correct. the answer is NO NO NO
>
> upvoted 1 times

ELQUMS 11 months, 1 week ago

No

Yes

No

upvoted 4 times

dbz_34 11 months, 1 week ago

no

yes

no

upvoted 4 times

You have an Azure subscription named Sub1 that contains a user named User1.

You need to ensure that User1 can purchase a Microsoft Entra Permissions Management license for Sub1. The solution must follow the principle of least privilege.

Which role should you assign to User1?

A. Global Administrator

B. Billing Administrator

C. Permissions Management Administrator

D. User Access Administrator

Suggested Answer: *B*

Community vote distribution

B (77%) A (23%)

ignitelatam Highly Voted 👍 11 months, 2 weeks ago

Selected Answer: B

Correct

upvoted 8 times

Alcpt 8 months, 1 week ago

No. Don't guess. It's A.
https://learn.microsoft.com/en-us/entra/permissions-management/product-roles-permissions#enabling-permissions-management
Enabling Permissions Management
To activate a trial or purchase a license, you must have Global Administrator permissions.

upvoted 1 times

omnomsnom 6 months ago

The article has been updated and now reads Billing Administrator required to purchase or active a trial. To onboard (after purchase), GA is needed. The question only asks about buying the license.

upvoted 3 times

Alcpt 7 months, 1 week ago

im guessing here. yes its B.
pity there is no delete button

upvoted 1 times

mohamedbenamor Most Recent ⏱ 1 month, 1 week ago

Selected Answer: B

https://learn.microsoft.com/en-us/entra/permissions-management/product-roles-permissions#enabling-permissions-management

upvoted 1 times

seleneliane 3 months, 2 weeks ago

It's A that i will choose!

upvoted 1 times

jim85 6 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/entra/permissions-management/product-roles-permissions - Billing Admin

upvoted 1 times

BMO3 8 months, 1 week ago

User1 need to be able to purchase the license. Only Global admins can purchase an Entra Permissions Management license, as stated in MS docs: https://learn.microsoft.com/en-us/entra/permissions-management/product-roles-permissions

upvoted 3 times

criminal1979 8 months, 3 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-us/entra/permissions-management/onboard-enable-tenant

upvoted 1 times

⊟ **Alcpt** 8 months, 1 week ago

No. You enable MEPM via billing admin. You use Global admin to buy licenses. Read the question. Don't guess.

upvoted 1 times

⊟ **emartiy** 9 months, 1 week ago

Selected Answer: B

Correct

upvoted 1 times

⊟ **Menard001** 9 months, 2 weeks ago

Selected Answer: B

The solution must follow the principle of least privilege.

is the global admin is least privilege account?
I think that is billing admin

upvoted 1 times

⊟ **penatuna** 11 months ago

Selected Answer: A

I would say A. Global Administrator.

"To activate a trial or purchase a license, you must have Global Administrator permissions."
https://learn.microsoft.com/en-us/entra/permissions-management/product-roles-permissions#enabling-permissions-management

"There are two ways to activate a trial or a full product license.
The first way is to go to the Microsoft 365 admin center.
• Sign in as a Global Administrator for your tenant.
• Go to Setup and sign up for a Microsoft Entra Permissions Management trial.
• For self-service, Go to the Microsoft 365 portal to sign up for a 45-day free trial or to purchase licenses.
The second way is through Volume Licensing or Enterprise agreements.
• If your organization falls under a volume license or enterprise agreement scenario, contact your Microsoft representative."
https://learn.microsoft.com/en-us/entra/permissions-management/onboard-enable-tenant#activate-a-free-trial-or-paid-license

upvoted 3 times

⊟ **Menard001** 9 months, 2 weeks ago

The solution must follow the principle of least privilege.

is the global admin is least privilege account?
I think that is billing admin

upvoted 1 times

⊟ **Millla** 9 months, 3 weeks ago

Correct answer

upvoted 1 times

⊟ **penatuna** 11 months ago

Wrong Answers:
B. Billing Administrator makes purchases, manages subscriptions, manages support tickets, and monitors service health. Can't add role assignments so cannot activate Permissions Management Administrator role.

C. Permissions Management Administrator
Assign the Permissions Management Administrator role to users who need to do the following tasks:
• Manage all aspects of Microsoft Entra Permissions Management, when the service is present.

D. User Access Administrator is an Azure RBAC role, that lets you manage user access to Azure resources. Nothing to do with Permission Management.

upvoted 1 times

⊟ **hml_2024** 3 months, 2 weeks ago

This is in yesterday exam. I choose "C".
upvoted 1 times

penatuna 7 months, 2 weeks ago
Ok, things have changed since I answered to this question. Before the link below said Global Admin, now it says Billing Administrator:
https://learn.microsoft.com/en-us/entra/permissions-management/product-roles-permissions#enabling-permissions-management
upvoted 1 times

ELQUMS 11 months, 1 week ago
Billing administrator
upvoted 3 times

throwaway10188 11 months, 2 weeks ago
To complete this task, you must have at least Billing Administrator permissions. You can't enable Permissions Management as a user from another tenant who has signed in via B2B or via Azure Lighthouse.

Prerequisites
To enable Permissions Management in your organization:
You must be eligible for or have an active assignment to the Permissions Management Administrator role as a user in that tenant.

Therefore, I think that Permissions Management Administrator might be the best role. C.

https://learn.microsoft.com/en-us/entra/permissions-management/onboard-enable-tenant
upvoted 2 times

Question #72 *Topic 1*

You have an Azure subscription that contains a user named User1 and two resource groups named RG1 and RG2.

You need to ensure that User1 can perform the following tasks:

• View all resources.
• Restart virtual machines.
• Create virtual machines in RG1 only.
• Create storage accounts in RG1 only.

What is the minimum number of role-based access control (RBAC) role assignments required?

A. 1

B. 2

C. 3

D. 4

Suggested Answer: *B*

Community vote distribution

C (60%) B (36%) 4%

penatuna Highly Voted 10 months ago

Selected Answer: B

You need two role assignments, one for RG1 and other for RG2. If you make just one assignment for both of the Resource groups, User1 will have Virtual machine & Storage account creating rights in both resource groups. If you put the scope on Subscription or Management group that has these Resource groups, the resource groups will inherit the role assignment from higher level (parent) resource.

You can make a custom role for RG1 with permissions shown below:
*/read - View all resources
Microsoft.Compute/virtualMachines/restart/action - Restart virtual machines.
Microsoft.Compute/virtualMachines/write - Creates a new virtual machine or updates an existing virtual machine.
Microsoft.Storage/storageAccounts/write - Creates a storage account with the specified parameters or update the properties or tags or adds custom domain for the specified storage account.

For RG2 you should make custom role with these permissions:
*/read - View all resources
Microsoft.Compute/virtualMachines/restart/action - Restart virtual machines.

upvoted 6 times

khangkowng1 Most Recent 3 weeks ago

Selected Answer: C

Minimum Number of Role Assignments:
To meet these requirements, User1 needs a combination of Reader, Virtual Machine Contributor, and Storage Account Contributor roles. Since there is overlap in the roles that allow User1 to restart VMs and create VMs, we can optimize the number of role assignments.

Reader role at the subscription level.
Virtual Machine Contributor role at RG1 (to allow both VM creation and VM restart in RG1).
Storage Account Contributor role at RG1.
Conclusion:
The minimum number of role assignments required is 3.

Thus, the correct answer is: C. 3

upvoted 1 times

[Removed] 7 months, 2 weeks ago

Selected Answer: C

A. 1: Assigning a single role likely wouldn't provide all the required permissions.

B. 2: It might be possible with two roles, but achieving granular control for resource group specific actions requires more than one.

C. 3: This is the most likely scenario. We need separate role assignments for broader and specific resource group permissions.

D. 4: While possible, 3 roles should be sufficient to achieve the desired outcome.

Here's a breakdown of the minimum required RBAC role assignments:

Reader role: This grants User1 the ability to view all resources across the subscription, fulfilling the first requirement.

Contributor role for RG1: This grants User1 permission to create virtual machines and storage accounts within resource group RG1, addressing the needs for resource creation in a specific group.

Virtual Machine Contributor role: This grants User1 the ability to restart virtual machines across the subscription, fulfilling the third requirement.

upvoted 4 times

emartiy 9 months, 1 week ago

Selected Answer: B

2 RBAC roles are sufficient to perform what in case.

upvoted 3 times

Alcpt 8 months, 1 week ago

Nope.

#1 Global reader to read the entire sub,

#2 vm contributor

#3 vm contributor

#4 storage account contributor

upvoted 4 times

emartiy 9 months, 1 week ago

I got this question checked via Copilot (Microsoft's ChatGpt:)) Answer is 4 roles.

1-view all resource (RG1 and RG2)

2-restart virtual machines scoped all rescource

3-Create virtual machine (Scoped resource based Virtual Machine Contributor role for RG1) (contributor role can create VM in RG1. If this role isn't given recourse scoped, can be able create VM in RG2 and it is not wanted based on question).

4-Create storage in RG1 (Scoped resource basedStorage Account Contributor role for RG1. If this role isn't given recourse scoped, can be able create storage in RG2 and it is not wanted based on question)

upvoted 2 times

Cybersecgirl 3 months, 2 weeks ago

When I checked it via copiloy it says 3, while chatgpt says 4 roles. I am more confused now.

upvoted 1 times

mb0812 9 months, 2 weeks ago

Selected Answer: C

Answer has to be C

View all resources: READER role

Restart virtual machines (it means RG1 and RG2 machines): VM contributor role

Create VM/Storage accounts in RG1: Contributor role for RG1

upvoted 4 times

Ragdoll 10 months, 1 week ago

Selected Answer: B

2 roles are sufficient:

- Reader on the subscription level. It fulfills the 1st requirement.

- Contributor or Owner on RG1, which fulfills the 2nd requirement

- There is nothing to do with RG2 because it's empty (I assume). So, no role should be assigned.

upvoted 2 times

mb0812 9 months, 2 weeks ago

How can you assume that RG2 has no VMs in it?

Answer has to be C

View all resources: READER role

Restart virtual machines (it means RG1 and RG2 machines): VM contributor role

Create VM/Storage accounts in RG1: Contributor role for RG1

upvoted 2 times

Sozo 10 months, 3 weeks ago

Selected Answer: C

To enable User1 to perform the specified tasks in Azure, you would need at least three role-based access control (RBAC) role assignments:

Reader Role: This role allows User1 to view all resources in both resource groups, RG1 and RG2.

Virtual Machine Contributor Role: This role permits User1 to restart virtual machines. It should be assigned at the scope of both RG1 and RG2 to cover all virtual machines.

Contributor Role for RG1: This role allows User1 to create virtual machines and storage accounts, but it should be assigned specifically to RG1 only.

Therefore, the minimum number of RBAC role assignments required is 3, making option C the correct answer.

upvoted 3 times

Doinitza 10 months, 3 weeks ago

It's 2 (B), by adding custom role/s.

upvoted 3 times

enklau 2 months, 2 weeks ago

yes i think the same

upvoted 1 times

loaysalameh 11 months, 1 week ago

Selected Answer: C

3 roles

Assign User1 the "Reader" role at the subscription level to view all resources.

Assign User1 the "Virtual Machine Contributor" role at the RG1 level to restart virtual machines and create virtual machines in RG1 only.

Assign User1 the "Storage Account Contributor" role at the RG1 level to create storage accounts in RG1 only.

upvoted 4 times

SFAY 11 months, 1 week ago

Selected Answer: C

If least privilege is not a concern then you just need one role - Contributor for both R1 and R2

However, I believe we will always want least privileges and in that case you will need three RBAC roles:

Reader - to view all resources in r1 and r2 as there are other resources besides VMs and SAs in the RGs.

VM Contributor - To create & restart VMs

Storage Account Contributor - To create storage accounts

upvoted 2 times

dbz_34 11 months, 1 week ago

Selected Answer: A

technically 1 role is possible since the question doesn't require the use of the least privileges the role of contributor could suffice?

upvoted 1 times

dbz_34 11 months, 1 week ago

i'm sorry i read the question too quickly only on rg1 to create a storage account and a virtual machine

upvoted 1 times

throwaway10188 11 months, 2 weeks ago

You can TECHNICALLY provide all of it is requested with 2 roles (which the question is asking for) but if you wanted to be as strict as possible 4 roles would be the best IMO.

upvoted 2 times

klayytech 8 months, 2 weeks ago

yes correct he asked about how many RBAC assignments not about how many roles you will choose

upvoted 1 times

Question #73 *Topic 1*

You work for a company named Contoso, Ltd. that has a Microsoft Entra tenant named contoso.com.

Contoso is working on a project with the following two partner companies:

• A company named A. Datum Corporation that has a Microsoft Entra tenant named adatum.com.
• A company named Fabrikam, Inc. that has a Microsoft Entra tenant named fabrikam.com.

When you attempt to invite a new guest user from adatum.com to contoso.com, you receive an error message.

You can successfully invite a new guest user from fabnkam.com to contoso.com.

You need to be able to invite new guest users from adatum.com to contoso.com.

What should you configure?

A. Guest invite settings

B. Verifiable credentials

C. Named locations

D. Collaboration restrictions

Suggested Answer: *D*

Community vote distribution

D (100%)

⊟ **penatuna** Highly Voted 3 months, 3 weeks ago

Selected Answer: D

You can select “Allow invitations to be sent to any domain (most inclusive)” to allow guest invites to be sent to any domain.

You can also select “Allow invitations only to the specified domains (most restrictive)”, and add adatum.com to it.

OR you can check if “Deny invitations to the specified domains” is selected, and contoso.com is in there.

However, you can find all of the above in Microsoft Entra admin centre | External Identities | External collaboration settings | Collaboration restrictions.

upvoted 5 times

⊟ **penatuna** 3 months, 3 weeks ago

You can use an allowlist or a blocklist to allow or block invitations to B2B collaboration users from specific organizations. For example, if you want to block personal email address domains, you can set up a blocklist that contains domains like Gmail.com and Outlook.com. Or, if your business has a partnership with other businesses like Contoso.com, Fabrikam.com, and Litware.com, and you want to restrict invitations to only these organizations, you can add Contoso.com, Fabrikam.com, and Litware.com to your allowlist.

You can create either an allowlist or a blocklist. You can't set up both types of lists. By default, whatever domains aren't in the allowlist are on the blocklist, and vice versa.

https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure
https://learn.microsoft.com/en-us/entra/external-id/allow-deny-list

upvoted 1 times

⊟ **avdan16** Most Recent 5 months, 1 week ago

You need to add adatum.com to the list of domains on External Identities >> External Collab Settings >> Collaboration Restrictions >> Allow invitations only to the specified domains.

upvoted 4 times

⊟ **SFAY** 5 months, 1 week ago

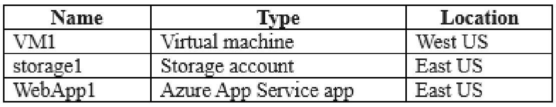
Selected Answer: D

Correct

upvoted 2 times

Question #74 *Topic 1*

You have an Azure subscription that contains a user-assigned managed identity named Managed1 in the East US Azure region. The subscription contains the resources shown in the following table.



Name	Type	Location
VM1	Virtual machine	West US
storage1	Storage account	East US
WebApp1	Azure App Service app	East US

Which resources can use Managed1 as their identity?

A. WebApp1 only

B. storage1 and WebApp1 only

C. VM1 and WebApp1 only

D. VM1, storage1, and WebApp1

Suggested Answer: *D*

Community vote distribution

C (53%) D (47%)

wheeldj Highly Voted 9 months ago

Selected Answer: D

Answer D is correct I think. see link

"In short, yes you can use user assigned managed identities in more than one Azure region. The longer answer is that while user assigned managed identities are created as regional resources the associated service principal (SP) created in Microsoft Entra ID is available globally"

https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/managed-identities-faq

upvoted 8 times

AleFerrillo 8 months ago

Storage accounts can't use Managed Identities (https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/managed-identities-status). Correct answer is C

upvoted 4 times

hml_2024 3 months, 2 weeks ago

after checking Microsoft co-pilot, it said Managed identities in Azure allow resources like virtual machines, web apps, and function apps to authenticate to other Azure services, including storage accounts, without needing to manage credentials.

upvoted 3 times

Alcpt 7 months, 1 week ago

D is correct, you can assign UAMI on all the resources under Identity.

upvoted 2 times

NICKTON81 Highly Voted 8 months, 2 weeks ago

Selected Answer: C

C is correct

https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/managed-identities-status

https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/managed-identities-faq

upvoted 6 times

Panama469 5 months, 3 weeks ago

Dude, that second link says that "In short, yes you can use user assigned managed identities in more than one Azure region"

So that means 'D' is correct.

upvoted 3 times

c3e0fc1 Most Recent 3 weeks, 3 days ago

Selected Answer: C

You cannot add a -USER-assigned managed identity to a storage account. Since you can do that to a VM, the only answer is C.

upvoted 2 times

⊟ **hml_2024** 4 months ago

This is from ChatGPT.

To determine which resources can use the Managed1 user-assigned managed identity, we need to consider that a user-assigned managed identity can only be assigned to resources in the same Azure region where it was created.

Managed1 is in the East US region, so it can only be assigned to resources that are also in the East US region.

Looking at the table:

VM1 is in the West US region, so it cannot use Managed1.
storage1 is in the East US region, so it can use Managed1.
WebApp1 is in the East US region, so it can use Managed1.

Therefore, the correct answer is:

B. storage1 and WebApp1 only.

upvoted 1 times

⊟ **Tony416** 4 months ago

Storage accounts can't use Managed Identities (https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/managed-identities-status)

The question is tricky and not about Region or Subscription but that services included in the scenario

upvoted 1 times

⊟ **jarattdavis** 5 months, 3 weeks ago

B is correct Answer: The resources that can use Managed1 are those also in the East US region. Therefore, storage1 and WebApp1 in East US can use Managed1 as their identity

upvoted 2 times

⊟ **jim85** 6 months, 2 weeks ago

D is the answer, user assigned managed identity can be used in other regions: https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/managed-identities-faq

upvoted 2 times

⊟ **NotanAdmin** 7 months, 2 weeks ago

D. VM1, storage1, and WebApp1

Copilot says: User-assigned managed identities can be used by multiple resources in Azure, and they are not restricted to a specific region. Therefore, **Managed1** can be used by **VM1**, **Storage1**, and **WebApp1** as their identity, regardless of the region they are in. The correct answer is: D. VM1, storage1, and WebApp1

upvoted 2 times

⊟ **bpaccount** 8 months, 2 weeks ago

How the hell are people supposed to get this question right in an proctored semi closed book exam, if us here, with access to Internet/Google/ChatGPT/CoPilot, can't even find the right answer :-D

upvoted 3 times

⊟ **NotanAdmin** 7 months, 2 weeks ago

Yes, Azure Storage accounts can use managed identities. Managed identities for Azure resources provide an automatically managed identity for applications and Azure resources to use when connecting to resources that support Azure Active Directory (Azure AD) authentication.

upvoted 1 times

⊟ **klayytech** 8 months, 2 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview see the video starting from M 10 storage account also can.

upvoted 4 times

⊟ **spatrick** 9 months ago

Explain how to add a user assigned managed identity:

https://microsoftlearning.github.io/Secure-storage-for-Azure-Files-and-Azure-Blob-Storage/Instructions/Labs/LAB_04_storage_web_app.html

upvoted 1 times

wheeldj 9 months ago

Answer D is correct I think. see link
"In short, yes you can use user assigned managed identities in more than one Azure region. The longer answer is that while user assigned managed identities are created as regional resources the associated service principal (SP) created in Microsoft Entra ID is available globally"
https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/managed-identities-faq

upvoted 2 times

klayytech 9 months ago

Selected Answer: C

So, the resources that can use Managed1 as their identity are:

VM1
WebApp1 (Azure App Service app)

note :
1- the Storage account dont have managed identity
2- managed identity assigned to all region
Therefore, the correct answer is B. storage1 and WebApp1 only.

upvoted 3 times

Nielll 9 months, 1 week ago

Selected Answer: C

Managed1 is a user-assigned managed identity, it can only be assigned to resources in the same region. So, Managed1 can only be assigned to resources within the East US region.
Therefore its C

upvoted 2 times

Nielll 9 months, 1 week ago

The user-assigned managed identity, Managed1, is located in the East US Azure region. Therefore, it can be used by resources that are in the same region. From the table, we know that both the storage account (storage1) and the Azure App Service app (WebApp1) are located in the East US region. The virtual machine (VM1), however, is located in the West US region.

So, the resources that can use Managed1 as their identity are:

storage1 (Storage account)
WebApp1 (Azure App Service app)
Therefore, the correct answer is B. storage1 and WebApp1 only.

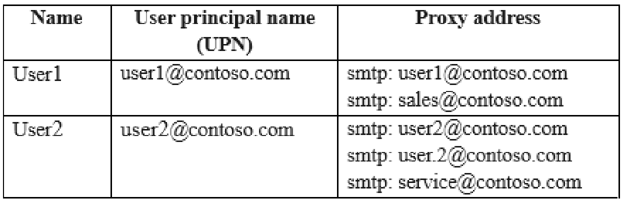
upvoted 3 times

Question #75 Topic 1

DRAG DROP

-

Your network contains an on-premises Active Directory domain named contoso.com that syncs with Microsoft Entra ID by using Microsoft Entra Connect. The domain contains the users shown in the following table.

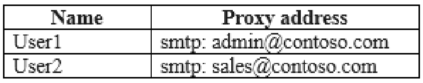


Name	User principal name (UPN)	Proxy address
User1	user1@contoso.com	smtp: user1@contoso.com smtp: sales@contoso.com
User2	user2@contoso.com	smtp: user2@contoso.com smtp: user.2@contoso.com smtp: service@contoso.com

From Active Directory Users and Computers, you add the following user:

• Name: User3
• UPN: user3@contoso.com
• Proxy addresses: smtp: user3@contoso.com, smtp: sales@contoso.com

From Active Directory Users and Computers, you update the proxyAddresses attribute for each user as shown in the following table.

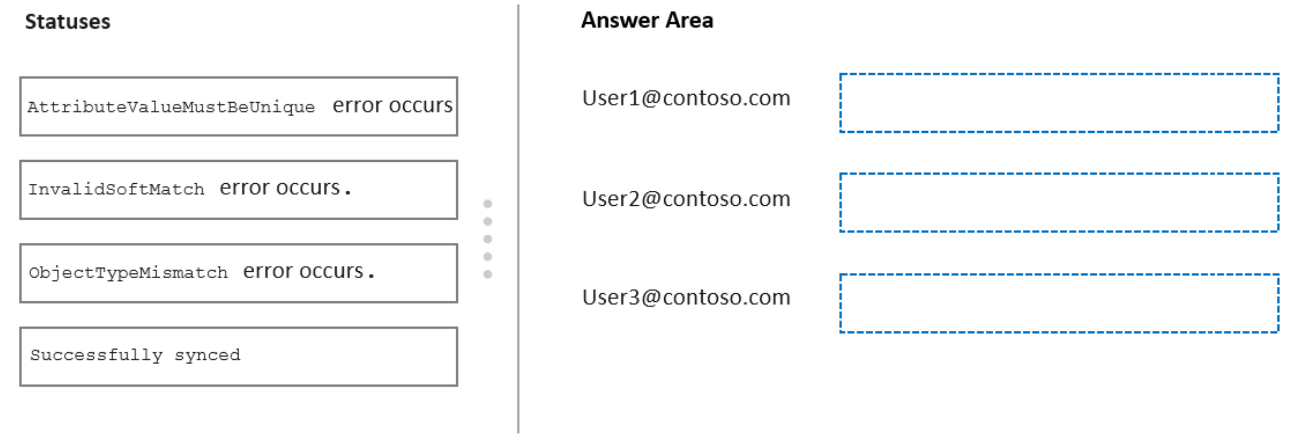


Name	Proxy address
User1	smtp: admin@contoso.com
User2	smtp: sales@contoso.com

You trigger a manual synchronization.

Which sync status will Microsoft Entra Connect sync return for each user? To answer, drag the appropriate status to the correct users. Each status 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.



Statuses

- AttributeValueMustBeUnique error occurs
- InvalidSoftMatch error occurs.
- ObjectTypeMismatch error occurs.
- Successfully synced

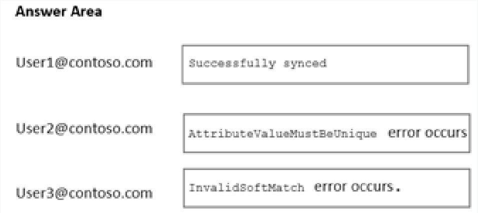
Answer Area

User1@contoso.com

User2@contoso.com

User3@contoso.com

Suggested Answer:



Answer Area

User1@contoso.com: Successfully synced

User2@contoso.com: AttributeValueMustBeUnique error occurs

User3@contoso.com: InvalidSoftMatch error occurs.

spatrick Highly Voted 9 months ago

correct:

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/tshoot-connect-sync-errors

InvalidSoftMatch error

The most common reason for the InvalidSoftMatch error is two objects with different sourceAnchor (immutableId) attributes that have the same value for the proxyAddresses or userPrincipalName attributes, which are used during the soft-match process on Microsoft Entra ID.

AttributeValueMustBeUnique error

The most common reason for the AttributeValueMustBeUnique error is that two objects with different sourceAnchor (immutableId) attributes have the same value for the proxyAddresses or userPrincipalName attributes

ObjectTypeMismatch error

The most common reason for the ObjectTypeMismatch error is that two objects of different type, like user, group, or contact, have the same value for the proxyAddresses attribute

upvoted 6 times

⊟ **Nail** 2 months, 1 week ago

Correct. I found it helpful to read through the example cases for InvalidSoftMatch and AttributeValueMustBeUnique on the page posted above. It makes it clear why User2 and User3 get different errors, i.e., it depends on whether they were already synchronized or they are a new object.

upvoted 1 times

⊟ **Nielll** Most Recent 9 months, 1 week ago

this seems to be correct. the 1st table assumes that aliases are already being synced.

upvoted 1 times

⊟ **Nielll** 9 months, 1 week ago

changed my mind

successfully synced

unique error

unique error

upvoted 2 times

⊟ **Nielll** 9 months, 1 week ago

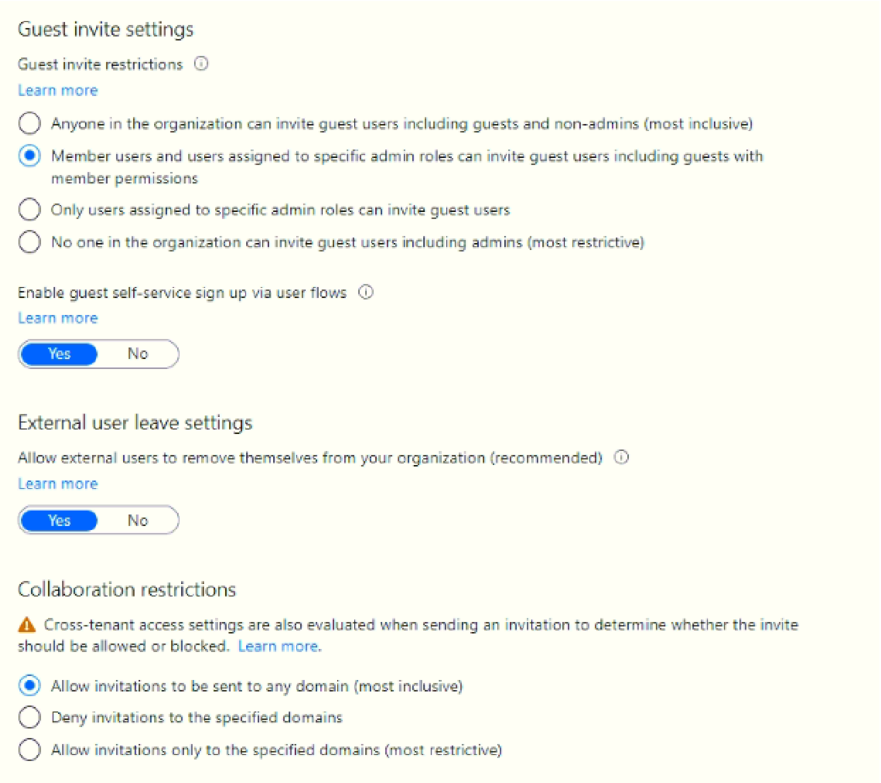
i changed my mind i again. i recreated this and verified that the given answers are corect

upvoted 4 times

Question #76 | *Topic 1*

You have a Microsoft 365 tenant that uses the domain name fabrikam.com.

The External collaboration settings are configured as shown in the Collaboration exhibit. (Click the Collaboration tab.)



Guest invite settings

Guest invite restrictions ⓘ

Learn more

○ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

● Member users and users assigned to specific admin roles can invite guest users including guests with member permissions

○ Only users assigned to specific admin roles can invite guest users

○ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

Learn more

[✓ Yes] No

External user leave settings

Allow external users to remove themselves from your organization (recommended) ⓘ

Learn more

[✓ Yes] No

Collaboration restrictions

⚠ Cross-tenant access settings are also evaluated when sending an invitation to determine whether the invite should be allowed or blocked. Learn more.

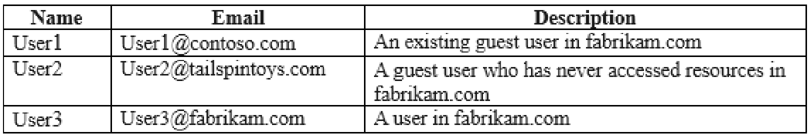
● Allow invitations to be sent to any domain (most inclusive)

○ Deny invitations to the specified domains

○ Allow invitations only to the specified domains (most restrictive)

The Email one-time passcode for guests setting is enabled for the tenant.

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	An existing guest user in fabrikam.com
User2	User2@tailspintoys.com	A guest 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. User1 only

B. User2 only

C. User1 and User2 only

D. User1, User2, and User3

Suggested Answer: *B*

Community vote distribution

B (62%) C (38%)

criminal1979 Highly Voted 9 months ago

Selected Answer: C

I say the answer is C in this case.

upvoted 6 times

Alcpt 8 months, 1 week ago

U guys need to study the material. Stop guessing

upvoted 2 times

criminal1979 5 months, 3 weeks ago

Yes, when the "Email one-time passcode for guests" setting is enabled in Azure AD, a passcode is sent via email every time a guest user needs to log in

upvoted 1 times

Nail 2 months, 1 week ago

I agree with criminal. Answer: C. If you look at the other question that was like this, User2 was an outlook.com user in that case so they should not receive the OTP because they already have a Microsoft account. The answer was User1 for the same reason as here, reauthentication will lead to OTP. If that was not correct, then NO answer was correct on that last question. So User 1 was the answer on the other question. So the answer here must be User1 for the same reason and User2 because it is not a Microsoft account this time.

upvoted 2 times

SilverFox Highly Voted 8 months, 3 weeks ago

Selected Answer: B

Repeat question.

upvoted 5 times

Matt19 Most Recent 3 weeks ago

Selected Answer: C

contoso.com and tailspintoys.com both are external domains - both should be sent a passcode - C

upvoted 1 times

Mole857 1 month ago

Selected Answer: B

Existing guest users in a tenancy will not receive the emailed one-time passcode if they have already redeemed their invitation. The email one-time passcode feature is for NEW guest users or those who haven't yet redeemed their invitation.

If you enable the email one-time passcode feature, it will only affect future redemption processes for NEW guest users. Existing guests will continue to use their current authentication method unless their redemption status is reset

upvoted 1 times

HaubeRR89 1 month ago

Selected Answer: C

Our Email OTP capability also has built-in lightweight lifecycle management. Each authentication session only lasts 24 hours, after which guests have to re-authenticate with a new email OTP.
https://techcommunity.microsoft.com/blog/identity/azure-ad-makes-sharing-and-collaboration-seamless-for-any-user-with-any-account/325949

upvoted 1 times

Matt19 3 months, 1 week ago

Selected Answer: C

C is correct.
User2 - should be asked for OTP everytime a guest user needs to login, if we enable Email one-time passcode for guests setting within: External Identities | All identity providers.

upvoted 1 times

07d6037 6 months, 4 weeks ago

Selected Answer: B

The correct answer is B

upvoted 1 times

Rucasll 7 months, 3 weeks ago

My doubt is whether the question is related to the moment the guest is logged in or is related to the next time they try to logon

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

CubicTeach 8 months ago

Selected Answer: B

I think it's "B", since user 1 is already un existing member by other meaning already received the one-time passcode

upvoted 3 times

⊟ **klayytech** 8 months, 3 weeks ago

Selected Answer: C

passcode apply only to None Microsoft Entra or Microsoft account like (outlook or MSN)

upvoted 1 times

⊟ **Alcpt** 8 months, 1 week ago

B. you will not send send ONE TIME PASSCODES a second time! Ever! Unless the guest leaves.

upvoted 2 times

⊟ **omnomsnom** 5 months, 3 weeks ago

OTP is for redemption but also re-authentication. How else would the user be authenticated when they move to a different computer, in the absence of MS or Entra account?

upvoted 1 times

Question #77 *Topic 1*

You have an Azure subscription named Sub1 that contains a virtual machine named VM1.

You need to enable Microsoft Entra login for VM1 and configure VM1 to access the resources in Sub1.

Which type of identity should you assign to VM1?

A. Microsoft Entra user account

B. user-assigned managed identity

C. Azure Automation account

D. system-assigned managed identity

Suggested Answer: *D*

Community vote distribution

D (100%)

Nielll Highly Voted 👍 3 months ago

Selected Answer: D

System-assigned managed identity: This type of managed identity is enabled directly on an Azure resource. In this case, enabling a system-assigned managed identity on VM1 would allow VM1 to authenticate with other Azure resources within Sub1, using the identity associated with VM1.

upvoted 11 times

Alcpt 2 months, 1 week ago

Correct SAMI before UAMI

upvoted 2 times

Question #78 *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 Microsoft Entra 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-WindowsProductKey cmdlet

B. the Update-MgGroup cmdlet

C. the Set-MgUserLicense cmdlet

D. the Update-MgUser cmdlet

Suggested Answer: *C*

Community vote distribution

C (100%)

Trader6 2 months, 2 weeks ago

Selected Answer: C

https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users.actions/set-mguserlicense?view=graph-powershell-1.0

upvoted 2 times

klayytech 2 months, 2 weeks ago

Selected Answer: C

C. the Set-MgUserLicense cmdlet

upvoted 2 times

dzdz 3 months ago

Selected Answer: C

C. the Set-MgUserLicense cmdlet

To remove the Office 365 Enterprise E3 licenses from the users who are now part of a group with Office 365 Enterprise E5 licenses assigned, you should use the Set-MgUserLicense cmdlet. This cmdlet allows you to modify the licenses assigned to a user. By using this cmdlet, you can remove the Office 365 Enterprise E3 licenses from all users who are part of the group where you assigned the Office 365 Enterprise E5 licenses.

upvoted 3 times

Question #79 *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 Microsoft Entra 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 Licenses blade in the Microsoft Entra admin center

B. the Administrative units blade in the Microsoft Entra admin center

C. the Identity Governance blade in the Microsoft Entra admin center

D. the Update-MgUser cmdlet

Suggested Answer: *A*

Community vote distribution

A (100%)

Trader6 2 months, 2 weeks ago

Selected Answer: A

Only possible answer

upvoted 1 times

dzdz 3 months ago

Selected Answer: A

A. the Licenses blade in the Microsoft Entra admin center

To remove the Office 365 Enterprise E3 licenses from the users who are now part of a group with Office 365 Enterprise E5 licenses assigned, you should use the "Licenses" blade in the Microsoft Entra admin center. This allows you to manage license assignments at a group level, making it easier to apply and remove licenses for multiple users simultaneously.

upvoted 2 times

Question #87

Topic 1

You have an Azure subscription that contains a storage account named storage1.

You plan to deploy an app named App1 that will be hosted on multiple virtual machines. The virtual machines will authenticate to a third-party API by using secrets.

You need to recommend an authentication solution for the virtual machines. The solution must meet the following requirements:

- Securely store secrets.
- Ensure that credentials do NOT need to be stored in the App1 code.
- Ensure that the virtual machines can access Azure resources by using Microsoft Entra authentication
- Minimize administrative effort.

What should you include in the recommendation?

A. user accounts and Storage Service Encryption

B. user-assigned managed identities and Azure Key Vault

C. user accounts and Azure Key Vault

D. system assigned managed identities and Storage Service Encryption

Suggested Answer: *B*

Community vote distribution

B (100%)

5f2afa7 4 days, 13 hours ago

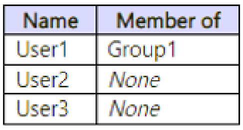
Selected Answer: B

Azure Key Vault for the 3rd party API creds, and a user assigned managed identity for the MULTIPLE VMs to access "Azure resources by using Entra authentication".

upvoted 1 times

Question #93 Topic 1

You have a Microsoft Entra tenant that contains the users shown in the following table.



Name	Member of
User1	Group1
User2	*None*
User3	*None*

You add an enterprise application named App1 and configure the following Self-service settings:

- Allow users to request access to this application: Yes
- To which group should assigned users be added: Group1
- Require approval before granting access to this application: Yes
- Who is allowed to approve access to this application: User2

Which users can request access to App1?

A. User3 only

B. User2 and User3 only

C. User1 and User3 only

D. User1, User2, and User3

Suggested Answer: *C*

Community vote distribution

D (100%)

Btn26 1 day, 8 hours ago

Selected Answer: D

Allow users to request access to this application: Yes: This setting allows any user in the tenant to request access to App1.
- **Require approval before granting access to this application: Yes**: This setting means that access requests need approval.
- **Who is allowed to approve access to this application: User2**: This setting designates User2 as the approver for access requests.

Since the setting "Allow users to request access to this application" is set to "Yes," any user in the tenant can request access to App1. This includes User1, User2, and User3.

Therefore, the correct answer is:
D. User1, User2, and User3
upvoted 1 times

Sunth65 4 days, 14 hours ago

Selected Answer: C

Approve access to this application: User2 !
upvoted 1 times

mert123 1 week, 2 days ago

Selected Answer: D

i think its D
upvoted 4 times

Question #1 *Topic 2*

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.

Suggested 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 3 years, 1 month 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 22 times

a6792d4 Most Recent 1 month, 2 weeks ago

Disabled is the appropriate status for users who are using security defaults or Conditional Access based multifactor authentication.

upvoted 1 times

ELQUMS 5 months, 1 week ago

Selected Answer: B

Correct

upvoted 1 times

kalyankrishna1 9 months, 2 weeks ago

Selected Answer: B

Correct answer

upvoted 1 times

EmnCours 11 months, 2 weeks ago

Selected Answer: B

B. Disable Security defaults

upvoted 1 times

mali1969 1 year 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 1 year ago

Selected Answer: B

B. Disable Security defaults

upvoted 1 times

ShoaibPKDXB 1 year, 1 month ago

Selected Answer: B

Correct B

upvoted 1 times

francescoc 1 year, 3 months 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 1 year, 5 months ago

Selected Answer: B

Deshabilite los valores predeterminados de seguridad.

upvoted 1 times

Oknip 1 year, 5 months ago

Selected Answer: B

Disable the security defaults to enable Conditional Access policies

upvoted 2 times

[Removed] 1 year, 6 months 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, 8 months ago

On exam- 10/28/22

upvoted 2 times

Seed001 1 year, 11 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 2 years ago

Selected Answer: B

You need to disable Security defaults to enable Conditional access policies, si the answer is correctt

upvoted 3 times

shine98 2 years ago

On the exam - June 12, 2022

upvoted 1 times

stromnessian 2 years, 4 months ago

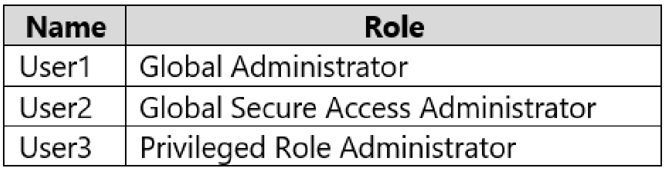
Selected Answer: B

Yes, it's B.

upvoted 1 times

Question #1 *Topic 2*

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



Name	Role
User1	Global Administrator
User2	Global Secure Access Administrator
User3	Privileged Role Administrator

You configure Microsoft Entra Internet Access.

Which users can manage Microsoft Entra Internet Access?

A. User1 only

B. User2 only

C. User3 only

D. User1 and User2 only

E. User1, User2, and User3

Suggested Answer: *A*

Community vote distribution

B (100%)

Btn26 1 day, 8 hours ago

Selected Answer: D

Global Administrator: Has full access to all administrative features in Microsoft Entra ID.

- **Global Secure Access Administrator**: This role is specifically designed to manage secure access features, including Microsoft Entra Internet Access.

- **Privileged Role Administrator**: Manages role assignments in Microsoft Entra ID but does not have specific permissions for managing secure access features.

Given these roles, the users who can manage Microsoft Entra Internet Access are:

D. User1 and User2 only

upvoted 1 times

Sunth65 4 days, 14 hours ago

Selected Answer: B

Global Secure Access Administrator Create and manage all aspects of Microsoft Entra Internet Access and Microsoft Entra Private Access, including managing access to public and private endpoints.

upvoted 1 times

Question #2 *Topic 2*

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

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

Community vote distribution

D (100%)

Ed2learn Highly Voted 3 years, 6 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 37 times

omnomsnom 5 months, 3 weeks ago
It's actually quite common for mobiles to not be allowed in some call centres that handle sensitive data or process card holder data. Exempting the network from MFA goes against zero-trust model. FIDO keys are the best solution.
upvoted 1 times

Beitran Highly Voted 3 years, 8 months ago
The only logical option.
upvoted 25 times

Nivos23 Most Recent 1 year, 2 months ago
Selected Answer: D
Correct Answer is D
upvoted 2 times

EmnCours 1 year, 5 months ago
Selected Answer: D
Correct Answer: D
upvoted 1 times

dule27 1 year, 6 months ago
Selected Answer: D
D. FIDO2 tokens
upvoted 1 times

ShoaibPKDXB 1 year, 7 months ago
Selected Answer: D
Correct D
upvoted 1 times

Aquintero 1 year, 11 months ago
Selected Answer: D
D. Fichas FIDO2
upvoted 2 times

Halwagy 1 year, 11 months ago

Selected Answer: D

The FiDO2 token

upvoted 1 times

[Removed] 2 years ago

Selected Answer: D

Ali_Pin explained correctly. FIDO2 is the correct answer.

upvoted 2 times

ali_pin 2 years, 6 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 16 times

sapien45 2 years, 6 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 2 years, 7 months ago

windows hello for business can also use a PIN instead of biometrics so both it and fido are viable but I think fido is better don't like the question as either could be user

upvoted 1 times

ZauberSRS 2 years, 1 month ago

No, Windows Hello Pin is store locally, they may change computer every day it says

upvoted 2 times

bleedinging 2 years, 7 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 2 years, 8 months ago

The call center computers are NOT configured for biometric identification

Answer- C

upvoted 1 times

PanBrown 2 years, 8 months ago

FIDO2 key is the only option in this situation.

upvoted 1 times

Yelad 2 years, 9 months ago

On the exam - March 28, 2022

upvoted 2 times

Jun143 2 years, 9 months ago

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

upvoted 1 times

Question #3 *Topic 2*

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

Suggested 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, 8 months ago
Client apps condition is the correct answer
upvoted 21 times

melatocaroca Highly Voted 👍 2 years, 5 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 14 times

> **Aquintero** 11 months, 1 week ago
> Estoy deacuerdo contigo, en este caso para mi la respuesta no esta o no es clara o esta confuza. 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 1 month, 3 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 2 times

sherifhamed 3 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 2 times

sherifhamed 3 months, 1 week 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 5 months, 3 weeks ago

On the exam, 09/07/2023

upvoted 4 times

AMZ 6 months, 1 week ago

Question valid - 06/23

upvoted 3 times

mali1969 6 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, 4 weeks ago

Selected Answer: C

C. a client apps condition

upvoted 1 times

ShoaibPKDXB 7 months, 4 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

Halwagy 11 months, 3 weeks ago

Selected Answer: C

Client App

upvoted 1 times

[Removed] 1 year ago

Selected Answer: C

Correct answer given.

upvoted 1 times

kerimnl 1 year, 2 months ago

Selected Answer: C

C. a client apps condition

upvoted 1 times

Tokiki 1 year, 6 months ago

C is correct

upvoted 1 times

shine98 1 year, 6 months ago

On the exam - June 12, 2022

upvoted 2 times

Nilz76 1 year, 8 months ago

This question was in the exam 28/April/2022

upvoted 2 times

Yelad 1 year, 9 months ago

On the exam - March 28, 2022

upvoted 1 times

Question #4 *Topic 2*

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

Suggested 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, 7 months ago
Correct - leaked credentials. Rest belongs to sign-in risk
upvoted 23 times

Nivos23 Most Recent 2 months ago
Selected Answer: D
D. leaked credentials
upvoted 1 times

sherifhamed 3 months, 1 week 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 5 months, 2 weeks ago
Selected Answer: D
Correct Answer: D
upvoted 1 times

mali1969 6 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, 4 weeks ago
Selected Answer: D
D. leaked credentials
upvoted 1 times

ShoaibPKDXB 7 months, 4 weeks ago
Selected Answer: D
correct D
upvoted 1 times

⊟ **francescoc** 9 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** 11 months, 1 week ago

Selected Answer: D

D. credenciales filtradas

upvoted 1 times

⊟ **[Removed]** 1 year ago

Selected Answer: D

Leaked credentials is the correct answer. The other options are sign-in risk.

upvoted 1 times

⊟ **BTL_Happy** 1 year, 1 month ago

this came out with different multiple choice.

upvoted 1 times

⊟ **Tokiki** 1 year, 6 months ago

D is correct

upvoted 1 times

⊟ **dangerdizzy** 1 year, 6 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, 8 months ago

Selected Answer: D

Absolutely D

upvoted 1 times

⊟ **PanBrown** 1 year, 8 months ago

Leaked Credentials is correct, consider credentials are always classified.

upvoted 1 times

⊟ **Jun143** 1 year, 9 months ago

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

upvoted 1 times

Question #5 *Topic 2*

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

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad

Community vote distribution
B (72%) C (28%)

Val_0 Highly Voted 3 years, 8 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 38 times

melatocaroca 3 years, 6 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 3 years, 5 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 the option to select as demoxyl told 2 months, 1 week ago C is the answer
upvoted 5 times

Beitran Highly Voted 3 years, 7 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 14 times

Azurefox79 3 years, 6 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 5 times

JerryGolais 3 years, 7 months ago
This is right. Link explains everything.
upvoted 2 times

jim85 Most Recent 6 months, 2 weeks ago

Selected Answer: C

C - https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices

1) you select what apps (as answer C says)

2) select Conditions > Filter devices

upvoted 1 times

RemmyT 7 months ago

Selected Answer: B

Answer: B

Target resources
Cloud apps -> Select apps
Office 365 SharePoint Online

Session
Use Conditional Access App Control
Block downloads (Preview)

Grant access
Require Microsoft Entra hybrid joined device

upvoted 2 times

Siraf 1 year ago

Correct Answer is B:

Within a Conditional Access policy, an administrator can make use of session controls to enable limited experiences within specific cloud applications. Organizations can use this control to require Microsoft Entra ID to pass device information to the selected cloud apps. The device information allows cloud apps to know if a connection is from a compliant or domain-joined device and update the session experience. This control only supports Office 365, SharePoint Online, and Exchange Online as selected cloud apps. When selected, the cloud app uses the device information to provide users with a limited or full experience. Limited when the device isn't managed or compliant and full when the device is managed and compliant.

https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-session

upvoted 1 times

haazybanj 1 year, 1 month 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 year, 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 1 year, 3 months 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 1 year, 4 months ago

Selected Answer: B

Correct Answer is: B

upvoted 2 times

⊟ **sehlohomoletsane** 1 year, 4 months ago

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions

upvoted 1 times

⊟ **hellawaits111** 1 year, 5 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** 1 year, 6 months ago

Selected Answer: C

Correction

C. an Azure AD conditional access policy that has client apps conditions configured

upvoted 1 times

⊟ **mali1969** 1 year, 6 months 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

⊟ **mali1969** 1 year, 4 months ago

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** 1 year, 6 months ago

C is the answer: https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad

upvoted 1 times

⊟ **dule27** 1 year, 6 months ago

Selected Answer: B

B. an Azure AD conditional access policy that has session controls configured

upvoted 1 times

⊟ **ShoaibPKDXB** 1 year, 7 months ago

Selected Answer: B

B correct

upvoted 1 times

⊟ **jojoseph** 1 year, 11 months ago

Selected Answer: B

B or C could be right. But I am inclined to B

upvoted 1 times

⊟ **Holii** 1 year, 6 months 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

Question #6 *Topic 2*

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

Suggested 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, 1 month 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 156 times

NickHSO 1 year, 11 months ago

Upvote for additional knowledge! thank you

upvoted 11 times

Official_Fridaws Highly Voted 👍 2 years, 1 month ago

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension

upvoted 5 times

haazybanj Most Recent ⏲ 1 month, 3 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 2 times

EmnCours 5 months, 2 weeks ago

Selected Answer: C

Correct Answer: C

upvoted 1 times

mali1969 6 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, 4 weeks ago

Selected Answer: C

C. Network Policy Server (NPS)

upvoted 1 times

ShoaibPKDXB 7 months, 4 weeks ago

Selected Answer: C

Correct C

upvoted 1 times

[Removed] 1 year ago

Selected Answer: C

C is correct.

upvoted 1 times

Zubairr13 1 year, 5 months ago

On the exam, 7/23/2022.

upvoted 2 times

Tokiki 1 year, 6 months ago

Yes, NPS is needed

upvoted 1 times

shine98 1 year, 6 months ago

On the exam - June 12, 2022

upvoted 1 times

Yelad 1 year, 9 months ago

On the exam - March 28, 2022

upvoted 1 times

Jun143 1 year, 9 months ago

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

upvoted 1 times

Pravda 1 year, 11 months ago

Selected Answer: C

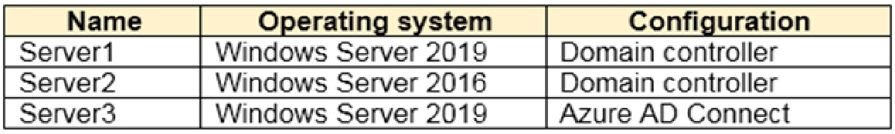
On the exam 1/20/2022

upvoted 2 times

Question #7 Topic 2

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

Suggested Answer: *D*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy

Community vote distribution

D (91%) 9%

⊟ **jhap** Highly Voted 2 years, 8 months 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 36 times

⊟ **Kronos** Most Recent 5 months ago

There is only one server functioning as the AZ AD Connect which is Server 3. What if Server 3 goes down? This is a single point of failure which I think should Server 4 be configured to be doing. So I would have A as an answer.

upvoted 3 times

⊟ **curtmcgirt** 6 months, 4 weeks ago

if Azure AD Password Protection requires an azure ad password protection proxy service server, and we only install that proxy service on server4, won't we still have a problem "if a single server fails" and that single server is named 'server4'?

from the linked article:

"You need network connectivity between at least one DC in each domain of the forest and one password protection proxy server." (so it breaks if single server4 goes down?)

"We recommend at least two Microsoft Entra Password Protection proxy servers per forest for redundancy, " (we only have one, server4, right?)

am i missing the part of the question that says we already have a proxy service installed on a second server?

upvoted 2 times

⊟ **NotanAdmin** 1 month, 2 weeks ago

As usual, the correct answer isn't necessarily the best answer as a long term solution.

upvoted 1 times

⊟ **EmnCours** 11 months, 2 weeks ago

Selected Answer: D

Correct Answer: D

upvoted 2 times

EmnCours 10 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 1 year 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 1 year ago

Selected Answer: D

D. the Azure AD Password Protection proxy service

upvoted 1 times

ShoaibPKDXB 1 year, 1 month ago

Selected Answer: D

D correct

upvoted 1 times

Marian2023 1 year, 4 months 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 1 year, 5 months ago

Selected Answer: D

D. el servicio de proxy de protección con contraseña de Azure AD

upvoted 2 times

[Removed] 1 year, 6 months ago

Selected Answer: D

The answer given is a correct answer. Azure AD Password Protection proxy service.

upvoted 2 times

den5_pepito83 1 year, 7 months ago

ON EXAM 14/11/2022

upvoted 3 times

SangSang 1 year, 7 months ago

which one do you choose in your exam?

upvoted 1 times

Imee 1 year, 9 months ago

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

upvoted 1 times

Zubairr13 1 year, 11 months ago

On the exam, 7/23/2022.

upvoted 1 times

rachee 1 year, 12 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 availble. 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, 12 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** 2 years 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** 2 years ago

On the exam - June 12, 2022

upvoted 1 times

⊟ **Nilz76** 2 years, 2 months ago

This question was in the exam 28/April/2022

upvoted 1 times

Question #8 *Topic 2*

DRAG DROP -

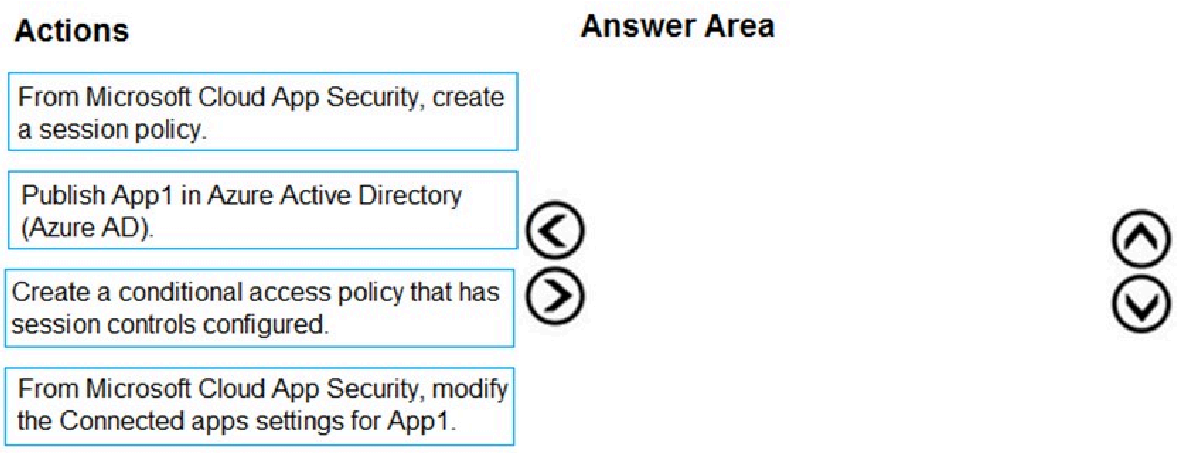
You have a Microsoft 365 E5 tenant.

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:

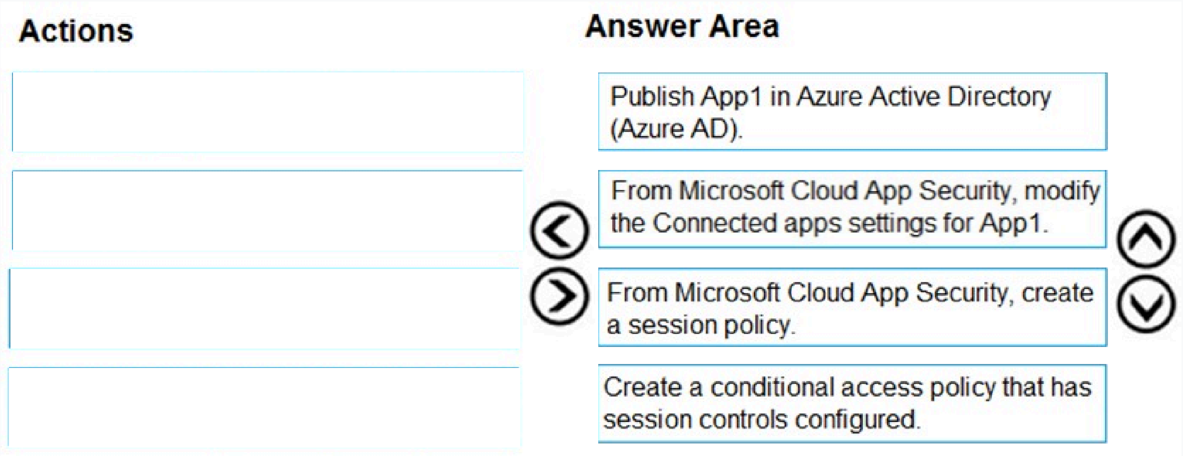


Actions

- 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.

Answer Area

Suggested 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 3 years, 6 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 92 times

Ed2learn 3 years, 6 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 2 times

w00t 2 years, 3 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 5 times

⊟ **NawafAli** 2 years, 11 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

⊟ **jack987** 2 years 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 3 times

⊟ **Xyz_40** 2 years, 7 months ago

Correct... perfect

upvoted 2 times

⊟ **Ed2learn** Highly Voted 3 years, 6 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 33 times

⊟ **melatocaroca** 3 years, 6 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** 2 years, 7 months ago

Nop, the last two should be interchanged.

upvoted 3 times

⊟ **Bloembar** 3 years, 5 months ago

Correct tested it on a lab envoriment

upvoted 4 times

⊟ **w00t** 2 years, 3 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 it's Connected Apps settings changed (Enable Session Controlled policy checkbox needs to be checked - this is not done by default)

upvoted 2 times

⊟ **EmnCours** Most Recent 1 year, 4 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 4 times

⊟ **Heshan** 1 year, 5 months ago

On the exam, 09/07/2023

upvoted 2 times

⊟ **dule27** 1 year, 6 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** 1 year, 6 months ago

Question valid - 06/23

upvoted 2 times

⊟ **eleazarrd** 1 year, 8 months 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** 1 year, 10 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 4 times

⊟ **hml_2024** 4 months ago

This is also from ChatGPT.
the correct order is:

Publish App1 in Azure Active Directory (Azure AD)
From Microsoft Cloud App Security, modify the Connected apps settings for App1
Create a conditional access policy that has session controls configured
From Microsoft Cloud App Security, create a session policy

upvoted 1 times

⊟ **Arjanussie** 1 year, 10 months ago

I agree with Jason
https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-deployment-aad

upvoted 1 times

⊟ **[Removed]** 2 years 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** 2 years, 3 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** 2 years, 3 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** 2 years, 3 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** 2 years, 5 months ago

On the exam, 7/23/2022.

upvoted 2 times

⊟ **shine98** 2 years, 6 months ago

On the exam - June 12, 2022

upvoted 1 times

⊟ **RandomNickname** 2 years, 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 it's 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 3 times

⊟ **Nilz76** 2 years, 8 months ago

This question was in the exam 28/April/2022

upvoted 1 times

Question #9 *Topic 2*

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

Suggested 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 2 years, 4 months ago

Selected Answer: C

If you think it's anything other than C, maybe you need to consider a career change.

upvoted 24 times

DiscGolfer 1 year, 4 months 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 3 times

ServerBrain 10 months, 1 week ago

yeah, it's never too late..

upvoted 2 times

Justin0020 2 months, 3 weeks ago

I think its A ;)

Just kidding

upvoted 1 times

Melwin86 Highly Voted 2 years, 7 months ago

Answer C in correct. Why everyone thinking that answer A is correct ?

upvoted 7 times

Alcpt Most Recent 2 months, 1 week ago

You need a career change. The answer is A. Authenticator did not need wifi or cell coverage to work.

upvoted 1 times

sherifhamed 9 months, 2 weeks 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 10 months, 3 weeks ago

Selected Answer: C

C. Windows Hello for Business

upvoted 1 times

DasChi_cken 11 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 biometics sensor you can use a PIN

upvoted 1 times

dule27 1 year ago

Selected Answer: C

C. Windows Hello for Business

upvoted 1 times

ShoaibPKDXB 1 year, 1 month ago

Selected Answer: C

C correct

upvoted 1 times

SusanGlenn5 1 year, 3 months ago

I think it's A

upvoted 1 times

ra1paul 1 year, 4 months ago

Definitely C.

upvoted 1 times

Cepheid 1 year, 6 months 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 1 year, 6 months ago

I think it's A though

upvoted 1 times

Rearalfonsina 1 year, 11 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** 2 years 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 7 times

⊟ **Rameshbetha** 2 years ago

have in exam on June 21 2022.

upvoted 1 times

⊟ **Benkyoujin** 2 years, 1 month ago

Selected Answer: C

C - hello for business. A mentions sending a notification vs. totp code. Hello for business is accceptable 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** 2 years, 3 months ago

On the exam - March 28, 2022

upvoted 1 times

Question #10 *Topic 2*

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

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

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

Suggested 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, 1 month 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 5 times

⊟ **syougun200x** Most Recent ⏱ 2 months, 3 weeks ago

To enable the alert function.

Azure Entre -> security -> MFA -> Fraud Alert

upvoted 1 times

⊟ **EmnCours** 4 months, 3 weeks ago

Selected Answer: B

You need to configure the fraud alert settings.

upvoted 2 times

⊟ **mali1969** 6 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, 4 weeks ago

Selected Answer: B

B. No is the answer

upvoted 1 times

⊟ **ShoaibPKDXB** 7 months, 4 weeks ago

Selected Answer: B

Correct B. NO

upvoted 1 times

⊟ **Aquintero** 11 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, 5 months ago

On the exam, 7/23/2022.

upvoted 1 times

⊟ **DemekeAd** 1 year, 8 months ago

No.

to block user

Browse to Azure Active Directory > Security > MFA > Block/unblock users.

upvoted 2 times

⊟ **Yelad** 1 year, 9 months ago

On the exam - March 28, 2022

upvoted 1 times

⊟ **Jun143** 1 year, 9 months ago

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

upvoted 1 times

⊟ **zmlapq99** 1 year, 11 months ago

On exam few days ago.

upvoted 1 times

⊟ **Pravda** 1 year, 11 months ago

On the exam 1/20/2022

upvoted 1 times

⊟ **Iamjudeicon** 2 years ago

Indeed No

upvoted 1 times

Question #11 *Topic 2*

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

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

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

Suggested 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 4 months, 3 weeks ago

Selected Answer: B

B. No is the correct answer

upvoted 1 times

dule27 6 months, 4 weeks ago

Selected Answer: B

B. No is the correct answer

upvoted 1 times

jack987 1 year 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] 1 year ago

Selected Answer: B

Fraud Settings need to be configured, meaning this solution does not meet the goal.

upvoted 2 times

Zubairr13 1 year, 5 months ago

On the exam, 7/23/2022.

upvoted 1 times

tqtuan1512 1 year, 7 months ago

I think it should be B

upvoted 1 times

mzsf3c 1 year, 8 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, 7 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, 9 months ago

On the exam - March 28, 2022

upvoted 1 times

TonytheTiger 1 year, 10 months ago

On the exam today - March 4, 2022

upvoted 1 times

zmlapq99 1 year, 11 months ago

On exam few days ago.

upvoted 1 times

Pravda 1 year, 11 months ago

On the exam 1/20/2022

upvoted 1 times

KB10 2 years, 1 month 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, 2 months ago

Should Be A

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

upvoted 1 times

Question #12 *Topic 2*

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

Suggested 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%)

⊟ **M0RK2000** Highly Voted 3 years, 1 month ago
go to MFA>settings>Fraud Alert>allow>autoblock>on>save
upvoted 11 times

⊟ **Panama469** 5 months, 3 weeks ago
Correct.

Also requires going to Authentication Methods...Settings... Report suspicious activity. It's Microsoft managed by default but to be sure you would want that set to enabled.
upvoted 1 times

⊟ **6c769e7** Most Recent 10 months ago
A is the correct answer, I was able to connect with the authenticator app without wifi
upvoted 2 times

⊟ **EmnCours** 1 year, 5 months 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** 1 year, 5 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** 1 year, 6 months ago
Selected Answer: B

B. No is the correct answer

upvoted 1 times

[Removed] 2 years ago

Selected Answer: B

Fraud Settings need to be configured, meaning this solution does not meet the goal.

upvoted 1 times

shoutiv 2 years 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

Joshuauu 2 years, 1 month ago

Is the given answer correct or incorrect? I would think the answer is A

upvoted 1 times

Zubairr13 2 years, 5 months ago

On the exam, 7/23/2022.

upvoted 1 times

Yelad 2 years, 9 months ago

On the exam - March 28, 2022

upvoted 1 times

TonytheTiger 2 years, 10 months ago

On the exam today - March 4, 2022

upvoted 1 times

zmlapq99 2 years, 11 months ago

On exam few days ago.

upvoted 2 times

Pravda 2 years, 11 months ago

On the exam 1/20/2022

upvoted 1 times

KB10 3 years, 1 month ago

Should be Yes refferenced 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** 3 years, 1 month ago
>
> Sorry my fault, answer is right
>
> upvoted 2 times

Question #13 Topic 2

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.

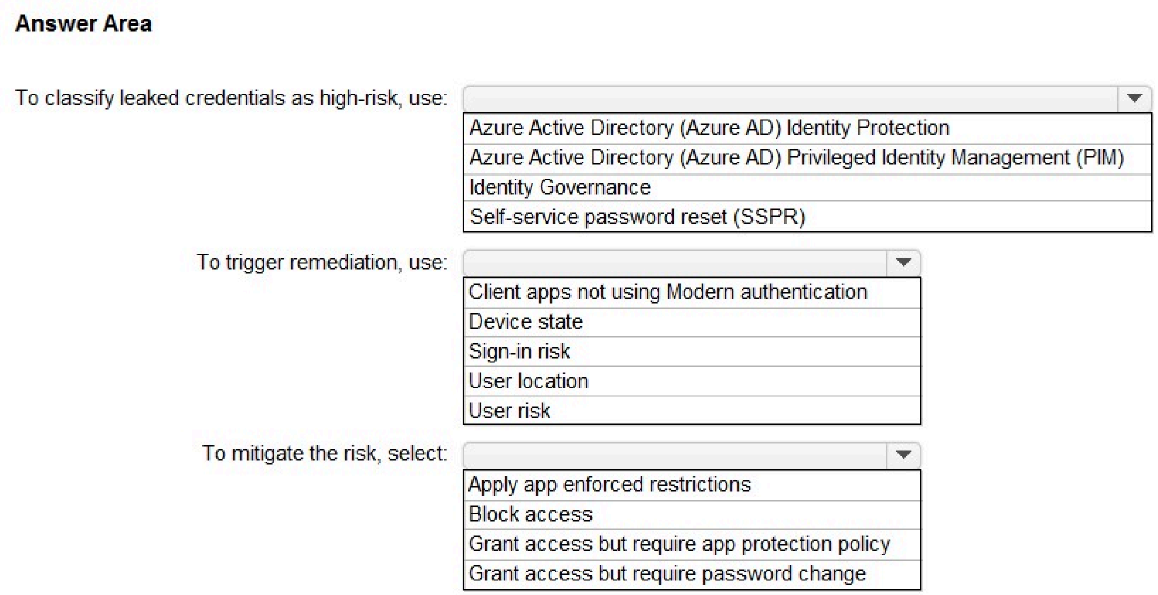
✑ Flag the sign-ins as a high-risk event.

✑ 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)

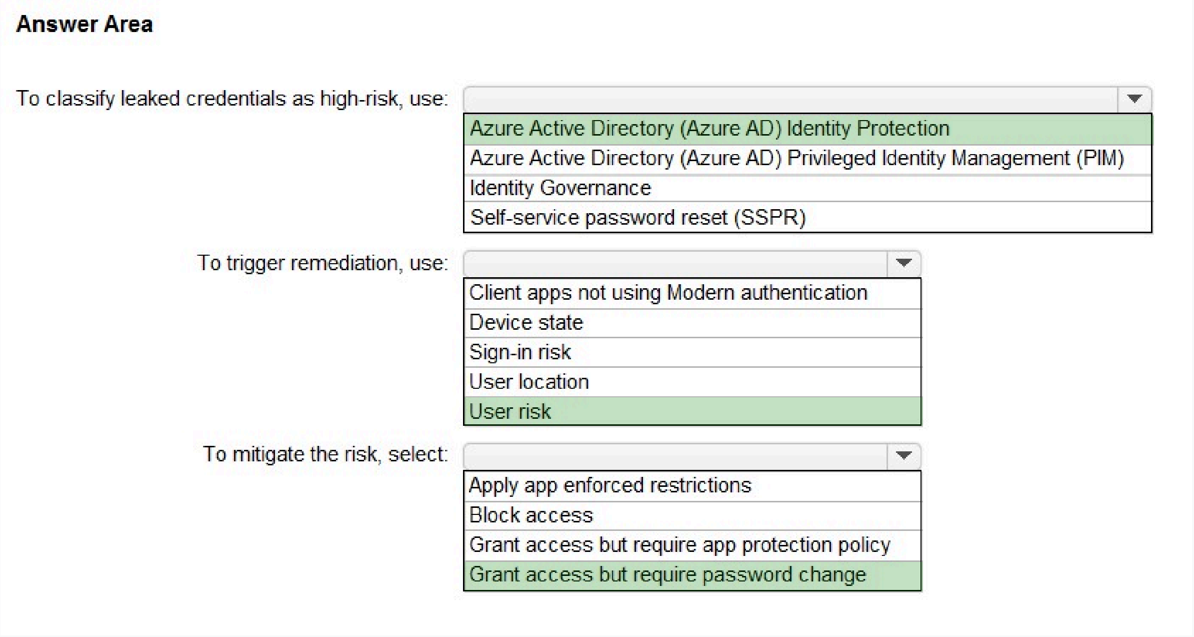
To trigger remediation, use:

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

Suggested 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 Highly Voted 3 years, 4 months ago

It's correct

upvoted 14 times

⊟ BaderJ Highly Voted 3 years, 3 months ago

Passed the exam today 23/09/2021

This question came in the exam.

upvoted 7 times

Ademola_12 Most Recent 10 months, 2 weeks ago

I'm just about to take this exam soon .

upvoted 3 times

Tuvshinjargal 10 months, 3 weeks ago

The correct answers are following.

Azure AD Identity Protection

Sign-in Risk (In the Sign-in Risk section, there is the possibility to flag the sign-in as high risk)

Block Access (There are 2 ways to enforce control 1. Block Access 2. Allow access [optionally require password change], there is no option to "GRANT" access)

upvoted 2 times

> **Tony416** 4 months ago
>
> Nope. See this link: https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-policies#user-risk-based-conditional-access-policy
>
> upvoted 1 times

EmnCours 1 year, 5 months ago

It's correct

upvoted 1 times

Heshan 1 year, 5 months ago

On the exam, 09/07/2023

upvoted 5 times

dule27 1 year, 6 months ago

Azure AD Identity protection

User risk

Grant access but require password change

upvoted 2 times

chrisp1992 2 years ago

Answer is correct.

upvoted 1 times

Zubairr13 2 years, 5 months ago

On the exam, 7/23/2022.

upvoted 4 times

rachee 2 years, 6 months ago

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

upvoted 2 times

Xyz_40 2 years, 7 months ago

correct.

upvoted 2 times

Jun143 2 years, 9 months ago

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

upvoted 2 times

Bluediamond 2 years, 10 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 6 times

> **Bluediamond** 2 years, 10 months ago
>
> NVM. It is right...read it wrong
>
> upvoted 3 times

Pravda 2 years, 11 months ago

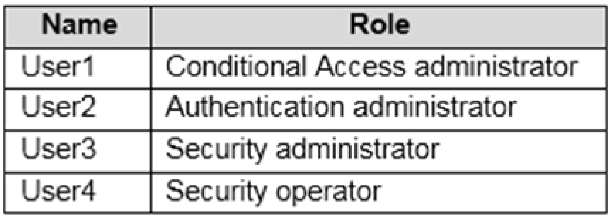
On the exam 1/20/2022

upvoted 2 times

Question #14 *Topic 2*

HOTSPOT -

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



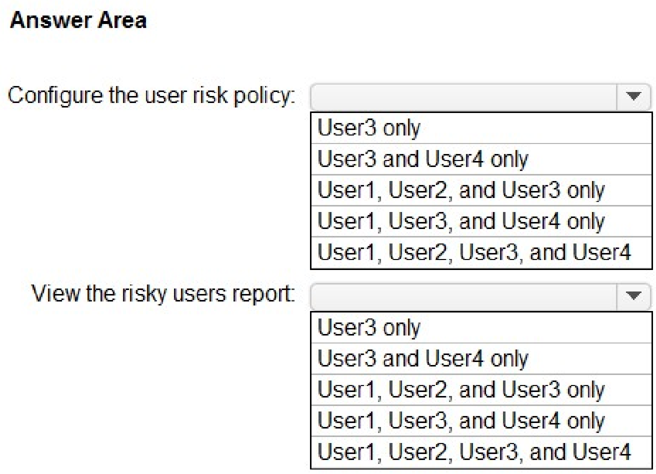
Name	Role
User1	Conditional Access administrator
User2	Authentication administrator
User3	Security administrator
User4	Security operator

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:

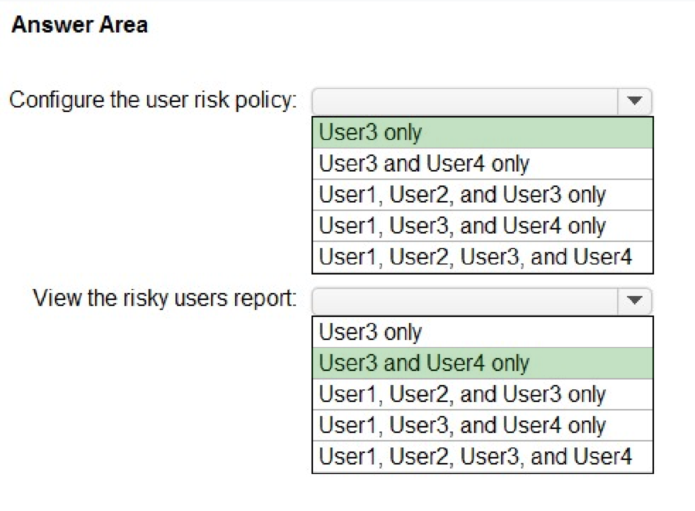


Answer Area

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

Suggested Answer:



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

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

oberte007 Highly Voted 2 years, 4 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 58 times

JCkD4Ni3L 2 months, 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 7 times

jack987 1 year ago

I agree with oberte007.

upvoted 1 times

DaBummer 2 years, 3 months ago

Currently, the Security Operator role cannot access the Risky sign-ins report.

https://docs.microsoft.com/en-us/learn/modules/manage-azure-active-directory-identity-protection/2-review-identity-protection-basics

upvoted 5 times

Dipronil 2 years, 1 month ago

Risky sign in report, but in the question it is saying as Risky users report. So User 3 and $ both can view this report

upvoted 4 times

Anju18 2 years, 4 months ago

agree your point

upvoted 2 times

007Ali Highly Voted 1 year, 11 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 = 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 = Create and delete all resources, and read and update standard properties in Azure AD Identity Protection

- Grants access to Risky Users Report

upvoted 37 times

dule27 Most Recent 6 months, 4 weeks ago

Configure the user risk policy: User 3 only

View the risky users report: User 3 and User 4 only

upvoted 3 times

LeTrinh 10 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 11 months, 1 week ago

configurar la politica solo el Usuario 3 y luego 3 y 4.

upvoted 2 times

[Removed] 1 year ago

Oberte is correct User 3 and then 3 and 4.

upvoted 2 times

Zubairr13 1 year, 5 months ago

On the exam, 7/23/2022.
upvoted 3 times

Silent_Muzinde 1 year, 9 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, 9 months ago

just pass the exam today. This came in the question.
upvoted 1 times

stromnessian 1 year, 10 months ago

Tested to confirm:
Configure: User 3 only
Read report: Users 3 and 4
upvoted 6 times

TonytheTiger 1 year, 10 months ago

On the exam today - March 4, 2022
upvoted 2 times

GPerez73 1 year, 10 months ago

First box: User3 // Second box: User3 and User4
Tested!
upvoted 4 times

KennethYY 1 year, 11 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, 11 months ago

On the exam 1/20/2022
upvoted 1 times

NawafAli 1 year, 12 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 2 years 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 3 times

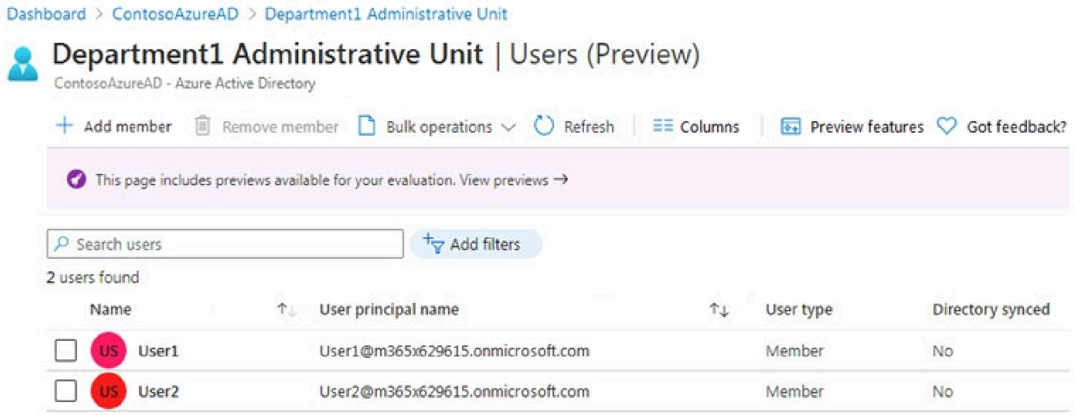
Javed8008 2 years, 1 month ago

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.

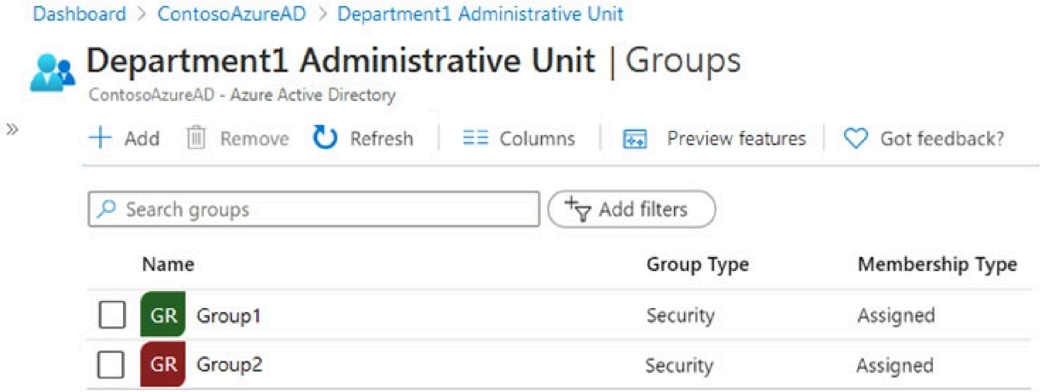
Department1 has the users shown in the Users exhibit. (Click the Users tab.)


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

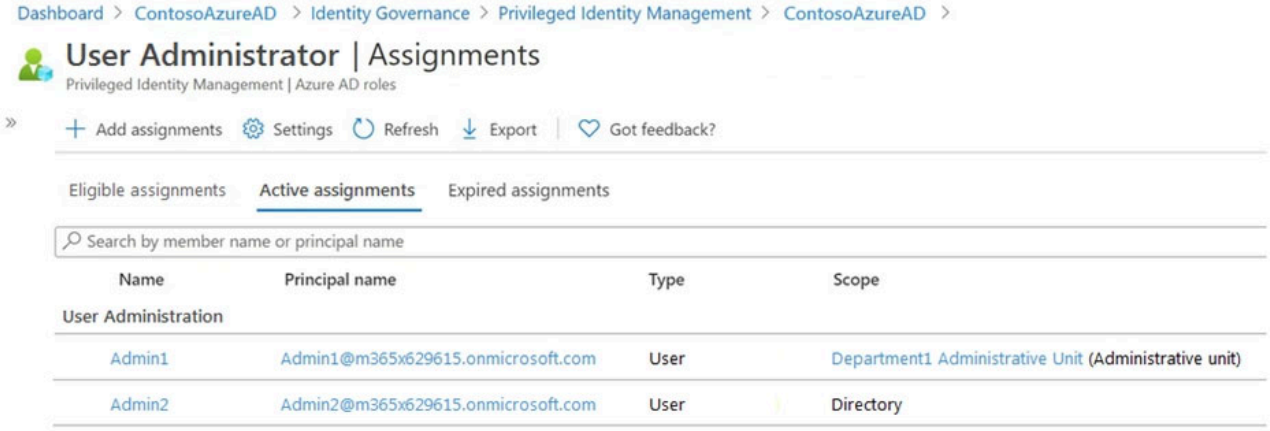
Name	User principal name	User type	Directory synced
US User1	User1@m365x629615.onmicrosoft.com	Member	No
US User2	User2@m365x629615.onmicrosoft.com	Member	No

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

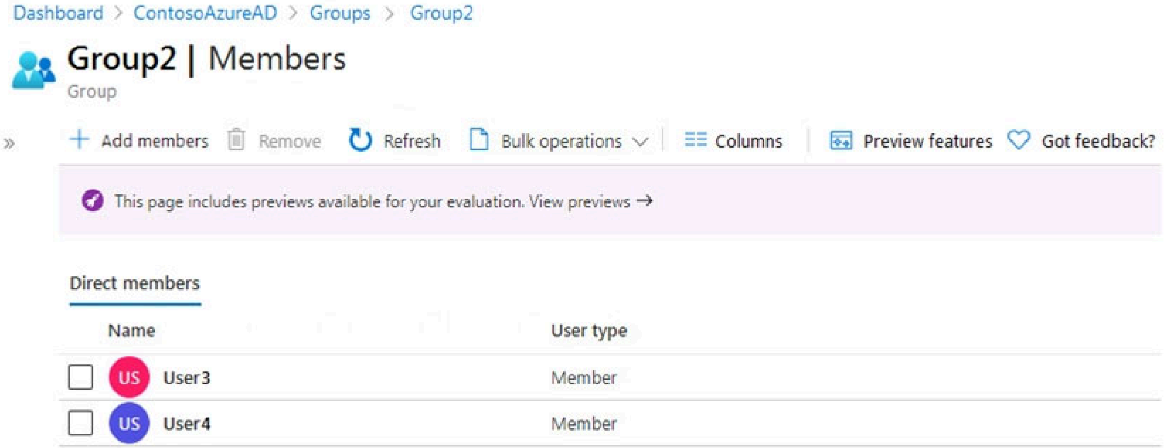
Name	Group Type	Membership Type
GR Group1	Security	Assigned
GR Group2	Security	Assigned

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.)

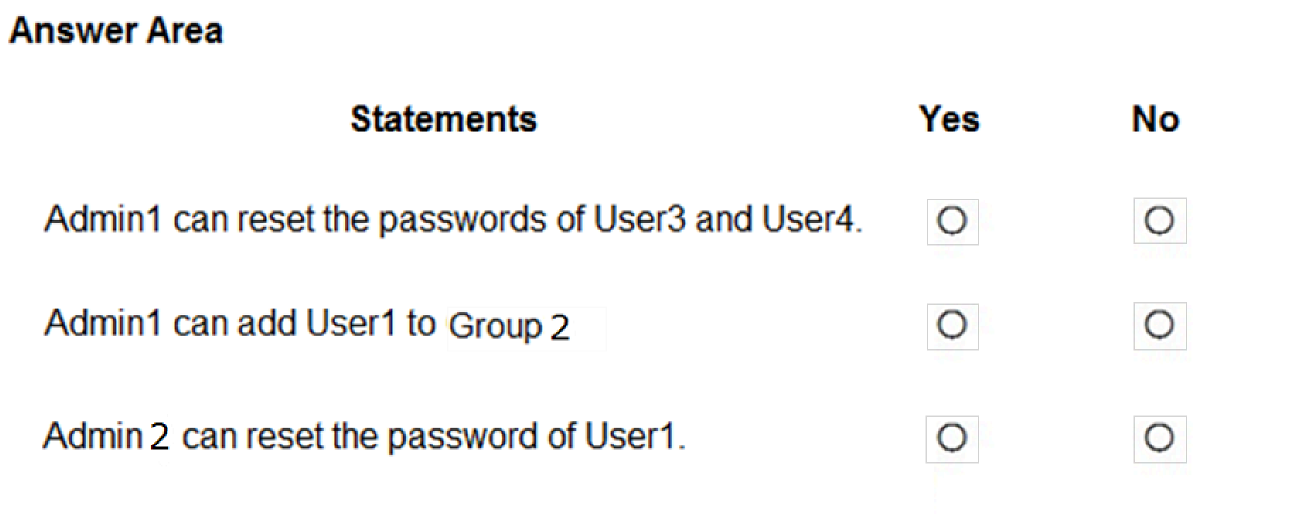

Dashboard > ContosoAzureAD > Groups > Group2
Group2 | Members
Group
+ Add members
Remove
Refresh
Bulk operations
Columns
Preview features
Got feedback?
This page includes previews available for your evaluation. View previews →
Direct members

Name	User type
US User3	Member
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.

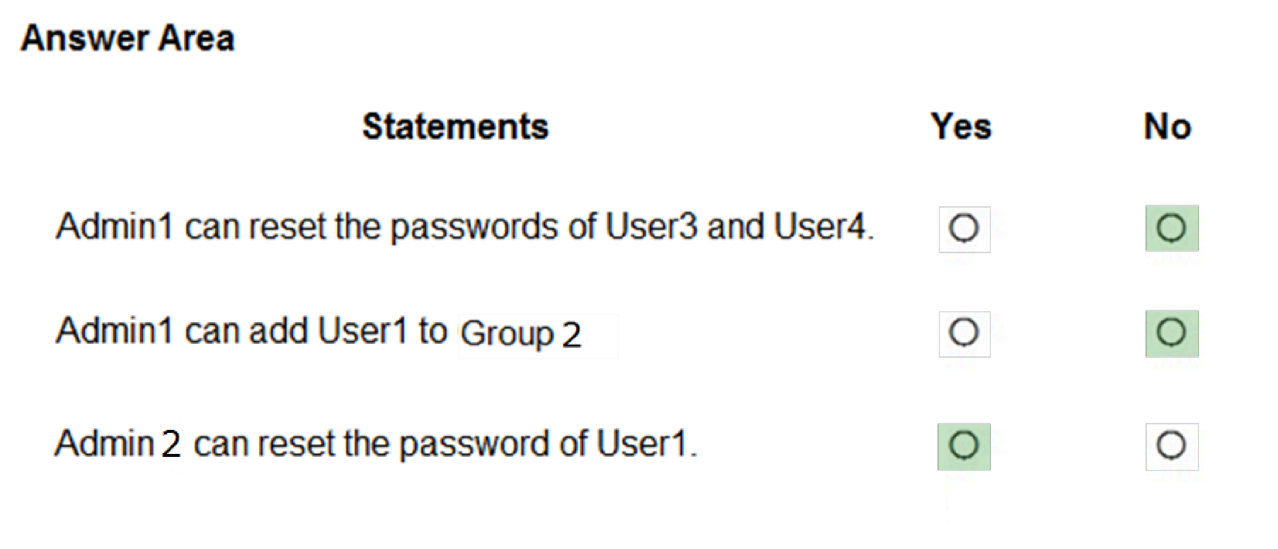
Hot Area:



Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group 2	○	○
Admin 2 can reset the password of User1.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	[✓ ○]
Admin1 can add User1 to Group 2	○	[✓ ○]
Admin 2 can reset the password of User1.	[✓ ○]	○

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units

⊟ **Beitran** Highly Voted 3 years, 8 months ago

So the correct answer is No, Yes, Yes

upvoted 110 times

⊟ **NawafAli** 2 years, 12 months ago

Correct answer, tested in lab.

upvoted 2 times

⊟ **xDinoKoalax** 2 years, 10 months ago

Tested in lab on Mar.06, 2022, the answer is NO, YES, YES

upvoted 8 times

⊟ **GlenRMag16** 2 years, 11 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

⊟ **tatendazw** 3 years, 2 months ago

correct, user admin can manage users and groups

https://docs.microsoft.com/en-us/azure/active-directory/roles/admin-units-assign-roles#available-roles

upvoted 2 times

⊟ **googie_egg** Highly Voted 3 years, 4 months ago

Tested in my own lab. No, Yes, Yes is correct.

upvoted 13 times

javifedz Most Recent 10 months ago

Agree. Correct answer is No, Yes, Yes

upvoted 1 times

Nivos23 1 year, 2 months ago

the correct answer is No, Yes, Yes

upvoted 2 times

Nyamnyam 1 year, 1 month ago

NO, YES, YES!

Why don't the Examtopics contributors ever update the info?

upvoted 3 times

calom52 1 month, 1 week ago

Because its based in Hong Kong

upvoted 1 times

joe9527 1 year, 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 year, 2 months ago

nvm. I'm making a fool of myself lol.

upvoted 2 times

joe9527 1 year, 2 months 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

EmnCours 1 year, 5 months ago

The correct answer is No, Yes, Yes.

https://learn.microsoft.com/en-gb/azure/active-directory/roles/administrative-units

upvoted 2 times

Heshan 1 year, 5 months ago

On the exam, 09/07/2023

upvoted 2 times

Sango 1 year, 6 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 1 year, 6 months ago

Question valid - 06/23

upvoted 2 times

dule27 1 year, 6 months ago

NO
YES
YES

upvoted 1 times

HelloItsSam 1 year, 10 months 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 1 year, 11 months ago

Para mi la respuesta es No, No, Si; Admin1 es administrador de de la unidad administrativa Deparment1, entonces el Grupo2 y el usuario1 pertenecen a la unidad administrativa de donde pertenece el administrador de AU Deparment1. 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** 1 year, 11 months ago

the correct answer is No, Yes, Yes

https://learn.microsoft.com/en-us/azure/active-directory/roles/administrative-units

upvoted 1 times

⊟ **Jhill777** 2 years, 1 month ago

No, Yes, Yes. Confirmed in lab.

upvoted 2 times

⊟ **Jhill777** 2 years, 1 month 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** 2 years, 3 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** 2 years, 3 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 provide 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** 2 years, 3 months ago

I wish I could delete messages... lol This is N, Y, Y...

upvoted 6 times

⊟ **[Removed]** 1 year, 8 months ago

Respect coming back 2 weeks later to fix your response

upvoted 7 times

⊟ **Ceuse** 2 years, 5 months ago

Q2 : In the Exam there was a group 3 outside of the Administrativ Unit, which Admin1 wanted to add User 1 into

upvoted 1 times

⊟ **Jhill777** 2 years, 1 month ago

Reproduced this in case it comes up. Add members is greyed out.

upvoted 1 times

Question #16 *Topic 2*

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

Suggested 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 👍 2 years ago
Correct Answer A
upvoted 5 times

EmnCours Most Recent 5 months, 2 weeks ago
Selected Answer: A
Report suspicious activity, the updated MFA Fraud Alert feature
upvoted 2 times

dule27 6 months, 4 weeks ago
Selected Answer: A
A. Yes is the correct answer
upvoted 1 times

Jhill777 1 year, 1 month ago
Selected Answer: A
Correct answer is A.
upvoted 1 times

samir45 1 year, 3 months ago
Selected Answer: A
Correct answer.
upvoted 1 times

Zubairr13 1 year, 5 months ago
On the exam, 7/23/2022.
upvoted 1 times

mzsf3c 1 year, 8 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

⊟ **Benkyoujin** 1 year, 7 months ago

You're wrong, just check in the portal.

upvoted 3 times

⊟ **Davidf** 1 year, 8 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

⊟ **Yelad** 1 year, 9 months ago

On the exam - March 28, 2022

upvoted 2 times

⊟ **Dineshshri** 1 year, 10 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

⊟ **TonytheTiger** 1 year, 10 months ago

On the exam today - March 4, 2022

upvoted 1 times

⊟ **zmlapq99** 1 year, 11 months ago

On exam few days ago.

upvoted 1 times

⊟ **Pravda** 1 year, 11 months ago

On the exam 1/20/2022

upvoted 1 times

Question #17 *Topic 2*

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

Suggested 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 2 years, 8 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 8 times

⊟ **DiscGolfer** 1 year, 10 months 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 2 years, 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 1 year, 4 months ago

Selected Answer: D

6 digit verification code is useable offline
upvoted 3 times

⊟ **stev_au** 1 year, 5 months 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

Nail 2 months, 1 week ago

"While working from the remote locations, the users connect their laptop to a wired network that has internet access." The users have internet access but only from their laptops. The reason why B and C are not correct is because they are not valid MFA verification options.

upvoted 1 times

EmnCours 1 year, 5 months ago

Selected Answer: D

D. a verification code from the Microsoft Authenticator app

upvoted 1 times

dule27 1 year, 6 months ago

Selected Answer: D

D. a verification code from the Microsoft Authenticator app

upvoted 1 times

ShoaibPKDXB 1 year, 7 months ago

Selected Answer: D

correct

upvoted 1 times

VeiN 2 years ago

Selected Answer: D

Hope this will illustrate better if somone is confused:

https://www.strath.ac.uk/professionalservices/is/cybersecurity/mfa/whatifidonthaveasignalorwi-ficonnectiononmyphone/

upvoted 2 times

Fcnet 2 years, 2 months 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 2 times

Fcnet 2 years, 2 months ago

oups 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/9nblgggzmcj6?activetab=pivot:overviewtab

upvoted 1 times

hieverybody 2 years ago

OS: Windows 10 Mobile version 14393.0 or higher, Windows 8 Mobile

No desktop versions.

upvoted 1 times

Fcnet 2 years, 2 months 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 2 years, 2 months 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** 2 years, 3 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** 2 years, 3 months ago
Disregard, i'm a dumb dumb. Of course, there is no "Email" Azure MFA option.

Answer is D
upvoted 1 times

Question #18 *Topic 2*

HOTSPOT -

You have a Microsoft 365 tenant.

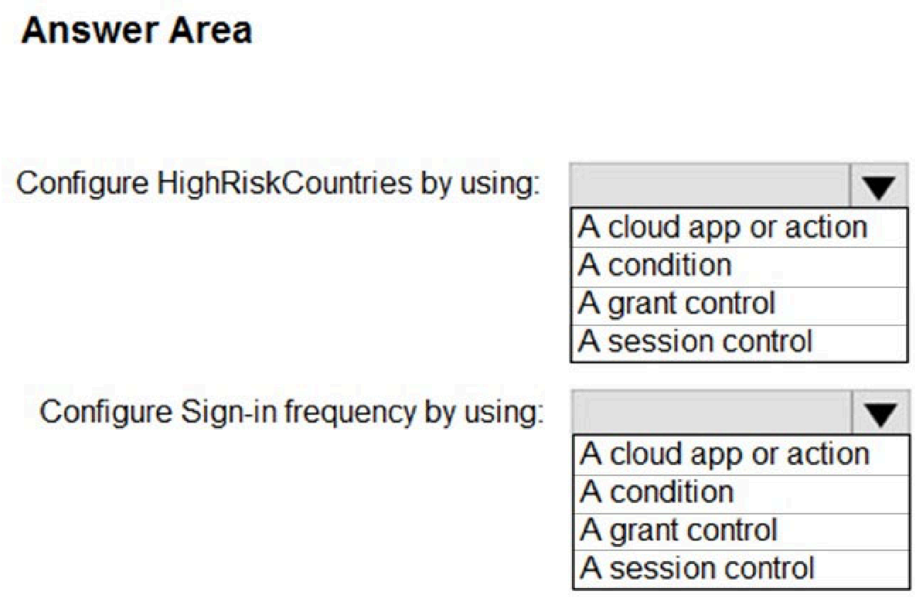
You create a named location named HighRiskCountries that contains a list of high-risk countries.

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

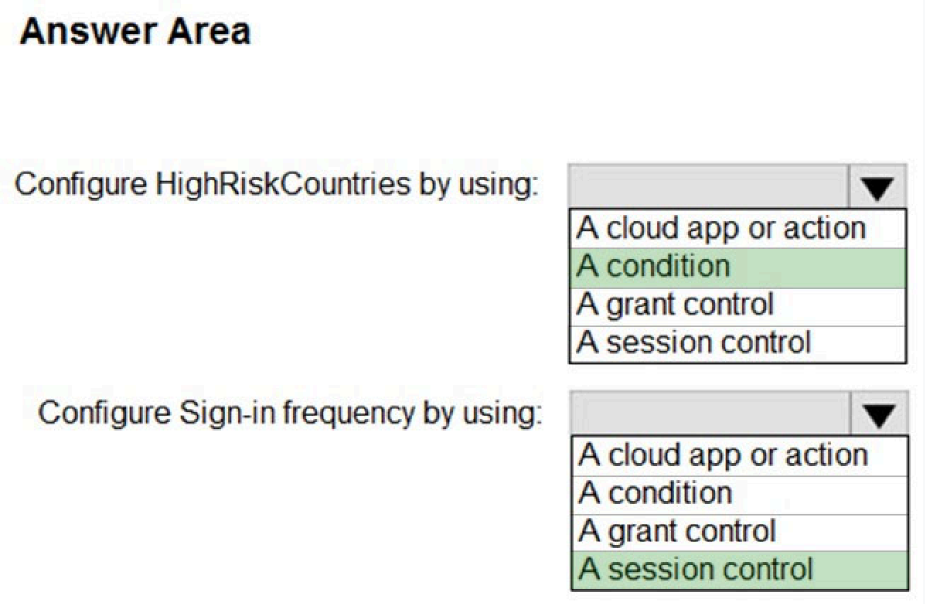
Configure HighRiskCountries by using:

- 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

Suggested Answer:



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]

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, 7 months ago

This is correct. CONDITION-->named LOCATION.

SESSION-->SIGN-IN FREQUENCY

upvoted 14 times

JCkD4Ni3L Most Recent 2 months, 1 week ago

Correct answers!

upvoted 2 times

EmnCours 5 months, 2 weeks ago

This is correct.

CONDITION-->named LOCATION.

SESSION-->SIGN-IN FREQUENCY

upvoted 3 times

⊟ **AMZ** 6 months, 1 week ago

Question valid - 06/23

upvoted 3 times

⊟ **dule27** 6 months, 4 weeks ago

High Risk Countires : A condition

Sign in frequency : A session control

upvoted 2 times

⊟ **Aquintero** 11 months, 1 week ago

Correcto, primero la condición y despues el control de sesion

upvoted 2 times

⊟ **[Removed]** 1 year ago

Given answers are correct.

upvoted 2 times

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

Given answer correct

upvoted 4 times

Question #19 *Topic 2*

HOTSPOT -

A user named User1 attempts to sign in to the tenant by entering the following incorrect passwords:

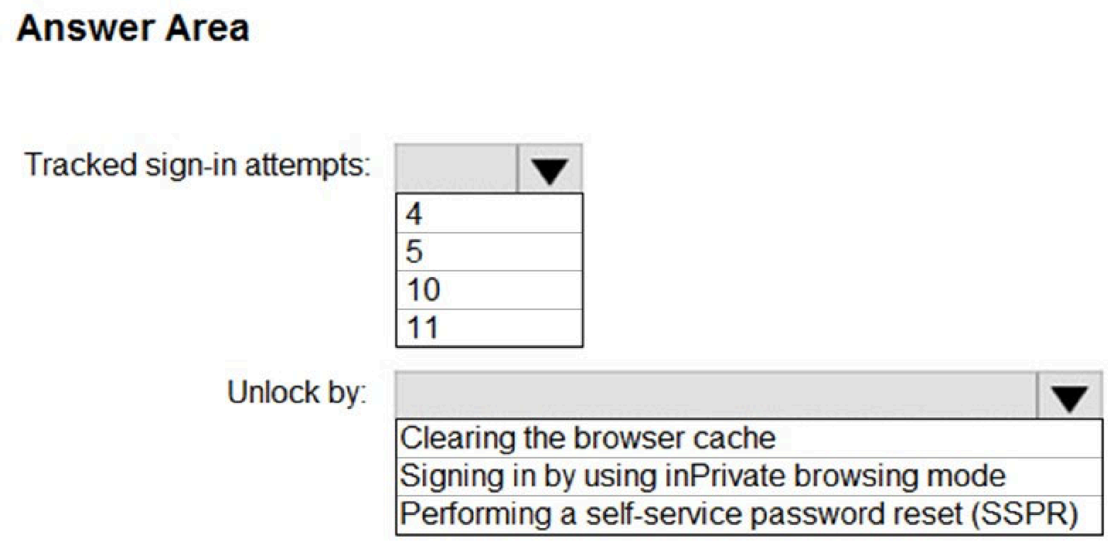
✑ Pa55w0rd12
✑ Pa55w0rd12
✑ Pa55w0rd12
✑ Pa55w.rd12
✑ Pa55w.rd123
✑ Pa55w.rd123
✑ Pa55w.rd123
✑ Pa55word12
✑ Pa55word12
✑ Pa55word12
✑ Pa55w.rd12

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:

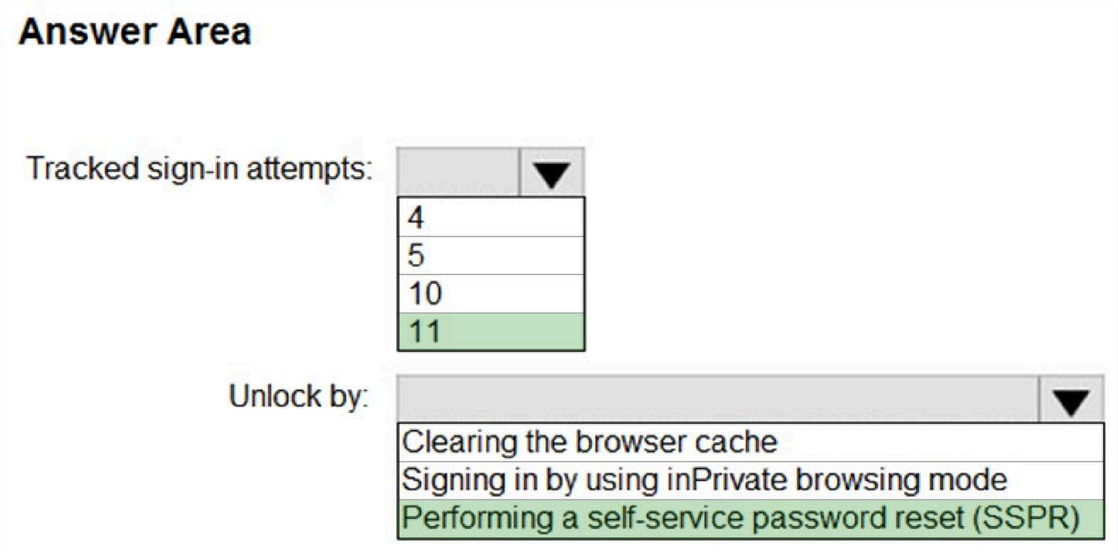


Answer Area

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)

Suggested Answer:



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)]

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

⊟ **dejo** Highly Voted 👍 1 year, 2 months 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 15 times

Hot_156 Highly Voted 1 year, 2 months 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 13 times

Nyamnyam Most Recent 1 month, 3 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 2 times

Nivos23 2 months 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 2 months ago

11
SSRP

upvoted 2 times

JCkD4Ni3L 2 months, 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 3 times

> **JCkD4Ni3L** 2 months, 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 4 months, 3 weeks ago

11
SSPR

upvoted 3 times

dule27 6 months ago

11
SSPR
upvoted 2 times

⊟ **Holii** 6 months, 3 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 2 times

⊟ **diego17** 9 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** 11 months, 1 week 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 4 times

⊟ **wsrudmen** 11 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 providen. And then it's not five. Check the 3 last pwd
upvoted 1 times

⊟ **BRoald** 11 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 thats described in the question.

Then i went to Portal.azure > AAD > Users > User 1 & User 2 > Sign-In Logs:

I got on both users exact 11 sign-in loggings. Every wrong or correct authentication is logged into Azure.

Final answers:

Tracked sign-in: 11
Unlock by: SSPR
upvoted 14 times

⊟ **TimophxMS700** 1 year 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 2 times

⊟ **[Removed]** 1 year ago

The given answer is correct.

upvoted 2 times

⊟ **Jhill777** 1 year, 1 month 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, 1 month 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, 1 month 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** 6 months, 3 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, 1 month 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".

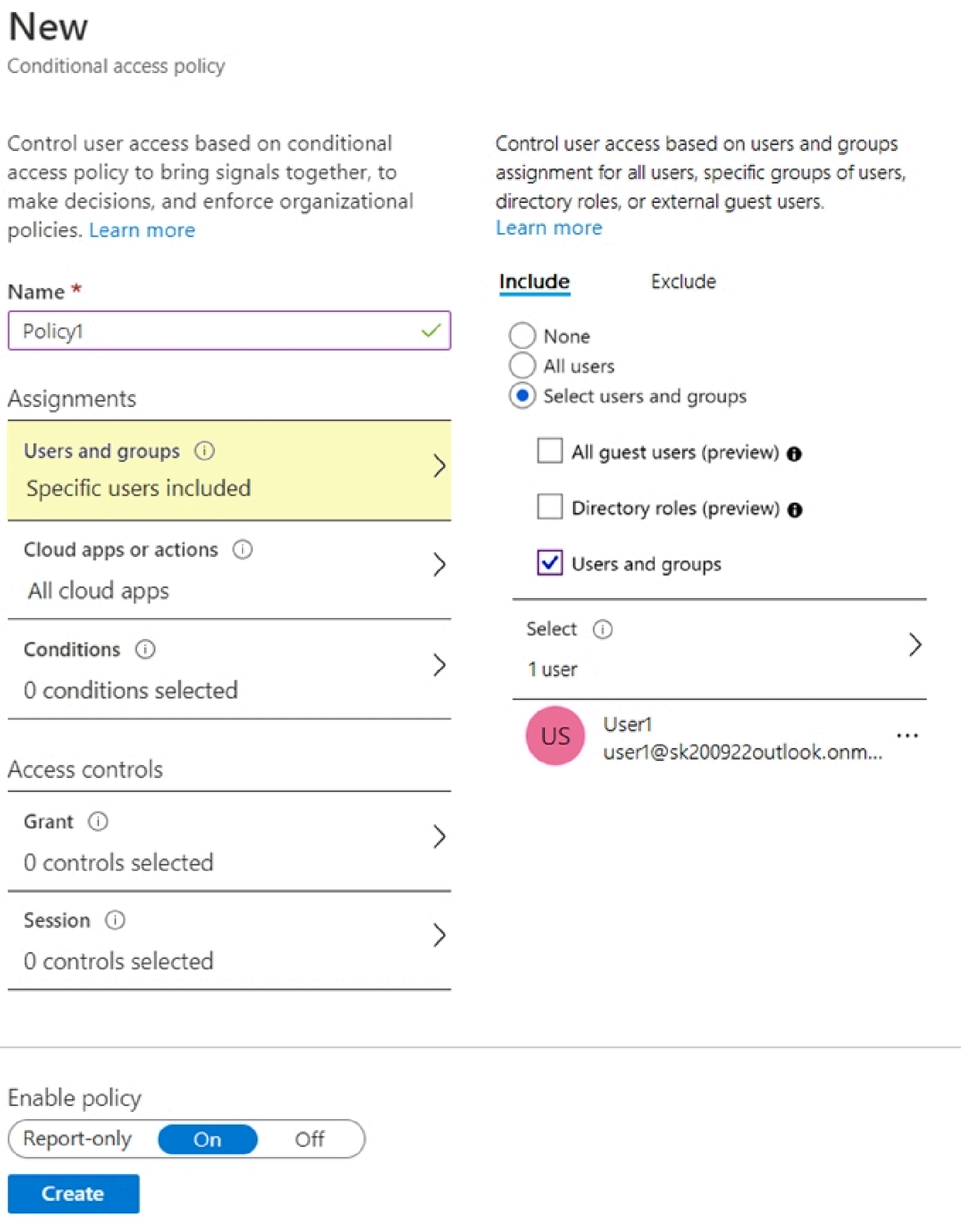
upvoted 2 times

Question #20 *Topic 2*

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 ⓘ
Specific users included

Cloud apps or actions ⓘ
All cloud apps

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
0 controls selected

Session ⓘ
0 controls selected

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users.
Learn more

Include Exclude

○ None
○ All users
● Select users and groups

□ All guest users (preview)

□ Directory roles (preview)

☑ Users and groups

Select ⓘ
1 user

US User1
user1@sk200922outlook.onm...

Enable policy

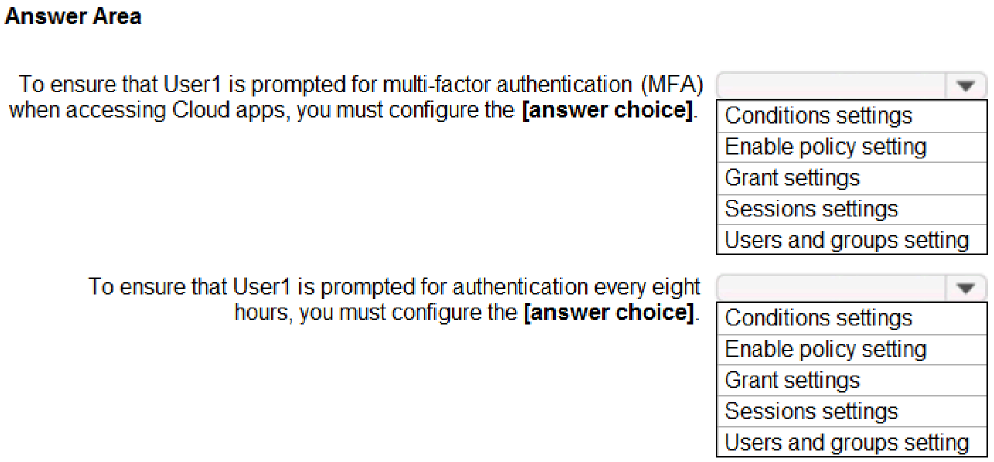
Report-only [✓ On] Off

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

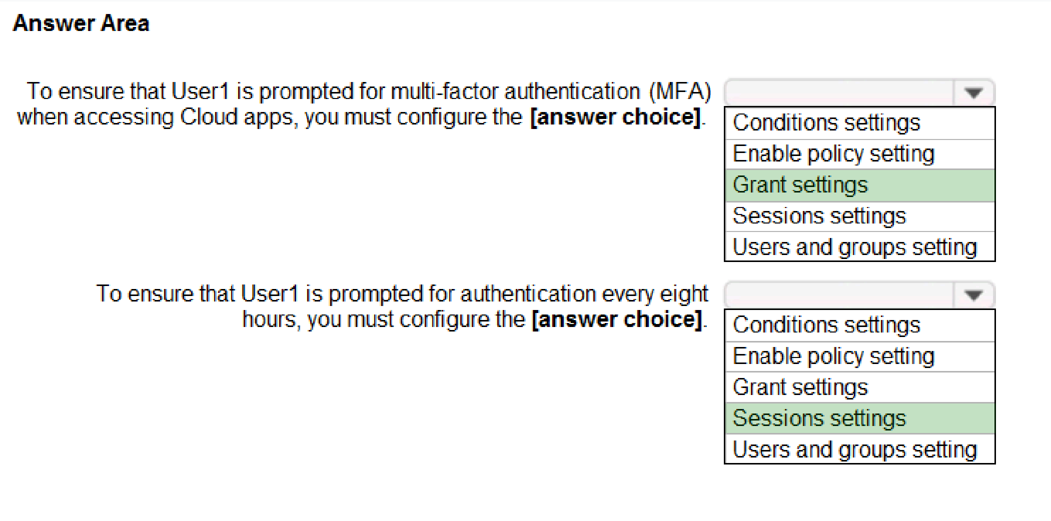
To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the **[answer choice]**.

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

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

Suggested Answer:



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

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 3 years, 6 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 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 37 times

Sugarrose 3 years, 4 months ago

Hi friend, do you have exam dump for sc-300 ?

upvoted 2 times

jimmyjose 1 year, 3 months ago

Hahahahahaha

upvoted 2 times

sergioandreslq 2 years, 6 months ago

Perfect answer and very well explained.

upvoted 2 times

MajorUrs Highly Voted 3 years, 7 months ago

Correct

upvoted 7 times

EmnCours Most Recent 1 year, 5 months ago

Correct

upvoted 2 times

dule27 1 year, 6 months ago

Prompted for MFA: Grant settings

Prompted for authentication every 8 hours: Session settings

upvoted 4 times

[Removed] 2 years ago

Answer given is correct.

upvoted 1 times

Imee 2 years, 3 months ago

on the exam 09222022, i answered the same. Passed the exam, btw.
upvoted 3 times

⊟ **Nail** 2 months, 1 week ago

Did you get 100%? Cuz that's the only way it matters ;)
upvoted 1 times

⊟ **Xyz_40** 2 years, 7 months ago

Correct. This can easily be done in your Azure tenant
upvoted 1 times

⊟ **Jun143** 2 years, 9 months ago

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

⊟ **Nhurexjayyy** 3 years ago

Correct.... https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime
upvoted 2 times

Question #21 *Topic 2*

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

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

Community vote distribution
B (79%) A (17%)

sezza_blunt Highly Voted 3 years, 6 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 79 times

Alcpt 8 months, 1 week ago
The Helpdesk admin does NO invalidate sessions capability.
upvoted 1 times

[Removed] 2 years, 10 months ago
I think it's B too. Helpdesk Administrator seems to be the correct answer.
upvoted 4 times

Domza 3 years, 6 months ago
There you go - Help Desk Admin - "Users with this role can change passwords, invalidate refresh tokens"
upvoted 5 times

Jhill777 2 years, 1 month ago
Authenication Administrator Role Permmissions includes:
microsoft.directory/users/invalidateAllRefreshTokens
Force sign-out by invalidating user refresh tokens.
upvoted 7 times

rozgonyi Highly Voted 3 years, 8 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 65 times

Acbrownit 2 years, 8 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 3 times

med4 3 years, 2 months 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 invalided them (invalided refresh token)
upvoted 26 times

Holii 1 year, 6 months 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

Sunth65 Most Recent 4 days, 13 hours ago
Selected Answer: A
A.
Authentication administrator is the correct answer.
Authentication Administrator can only reset non admin accounts password
upvoted 1 times

Nail 2 months, 1 week ago
Selected Answer: A
Authentication Administrator and Helpdesk Administrator both have microsoft.directory/users/invalidateAllRefreshTokens and microsoft.directory/users/password/update permissions so I really feel like it comes down to the "non-admin" part of the question. Helpdesk Administrators have more permissions than they need in this area, i.e., they can reset passwords of admins. Authentication Administrators can only reset the passwords of non-admins so the answer is Authentication Administrators.
upvoted 1 times

ItzVerified 8 months, 2 weeks ago
Selected Answer: B
Help Desk Admin - "Users with this role can change passwords, invalidate refresh tokens"
upvoted 1 times

NICKTON81 8 months, 2 weeks ago
Selected Answer: B
B
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#helpdesk-administrator
upvoted 1 times

Bhavneet1802 10 months, 1 week ago
Selected Answer: B
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.
upvoted 2 times

JanioHSilva 1 year ago
Selected Answer: B
Based on this, it seems that the Authentication Administrator role would be the most suitable, as it allows you to reset passwords for non-administrators. However, the ability to invalidate sessions is also required, and the Authentication Administrator role does not provide this.

The Helpdesk Administrator role, on the other hand, allows both password reset and session invalidation for non-administrators, which satisfies both requirements for SecAdmin1.

upvoted 3 times

⊟ **Nyamnyam** 1 year, 1 month 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 3 times

⊟ **haazybanj** 1 year, 1 month 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 3 times

⊟ **haazybanj** 1 year, 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** 1 year, 1 month 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 2 times

⊟ **Nivos23** 1 year, 2 months ago

Selected Answer: B

I think it's B

upvoted 2 times

⊟ **sherifhamed** 1 year, 3 months 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** 1 year, 6 months ago

Selected Answer: A

A. Authentication administrator

upvoted 1 times

⊟ **Sango** 1 year, 6 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 3 times

⊟ **Garito** 1 year, 6 months ago

Selected Answer: B

Answered correctly in similar question.

upvoted 2 times

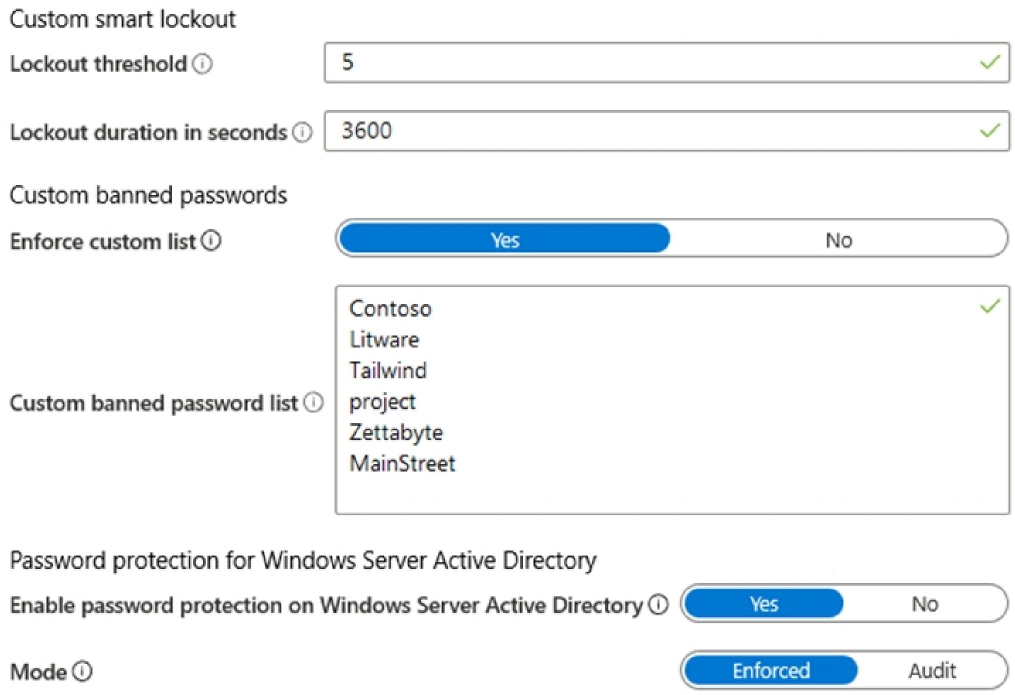
⊟ **mali1969** 1 year, 6 months ago

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

Question #22 Topic 2

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

Suggested Answer: *C*

Reference:

https://blog.enablingtechcorp.com/azure-ad-password-protection-password-evaluation

Community vote distribution

C (85%) D (15%)

arghhhh Highly Voted 2 years, 7 months ago

Test on tenant, all three are blocked.

Answer is C

upvoted 38 times

Goseu Highly Voted 2 years, 7 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 17 times

Holii 6 months, 3 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 3 times

Holii 6 months, 3 weeks ago

To add; this is definitely C. Not to misguide anyone with my curiosity lol.

upvoted 2 times

Holii 6 months, 3 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 6 times

poesklap Most Recent 1 month ago

Selected Answer: C

Answer is C

upvoted 1 times

dule27 6 months ago

Selected Answer: C

C. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd

upvoted 1 times

Aquintero 11 months, 1 week ago

Selected Answer: C

C. C0nt0s0, Pr0jectlitw@re y T@ilw1nd

upvoted 1 times

[Removed] 1 year ago

Selected Answer: C

All passwords will be blocked.

upvoted 1 times

Jhill777 1 year, 1 month 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 2 times

reastman66 1 year, 1 month 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 on 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, 3 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, 4 months ago

Selected Answer: D

Tested

upvoted 2 times

Tokiki 1 year, 6 months ago

yes. it need 5 pts.

upvoted 2 times

Nilz76 1 year, 8 months ago

This question was in the exam 28/April/2022

upvoted 1 times

Nilz76 1 year, 9 months ago

Selected Answer: C

Tested in my tenant, Answer is C

upvoted 1 times

Yelad 1 year, 9 months ago

On the exam - March 28, 2022

upvoted 1 times

Jun143 1 year, 9 months ago

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

upvoted 1 times

stromnessian 1 year, 10 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

Question #23 *Topic 2*

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

Suggested 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 👍 3 years, 2 months ago
Security questions is not an option for MFA. Using the Authenticator app does not need network connectivity, thus the correct value
upvoted 45 times

sezza_blunt 3 years 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, 12 months ago
WRONG do not have Wi-Fi access or mobile phone connectivity.
upvoted 2 times

Acbrownit 2 years, 2 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

ReffG 2 years, 5 months ago
no it is correct. TOTP also works offline.
upvoted 2 times

J4U 2 years, 8 months 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

BluMoon 2 years 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

lime568 2 years, 3 months ago

but need internet. no Wifi no mobile phone

upvoted 1 times

tinhnd 9 months, 2 weeks ago

All OTP apps or FIDO2 don't need internet connection to work.

upvoted 1 times

Benkyoujin 2 years, 1 month ago

Incorrect and you can test this.

upvoted 1 times

Cheif 3 years, 2 months ago

But they don't have mobile phones? how will they access the mobile authenticator app?

upvoted 1 times

tinhnd 9 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

B0 3 years, 1 month ago

but they do :) All users have mobile phones and laptops.

upvoted 4 times

Cheif 3 years, 2 months ago

Scratch that A is the correct answer, doesn't need internet IMO

upvoted 7 times

Ed2learn 3 years 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 8 months, 1 week 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 4 times

G5kawde 3 months, 1 week ago

hahaha

upvoted 1 times

melatocaroca 2 years, 12 months ago

WRONG do not have Wi-Fi access or mobile phone connectivity.

upvoted 1 times

leeuw86 Highly Voted 👍 3 years 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

Ed2learn 3 years 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

sezza_blunt 3 years ago

That changes it a bit. The notification requires mobile connectivity. Did you choose WHFB as the correct answer?

upvoted 2 times

easypeacy Most Recent ⊙ 9 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 11 months, 2 weeks ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

dule27 1 year ago

Selected Answer: A

A. a verification code from the Microsoft Authenticator app

upvoted 1 times

LeTrinh 1 year, 4 months ago

https://drake.teamdynamix.com/TDClient/2025/Portal/KB/ArticleDet?ID=50929

upvoted 2 times

[Removed] 1 year, 6 months ago

Selected Answer: A

Correct answer.

upvoted 2 times

PadyLoki 1 year, 11 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, 11 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 2 years ago

A is correct

upvoted 1 times

sapien45 2 years 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 2 years ago

On the exam - June 12, 2022

upvoted 1 times

YetiSpaghetti 2 years ago

Selected Answer: A

A is obviously the answer. Voice needs mobile connectivity. MFA authenticators do not.

upvoted 1 times

> **RandomNickname** 2 years ago
>
> Voice doesn't necessary need to be do a mobile phone, and could be to 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 2 years, 1 month ago

Question needs more information since it can be both A or C.
See below for accept 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** 2 years, 1 month 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** 2 years, 1 month 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** 2 years, 2 months ago

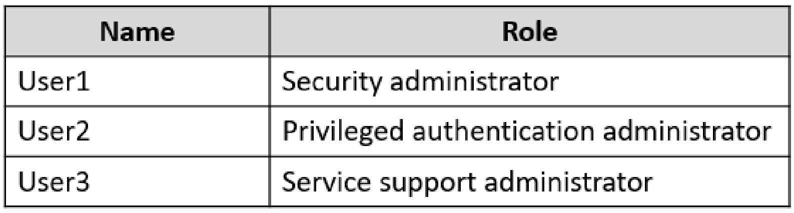
This question was in the exam 28/April/2022

upvoted 1 times

Question #24 Topic 2

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

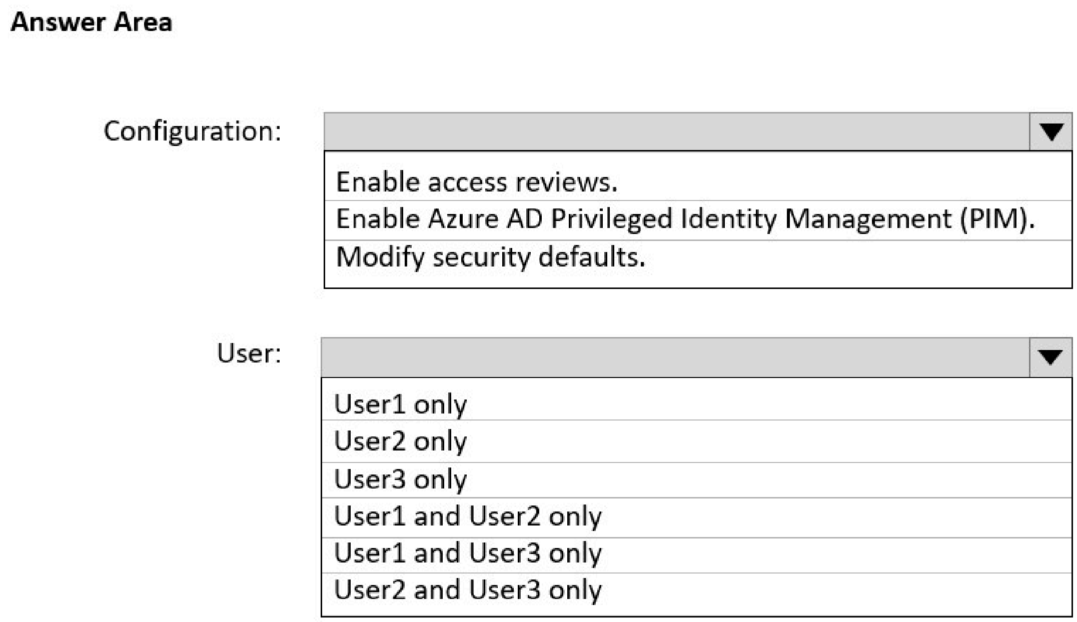
User2 reports that he can only configure multi-factor authentication (MFA) to use the Microsoft Authenticator app.

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:

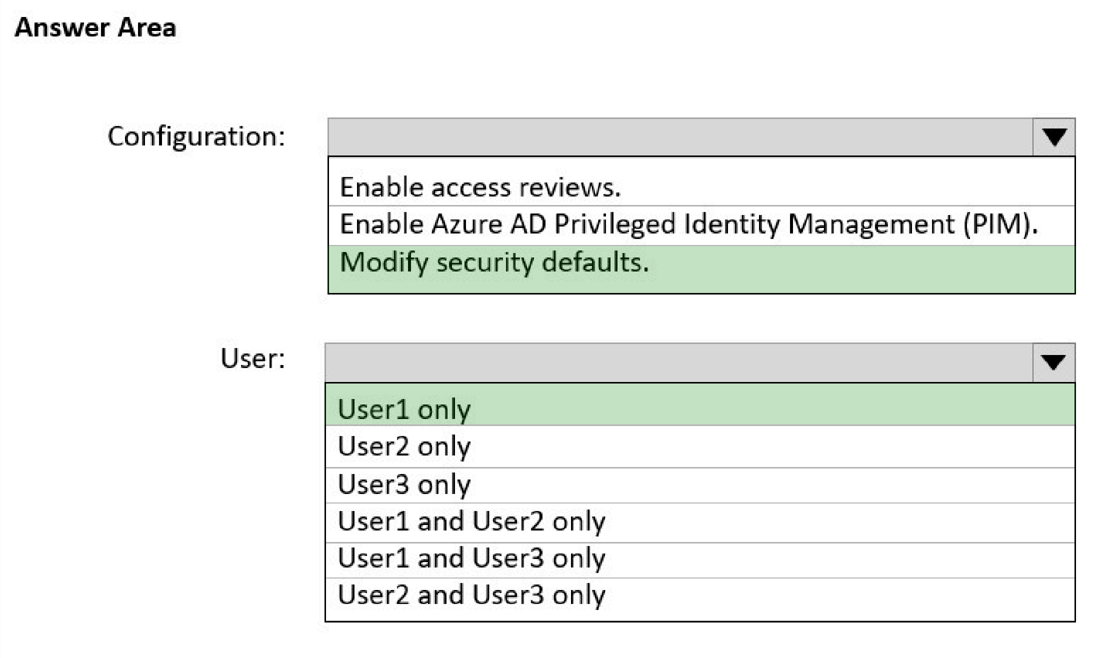


Answer Area

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

Suggested Answer:



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

Box 1: Modify security defaults.

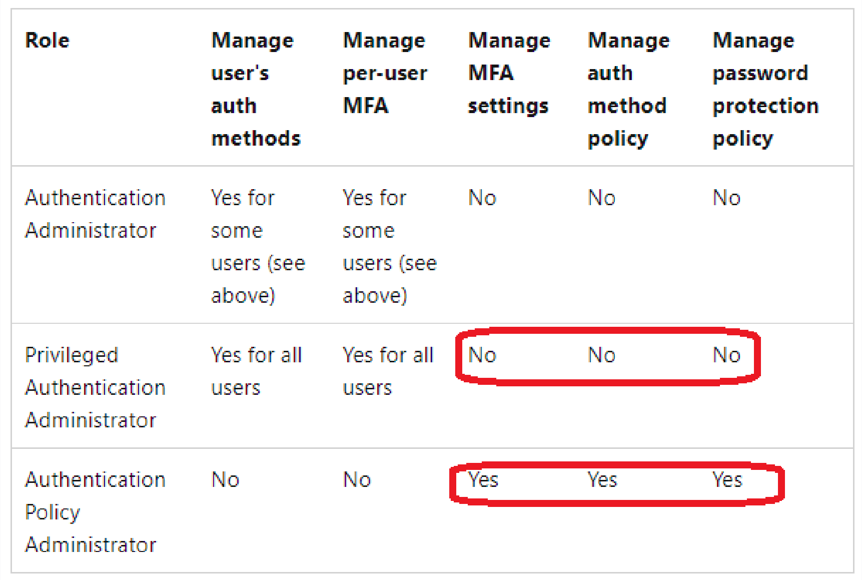
Privileged Authentication Administrator

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

geobarou Highly Voted 1 year, 9 months ago

Checked in SC300 MOC book. The answer is correct

upvoted 11 times

Cepheid Highly Voted 1 year, 6 months 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 9 times

BB6919 1 year, 6 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 2 times

kanew 1 year, 1 month 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 3 times

JuanZ Most Recent 2 months, 1 week ago

Modify security settiings

Privileged Authentication Administrator

This is a privileged role. Assign the Privileged Authentication Administrator role to users who need to do the following:

Set or reset any authentication method (including passwords) for any user, including Global Administrators.

upvoted 2 times

Tuvshinjargal 4 months, 3 weeks ago

I think it is PIM and User 1. User 1 can the appropriate permission to User 2 for a while with PIM. There is no way to modify Security Defaults.

upvoted 1 times

vaaws 7 months, 2 weeks ago

Security Defaults

User2

upvoted 3 times

> **SFAY** 5 months, 1 week ago
>
> User 2 is not the right answer. User 2 already has a PAA role assigned however is unable to do the task. Therefore, the only other possible choice is Security Admin which is User 1.
>
> upvoted 1 times

dule27 1 year ago

Modify security defaults

User1 only

upvoted 3 times

ShoaibPKDXB 1 year, 1 month ago

Correct

upvoted 1 times

BB6919 1 year, 6 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 1 year, 6 months 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 2 times

[Removed] 1 year, 6 months ago

Agree with DeepMoon. Security Defaults cannot be modified, it must be PIM. 2nd answer is correct.

upvoted 3 times

ooltie 1 year, 8 months 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, 9 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 2 times

Question #25 *Topic 2*

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

Suggested 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%)

Siraf 6 months, 1 week ago
Answer is C:

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.
https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks
upvoted 4 times

Leon1969 9 months, 1 week ago
When administrators require one method be used to reset a password, verification code is the only option available
upvoted 2 times

sherifhamed 9 months, 2 weeks 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 4 times

EmnCours 11 months, 2 weeks ago
Selected Answer: C
Correct Answer: C
upvoted 1 times

dule27 1 year ago
Selected Answer: C
C. a mobile app code

upvoted 1 times

ShoaibPKDXB 1 year, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

jojoseph 1 year, 5 months ago

Selected Answer: C

definitely C

upvoted 1 times

Boogs 1 year, 9 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, 9 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

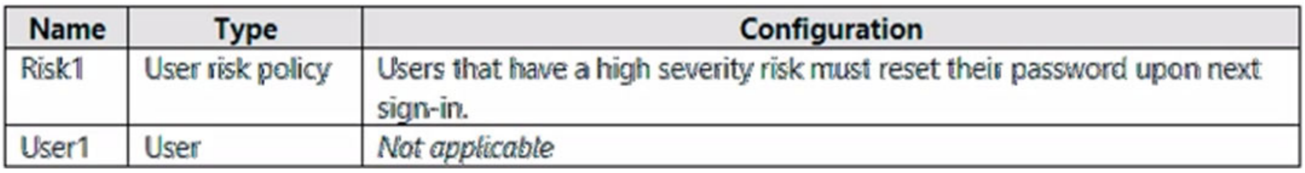
From <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

upvoted 3 times

> **CloudRat** 1 year, 5 months 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

Question #26 *Topic 2*

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 MIFA registration for User1.

D. Configure a sign-in risk policy.

Suggested 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 (93%) 7%

⊟ **Buzz8** Highly Voted 1 year, 1 month ago

Selected Answer: B

The questions 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 8 times

⊟ **Sunth65** Most Recent 4 days, 13 hours ago

Selected Answer: B

Only this one effecting user1.

B. Mark User1 as compromised. !

All these effecting Tenant. !!

A. Reconfigure the user risk, policy to trigger on medium or low severity.

C. Reset the Azure MIFA registration for User1.

D. Configure a sign-in risk policy.

upvoted 1 times

⊟ **dule27** 6 months, 3 weeks ago

Selected Answer: B

B. Mark User1 as compromised

upvoted 1 times

⊟ **ShoaibPKDXB** 7 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

⊟ **kanew** 8 months ago

Selected Answer: B

Correct and less effort than A which will impact all users

upvoted 1 times

⊟ **Aquintero** 11 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** 1 year 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]** 1 year ago

Selected Answer: B

Given answer is correct.

upvoted 1 times

⊟ **kerimnl** 1 year, 1 month ago

Selected Answer: A

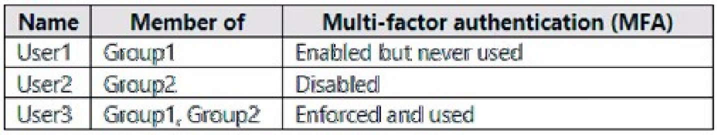
I think the correct answer is A.

upvoted 1 times

Question #27 *Topic 2*

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:

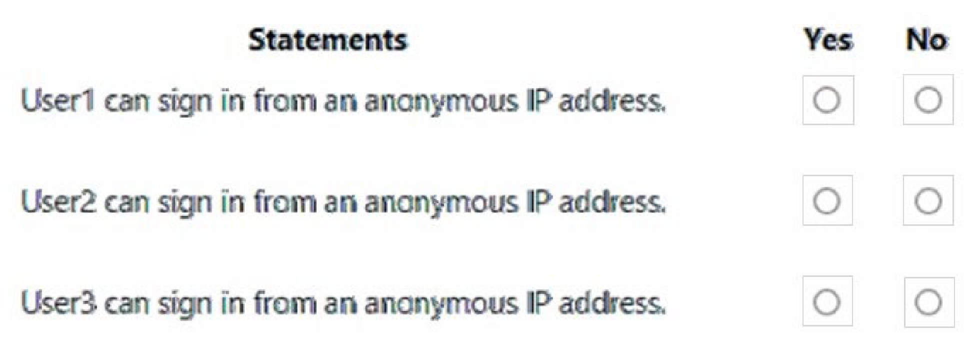
- Access: Require multi-factor authentication

✑ Enforce policy: On

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

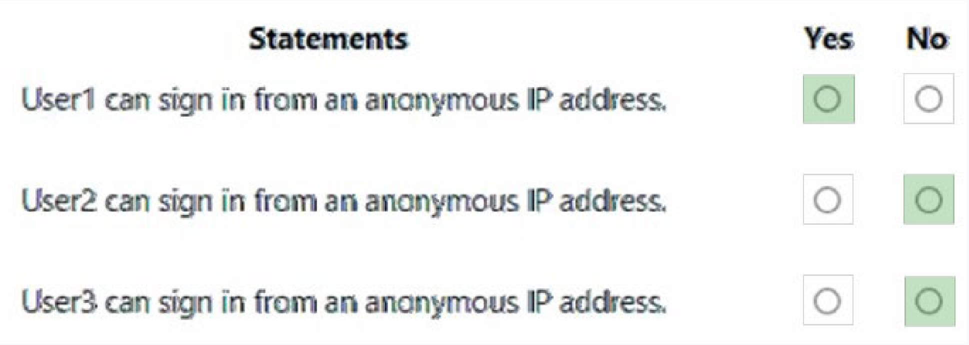
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
User1 can sign in from an anonymous IP address.	○	○
User2 can sign in from an anonymous IP address.	○	○
User3 can sign in from an anonymous IP address.	○	○

Suggested Answer:



Statements	Yes	No
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 2 years, 4 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 62 times

existingname 2 years, 4 months ago

On the exam today, I answered Yes No Yes

upvoted 11 times

kanew 1 year, 7 months ago

Perfectly explained - I agree it's Y,N,Y

upvoted 6 times

mcas 2 years 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 2 years 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 4 times

LeTrinh 1 year, 10 months ago

You're right, Purek77
https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

upvoted 1 times

Holii 1 year, 6 months 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

ItchyBrain81 2 years, 3 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

0byte Highly Voted 2 years, 2 months 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 is 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

enklau Most Recent 2 months, 2 weeks ago

i'll go with yes no yes, as they assume that user1/3 are already logged in the scope of the policy, so the user-risk policy has nothing to do with anonimous ips

upvoted 1 times

emartiy 9 months, 1 week ago

Definitely YES NO YES..
1) Yes-
---User1 is not member Group2. So, when User1 login via Anonymous IP User Sign-in policy isn't applied for this user and can login without any interrupt.
2) No-
---User2 is member of Group2 which is Risky sing-in policy applied due to login via Anonymous IP and User2 MFA disabled which related policy asks for but user2 won't be able to complete for sign-in.
3) Yes-
---User3 is member of Group2 which is Risky sing-in policy applied due to login via Anonymous IP and User3's MFA is enabled and in use. So, this user can continue with MFA once it asked by the Risky sign-in policy..

Note: User Risky Policy works based on Leaked credentials and Azure AD threat intelligence according to on user risk level. Check Microsoft Learn for more info.

Note2: Risky Sign-in Policy works based on Anonymous IP address Atypical travel, Malware, linked IP address, Unfamiliar sign-in properties, Leaked credentials, and Password spray. It triggered according to each login attempt's source, method etc.

upvoted 2 times

MatExam 11 months, 1 week ago

All seems correct about what is said for user 1 and 3, But I don't agree on user 2....
User 2 has the status disabled, this simply means MFA is not enforced, but it can still be used. To quote MS:
"When the MFA status is disabled, it means that the user is not required to provide additional authentication beyond their password to access their account. However, it is possible that MFA is still being used in some capacity, such as for certain applications or services."

Disabled only means the user is not enrolled in per-user MFA, but it doesn't mean MFA is not configured...
https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-userstates

So answer "should" be Y-Y-Y... but you neven know what MS is after so it is always a gamble.. It is not like you can defend your answer.

upvoted 2 times

MatExam 11 months, 1 week ago

Even more, if the user-risk policy would hit user 1, then the user would remediate, SSPR would kick in which also requires MFA. Since the status is "enabled" it means no MFA method is registered, for sure, so remediation would not work...
In contrast with user2, which has status "disabled" you don't know if there is a method registered or not... so this is in ways Shrodingers User :D

upvoted 1 times

BenLam 1 year, 2 months 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 1 year, 4 months ago

Yes
No
Yes

upvoted 2 times

dule27 1 year, 6 months ago

Yes
No
Yes

upvoted 2 times

TomasValtor 1 year, 7 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 1 year, 11 months ago

para mi la respuesta correcta es Yes, No, Yes

upvoted 1 times

⊟ **jojoseph** 1 year, 11 months ago

Yes No Yes

upvoted 1 times

⊟ **jack987** 2 years 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 2 times

⊟ **jack987** 2 years 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** 2 years 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 3 times

⊟ **Cepheid** 2 years ago

Block wins over grant. However, we're talking here about user and sign in risk policies. The questions concerns a sign in risk type. It should be Y,N,Y.

upvoted 4 times

⊟ **purek77** 2 years 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]** 2 years ago

Given answer is correct!

upvoted 1 times

Question #28 *Topic 2*

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

Suggested 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%)

shoutiv Highly Voted 1 year, 6 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 5 times

HartMS Most Recent 3 months, 1 week ago

An Email address is a correct answer, as it does not matter if it's an internal email or external

upvoted 2 times

dule27 1 year ago

Selected Answer: A

A. an email to an address outside your organization

upvoted 2 times

ShoaibPKDXB 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 2 times

Jawad1462 1 year, 8 months ago

Selected Answer: A

Is the correct answer

upvoted 1 times

TheMCT 1 year, 8 months ago

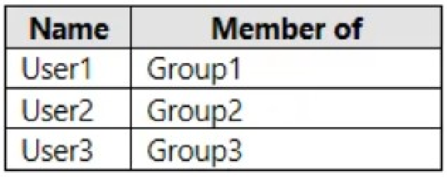
The given answer is correct!

upvoted 1 times

Question #29

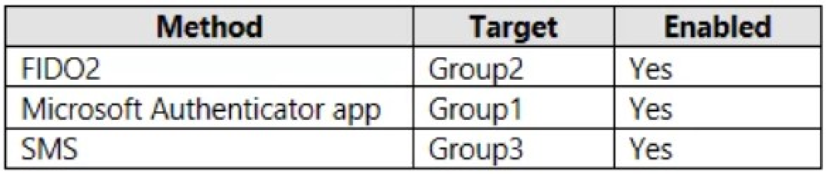
Topic 2

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

Suggested 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%)

KoenJas 5 months, 2 weeks ago

Imo it should also be the sms categorie, right? Like; they also read something in numberic form from their mobiledevice lol.

upvoted 1 times

Nail 2 months, 1 week ago

That wouldn't be "matching" though.

upvoted 1 times

emartiy 9 months, 1 week ago

Selected Answer: A

For 3 options, only Microsoft Authenticaiton app provide code (it also works offline).

Answer is User1 Only

upvoted 2 times

emartiy 9 months, 1 week ago

For 3 options, only Microsoft Authenticaiton app provide code (it also works offline).

Answer is User1 Only

upvoted 2 times

EmnCours 1 year, 5 months ago

Selected Answer: A

Answer is A

upvoted 2 times

dule27 1 year, 6 months ago

Selected Answer: A

A. User1 only (MA App)

upvoted 2 times

jojoseph 1 year, 11 months ago

Selected Answer: A

A is right

upvoted 1 times

zokaniedereenhet 2 years ago

SMS is a preview feature, might also work?!

upvoted 1 times

ZauberSRS 2 years, 1 month ago

Selected Answer: A

Answer: A

I have had this for a least a year on my private MS account with MFA

upvoted 2 times

LHADUK 2 years, 1 month 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 2 years, 2 months 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 4 times

> **kanew** 1 year, 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 2 years, 3 months ago

The answer makes sense it is the only possible answer. But the question doesn't make sense.

upvoted 4 times

> **[Removed]** 1 year, 8 months ago
>
> I think what pointed it out to me after incorrectly answering was the part saying "...shown in the APP..."
>
> upvoted 1 times
>
> > **[Removed]** 1 year, 8 months 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 2 years, 3 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.

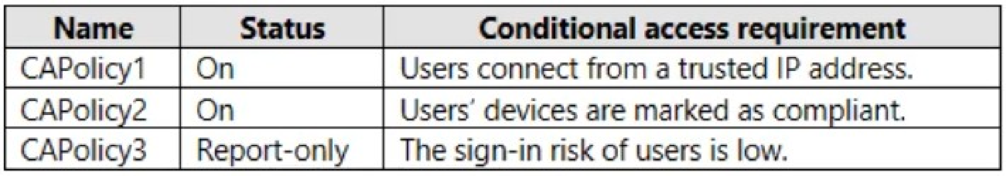
what is this?

"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

Question #30 *Topic 2*

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

Suggested 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, 3 months ago
Correct.
upvoted 6 times

shoutiv Highly Voted 1 year 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 5 times

EmnCours Most Recent 5 months, 2 weeks ago
Selected Answer: C
Correct Answer: C
upvoted 2 times

dule27 6 months, 2 weeks ago
Selected Answer: C
C. The What If tool
upvoted 1 times

ShoaibPKDXB 7 months, 3 weeks ago
Selected Answer: C
C is correct
upvoted 1 times

Aquintero 11 months, 1 week ago
Selected Answer: C

de acuerdo la respuesta es: C. La herramienta What If

upvoted 1 times

Question #31 *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 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

Suggested 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 (96%) 4%

birrach Highly Voted 2 years, 3 months ago
Selected Answer: C
App Passwords are a legacy feature for old Office versions. Windows Hello is the way to go.
upvoted 14 times

ndawg07 Highly Voted 2 years, 4 months ago
Selected Answer: C
C should be the answer.
upvoted 9 times

Panama469 Most Recent 5 months, 3 weeks ago
Exam has 311 questions... well minus 50 for the number of times this question pops up!
upvoted 2 times

emartiy 9 months, 1 week ago
Selected Answer: A
Actually, this situation won't stop to complete MFA via phone while almost all Laptops support Hotspot feature which you can turn on to share your wired internet via Laptop :) So, you can get your phone connected to the internet and continue your work... However, it is not in case for this question. If you are not able to perform 2 step verification for any reason, for example old apps do not support MFA, you still have option to use app password. So, if you set an app password for the app you will use at Laptop which will be connected to the internet via Wired internet, you can use that app password to by-pass MFA. Have good points!
upvoted 1 times

oroboro 11 months, 3 weeks ago
A. App password is more correct according to this:
When a user account is enforced for Microsoft Entra multifactor authentication, the regular sign-in prompt is interrupted by a request for additional verification. Some older applications don't understand this break in the sign-in process, so authentication fails. To maintain user account security and leave Microsoft Entra multifactor authentication enforced, app passwords can be used instead of the user's regular username and password. When an app password used during sign-in, there's no additional verification prompt, so authentication is successful.
https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-app-passwords
upvoted 1 times

poesklap 1 year, 1 month ago

Selected Answer: C

Windows Hello for Business is the correct answer.

upvoted 1 times

BenLam 1 year, 2 months 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 2 times

shuhaidawahab 1 year, 2 months 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 1 year, 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

dule27 1 year, 6 months ago

Selected Answer: C

C. Windows Hello for Business

upvoted 1 times

ShoaibPKDXB 1 year, 7 months ago

Selected Answer: C

C is correct

upvoted 1 times

kanew 1 year, 7 months ago

Selected Answer: C

C is the correct answer. A is legacy authentication and would bypass MFA

upvoted 1 times

Aquintero 1 year, 11 months ago

Selected Answer: C

Windows Hello

upvoted 2 times

chrisp1992 2 years ago

Selected Answer: C

App Passwords are legacy

upvoted 4 times

[Removed] 2 years ago

Selected Answer: C

Windows Hello for Business is the correct answer.

upvoted 4 times

samir45 2 years, 3 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 2 years, 3 months ago

It says "You plan to implement multi-factor authentication (MFA)." that doesnt mean either they have the a option to implement an App... but you are assuming that

upvoted 3 times

⊟ **Hot_156** 2 years, 3 months ago

Selected Answer: C

C is the answer

upvoted 5 times

Question #31 *Topic 2*

You have a Microsoft 365 E5 subscription.

You need to ensure that users can only access resources in the subscription from a device that has the Global Secure Access client connected.

What should you do first?

A. Enable Global Secure Access signaling.

B. Enable tagging to enforce tenant restrictions.

C. Create a named location.

D. Create a remote network.

Suggested Answer: *D*

Community vote distribution

A (100%)

d526b99 2 days, 14 hours ago

Selected Answer: A

The correct answer is:
A. Enable Global Secure Access signaling.

Explanation:
Global Secure Access signaling is the key step to enforce that users can only access resources when connected through the GSA client. This signaling is needed to establish the security posture for users trying to access resources and ensure that the access is restricted to users with the GSA client.

upvoted 2 times

Question #32 *Topic 2*

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)

Suggested 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 3 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 2 times

EmnCours 5 months, 2 weeks ago
Selected Answer: A
Correct Answer: A
upvoted 1 times

dule27 6 months, 2 weeks ago
Selected Answer: A
A. the Conditional Access What If tool
upvoted 1 times

kmk_01 8 months, 3 weeks ago
Selected Answer: A
Agreed
upvoted 1 times

Aquintero 11 months, 1 week ago
Selected Answer: A
A. la herramienta What If de acceso condicional
upvoted 1 times

BRoald 12 months ago

Selected Answer: A

So easy it feels like a trick

upvoted 2 times

shoutiv 1 year 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] 1 year ago

Selected Answer: A

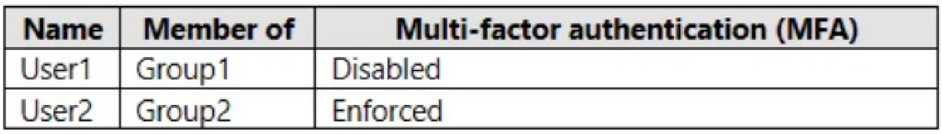
Given answer is correct.

upvoted 1 times

Question #33 Topic 2

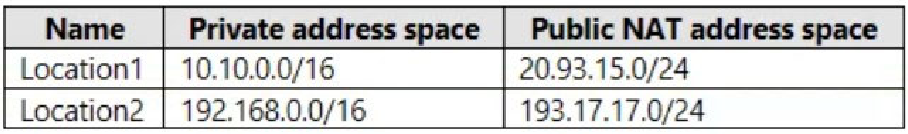
HOTSPOT -

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

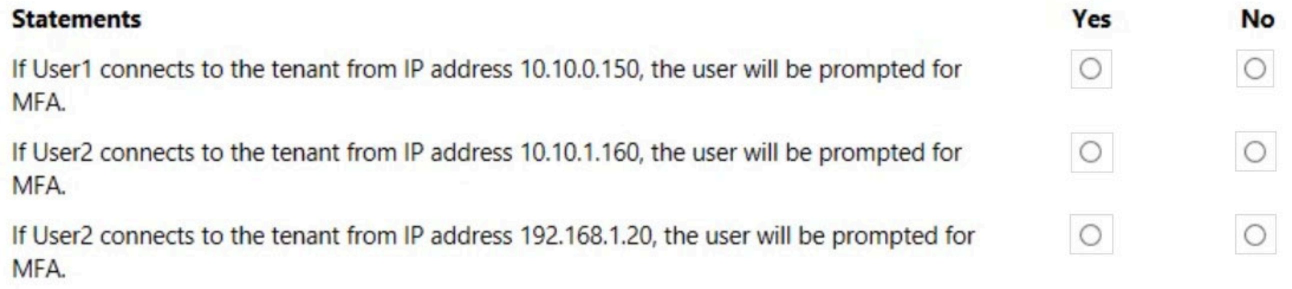
- Grant
- Grant access: Require multi-factor authentication
- Session: 0 controls selected

✑ Enable policy: On

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

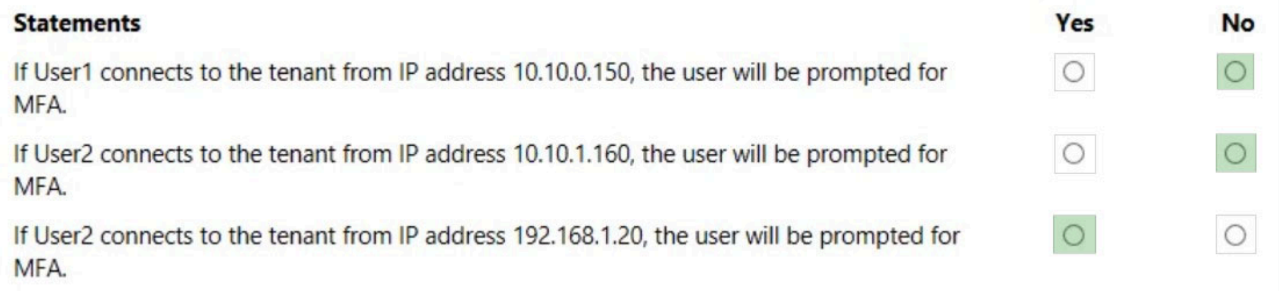
NOTE: Each correct selection is worth one point.

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.	○	○
If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.	○	○
If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA.	○	○

Suggested Answer:



Statements	Yes	No
If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.	○	[✓ ○]
If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.	○	[✓ ○]
If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA.	[✓ ○]	○

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 2 years, 3 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 27 times

f2bf85a 1 year, 8 months 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 8 times

Nail 2 months, 1 week ago

CA policy has nothing to do with User2 since that user is in Group2 and the CA policy is only applied to Group1.

upvoted 2 times

aks_exam 11 months ago

fmm.. so then the answer should be N Y Y if user2 must be authenticated cause of enforce setting.

upvoted 1 times

Nail 2 months, 1 week ago

No, because in the last case User2 is coming from a trusted IP range. NYN.

upvoted 1 times

hyc1983 Highly Voted 2 years, 1 month 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 18 times

MrPrasox 2 years, 1 month ago

Fully agree with NYN answers and with posted explanation.

upvoted 1 times

mibur 2 years 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 4 times

wooyourdaddy 1 year, 11 months 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

kanew 1 year, 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 1 year, 7 months ago

My Bad, the last one is a No. See my reasons on the post a couple below this

upvoted 2 times

Nivos23 1 year, 2 months ago

I agree with you
no
yes
no

upvoted 2 times

b233f0a 1 year, 6 months 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 9 times

RemmyT Most Recent 6 months, 3 weeks ago

NO YES YES

User1 is member of Group1 -> CAPolicy1 applies
10.10.1.150 (Location1) connect to Azure with an IP from 20.93.15.0/24 range
User1/Group1 -> CAPolicy1 -> Requires MFA : cannot login (MFA disabled)

User2 is member of Group2 -> CAPolicy1 does not apply
User2/Group2 -> MFA enforced -> will be prompted for MFA from any location
10.10.1.160 (Location1) connect to Azure with an IP from 20.93.15.0/24 range
192.168.1.20 (Location2) connect to Azure with an IP from 193.17.17.0/24 range

193.17.17.0/24 range - is trusted only in context of CAPolicy1

upvoted 1 times

Rucasll 7 months, 3 weeks ago

Enabling MFA for a user means that the user has the option to set up MFA, but it is not required. Enforcing MFA means that the user is required to set up MFA and cannot access their account until they have completed the MFA setup process.

If you enforce MFA for a user, they will be prompted to set up MFA the next time they log in to their account. They will not be able to access their account until they have completed the MFA setup process. Once they have completed the setup process, they will be required to use MFA every time they log in to their account.

Enabling MFA gives the user the option to set it up, but they can still access their account without MFA. Enforcing MFA requires the user to set it up and use it every time they log in.

upvoted 1 times

emartiy 9 months, 1 week ago

CAPolicy1 workload is Group1. So, User1 is member of that group and this policy address that user. User2 is not member of Group1. This CAPolicy1 won't be applied for this user..However, user2 has MFA enforced.. This is tricky point...

1) No - Why? User1 is member of group1 and CAPolicy1 will apply. Since user1 login from IP address in Location1 which is marked as trusted location, MFA won't be prompted... If user one try to login from an untrusted location, since MFA isn't enabled, when it is forced via policy, user1 login won't success..
2) YES - MFA is forced for user2. Even CAPolicy1 isn't assign to user2 due to user group, for each sign-in form any IP range user2 will be prompted MFA.
3) YES - Same above option 2.
NO - YES - YES.
upvoted 1 times

zlzl 10 months, 1 week ago
Tested on Azure
1. No. Because CAPolicy1 not applied, because of the location does not meet trust location requirement. Only public IP can be captured.
2. Yes. MFA is enforced for this user2
3. No. MFA is enforced for this user2, but the location is in the MFA trust IP ranges, so MFA is skipped.

Additional finding: the IP configured in MFA trusted ips will also fall into the "all trust locations" in conditional access policy
upvoted 2 times

Shuihe 11 months ago
Hi guys, just one question, 10.10.0.0/16 and 192.168.0.0/16 are both private IP, meaning you can set up these IP segments in any network. So, if user2 connects to the tenant from IP 192.168.1.20, how do you know it's from the public IP 193.17.17.0/24?
upvoted 1 times

Nyamnyam 1 year, 1 month 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 2 times

syougun200x 1 year, 3 months 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 4 times

Hawklx 1 year, 6 months 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 users 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** 1 year, 4 months ago
User1 MFA is disabled, so user1 can't be prompted isn't it?
upvoted 1 times

⊟ **ivzdf** 1 year, 5 months ago
Completely agree
upvoted 1 times

⊟ **ivzdf** 1 year, 5 months 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** 1 year, 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** 1 year, 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** 1 year, 8 months ago
The answer shown is correct, but the explanation for it it 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

⊟ **kanew** 1 year, 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

⊟ **Holii** 1 year, 6 months 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 1923.17.17.0/24, 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** 1 year, 6 months ago
*correction: trusted location is the private IP range, which is likely a misconfiguration, because we needed the public NAT here.
upvoted 1 times

⊟ **f2bf85a** 1 year, 8 months 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 Enforcent is bypassed.
upvoted 2 times

⊟ **f2bf85a** 1 year, 8 months ago
Sorry, it is No Yes NO (made a mistake on the 3rd one)
upvoted 1 times

⊟ **iwantmyexamsobad** 1 year, 9 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 thereforme 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** 1 year, 9 months ago
The level of confusion seems to display the level ridiculousness of some of these questions
upvoted 2 times

⊟ **StijnDW** 1 year, 9 months ago
wooyourdaddy explained the reasoning though
upvoted 1 times

⊟ **Taigr** 1 year, 10 months 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** 1 year, 8 months ago
It is /16 not /24
upvoted 1 times

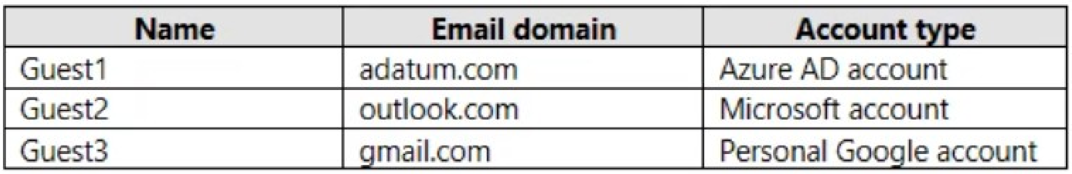
⊟ **AWS56** 1 year, 10 months ago
No-Yes-No
upvoted 1 times

Question #34 *Topic 2*

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.

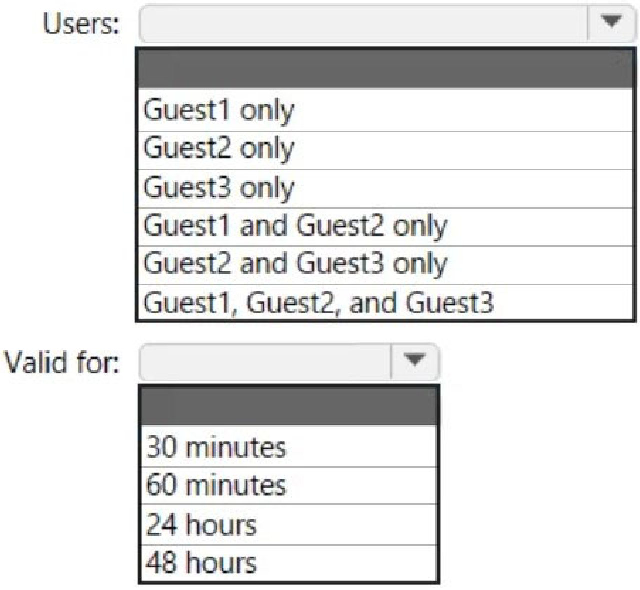


Name	Email domain	Account type
Guest1	adatum.com	Azure AD account
Guest2	outlook.com	Microsoft account
Guest3	gmail.com	Personal Google account

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.

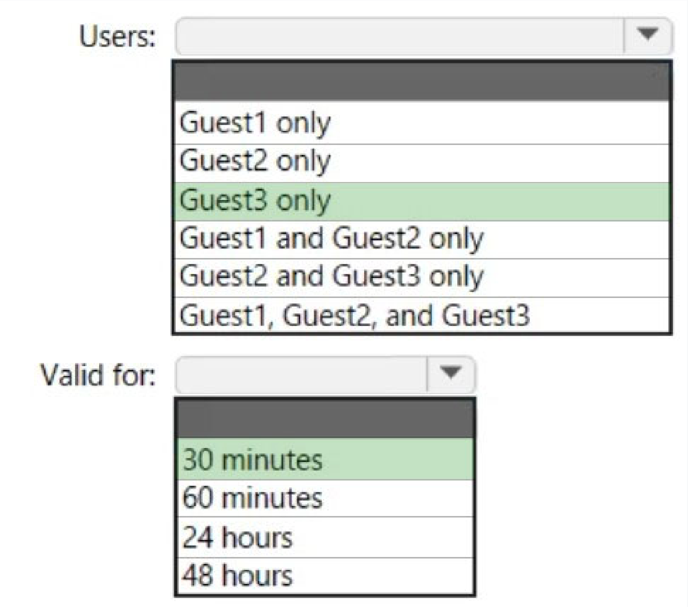
Hot Area:



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

Suggested 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

emartiy 3 months, 1 week ago

Example
Guest user nicole@firstupconsultants.com is invited to Fabrikam, which doesn't have Google federation set up. Nicole doesn't have a Microsoft account. They'll receive a one-time passcode for authentication

what about User1 which has Azure AD Account adatum.com domain? Based on the above example, User and User3 would receive one-time passcode, ??

upvoted 1 times

dbmc 9 months ago

Correct, and was on exam today.

upvoted 4 times

mfarhat1994 9 months ago

how was the exam and were these questions in the exam ?

upvoted 2 times

EmnCours 10 months, 3 weeks ago

Users:Guest 3 Only
Valid: 30 minutes

upvoted 3 times

EmnCours 11 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 3 times

dule27 1 year ago

Users:Guest 3 Only
Valid: 30 minutes

upvoted 4 times

Pedro2021 1 year, 6 months ago

Guest 3 and 30 minutes

upvoted 3 times

[Removed] 1 year, 6 months ago

Answers correct.

upvoted 1 times

kk1 1 year, 8 months ago

It is correct for 30 min. access

upvoted 1 times

⊟ **gwajwara** 1 year, 10 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 4 times

⊟ **BRoald** 1 year, 6 months ago

Great link! The given answers are correct in this case

upvoted 2 times

⊟ **existingname** 1 year, 10 months ago

correct, in the exam today

upvoted 4 times

Question #35 *Topic 2*

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

Suggested Answer: *D*

Community vote distribution

B (96%) 4%

emartiy 3 months, 1 week ago

Selected Answer: B

B. a conditional access policy in Azure Active Directory (Azure AD)

you can block user interactive sign-in via a client uses basic auth with Conditional Access policy checking..

upvoted 4 times

curtmcgirt 7 months, 3 weeks ago

Selected Answer: B

B is correct.

upvoted 1 times

Nyamnyam 8 months 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 2 times

sherifhamed 9 months, 2 weeks 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 10 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 11 months, 2 weeks ago

Selected Answer: B

Correct Answer: D

upvoted 2 times

dule27 1 year ago

Selected Answer: B

B. a conditional access policy in Azure Active Directory (Azure AD)

upvoted 3 times

Aidanjl 1 year 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** 1 year 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 1 year 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 1 year, 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

sbnpj 1 year, 2 months ago

Selected Answer: B

Conditional access policy is used for blocking legacy auth.

upvoted 1 times

Guestie 1 year, 4 months ago

Selected Answer: B

The question says nothing about what type of device or what tjhe application being used is so setting an App control policy will not do anything. CA polciies allow legacy auth to be blocked regardless of device.

upvoted 1 times

wsrudmen 1 year, 5 months ago

Selected Answer: B

B also

upvoted 1 times

Oknip 1 year, 5 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

upvoted 1 times

ydecac 1 year, 5 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

upvoted 3 times

Halwagy 1 year, 5 months ago

Selected Answer: B

as you can block legacy connection to Exchange from CA

upvoted 1 times

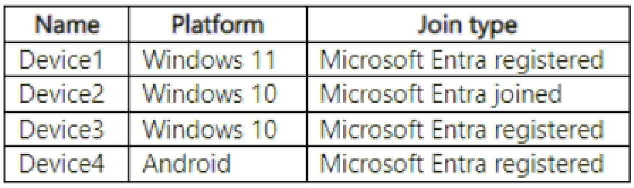
RobbieBoyBlue 1 year, 5 months ago

B for me

upvoted 1 times

Question #35 *Topic 2*

You have a Microsoft Entra tenant that contains the devices shown in the following table.



Name	Platform	Join type
Device1	Windows 11	Microsoft Entra registered
Device2	Windows 10	Microsoft Entra joined
Device3	Windows 10	Microsoft Entra registered
Device4	Android	Microsoft Entra registered

You plan to configure Microsoft Entra Private Access.

You deploy the Global Secure Access client to compatible devices.

From which devices can you use Private Access?

A. Device1 only

B. Device2 only

C. Device2 and Device4 only

D. Device1, Device2, and Device3 only

E. Device1, Device2, Device3, and Device4

Suggested Answer: *C*

Community vote distribution

B (100%)

Btn26 13 hours, 58 minutes ago

Selected Answer: E

EPA can be used with both Azure AD Joined and Azure AD Registered devices.
The Global Secure Access client can be deployed on various platforms, including Windows, macOS, iOS, Android, and Linux.
In this scenario:

Device1 (Windows 11, Microsoft Entra registered)
Device2 (Windows 10, Microsoft Entra joined)
Device3 (Windows 10, Microsoft Entra registered)
Device4 (Android, Microsoft Entra registered)
All these devices are either Azure AD Joined or Azure AD Registered and can have the Global Secure Access client deployed. Therefore, all four devices can potentially use Private Access.

Therefore, the correct answer is E. Device1, Device2, Device3, and Device4.
upvoted 1 times

Btn26 13 hours, 8 minutes ago

Changing answer to B.
Microsoft Entra Private Access compatibility requires:

Global Secure Access Client compatibility.
Join type and platform support:
Windows devices must be Microsoft Entra joined (not just registered).
Android devices are not supported for Private Access
upvoted 1 times

barlar 1 week ago

Selected Answer: B

Isn't B a better option? for Android though it seems just registered is enough but there is more to it, the question doesn't say anything about how its managed or if the authenticator app is intalled.

*Android devices must be Microsoft Entra registered devices.

-->Devices not managed by your organization must have the Microsoft Authenticator app must be installed.

-->Devices not managed through Intune must have the Company Portal app installed.

-->Device enrollment is required for Intune device compliance policies to be enforced.

upvoted 1 times

Question #36 *Topic 2*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

mali1969 Highly Voted 1 year 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

emartiy Most Recent 3 months, 1 week ago

Selected Answer: A

A system-assigned managed identity

upvoted 1 times

haazybanj 8 months 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 11 months, 2 weeks ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

dule27 1 year ago

Selected Answer: A

A. a system-assigned managed identity

upvoted 1 times

⊟ **ShoaibPKDXB** 1 year, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

⊟ **chikorita** 1 year, 3 months ago

A is correct: system assigned MI

upvoted 1 times

⊟ **Oknip** 1 year, 5 months ago

Selected Answer: A

A is correct

upvoted 2 times

⊟ **Halwagy** 1 year, 5 months ago

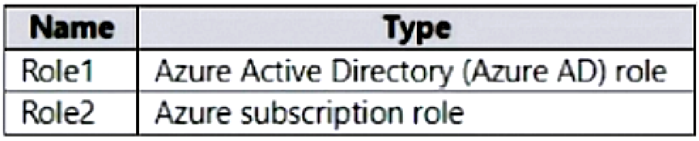
Selected Answer: A

Anser is correct

upvoted 2 times

Question #37 *Topic 2*

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

Suggested Answer: *C*

Community vote distribution

C (79%) A (21%)

haskelatchi Highly Voted 1 year, 7 months ago

I have cleared 3 certifications and can confirm the answer is F

upvoted 22 times

UKG 1 year, 5 months ago

looooool

upvoted 4 times

voituredecourse Highly Voted 1 year, 6 months ago

I have cleared 19 certifications, it is definitely C

upvoted 12 times

barlar Most Recent 1 week ago

Selected Answer: C

I have never cleared a certification, but i would still pick C

upvoted 1 times

Panama469 5 months, 3 weeks ago

C:

All your base are belong to us

upvoted 2 times

emartiy 9 months, 1 week ago

Selected Answer: C

Role 1 is custom role which is Azure AD Role.. If you want to clone Azure Sub.. role ,you need to clone one role type it even built-in or custom... So Answer is C.. Think wide!

upvoted 2 times

curtmcgirt 1 year ago

Selected Answer: C

you can clone Azure subscription roles to make new Azure subscription roles.

upvoted 2 times

kijken 1 year, 1 month 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 year, 1 month 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 4 times

kijken 1 year, 1 month ago

Thank you for clarifying. Now I understand the question and answer is C :)

upvoted 1 times

haazybanj 1 year, 1 month ago

I have cleared 29 certifications but can't confirm the answer.

upvoted 3 times

dule27 1 year, 6 months ago

Selected Answer: C

C. built-in Azure subscription roles and Role2 only

upvoted 5 times

kmk_01 1 year, 8 months ago

Selected Answer: C

I have passed AZ-104 & AZ-305, I would go for Option C too.

upvoted 5 times

chikorita 1 year, 9 months ago

i have cleared 2 certifications

i can confirm its C: built-in Azure subscription roles and Role2 only

upvoted 3 times

topzz 1 year, 9 months ago

thanks for confirming that you cleared 2 certs, otherwise your statement wouldn't have been as valuable.

upvoted 10 times

kmk_01 1 year, 8 months ago

LOL. I have passed AZ-104 & AZ-305, I would go for Option C too.

upvoted 3 times

Zak366 1 year, 10 months 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 5 times

dejo 1 year, 10 months 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 4 times

wsrudmen 1 year, 11 months 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 1 year, 11 months ago

The answer is correct. C. tested in the lab. You can clone Role2 (CustomRole) and Azure Built-in Roles

upvoted 5 times

Halwagy 1 year, 11 months ago

Selected Answer: A

it is not clear,

but Role2 only or Bulti-in Azure subscription role only not both of them

upvoted 3 times

Question #38 *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 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

Suggested Answer: *B*

Community vote distribution

A (70%) R (30%)

Holii Highly Voted 👍 1 year, 6 months ago

I swear if I see this question again with the selected answer being "An App Password" im gonna scream

upvoted 17 times

cpaljchc4 11 months, 2 weeks ago

You sure not an App passcode?

upvoted 3 times

rohitrc8521 1 year, 2 months ago

looooooooool

upvoted 2 times

kevin_office Highly Voted 👍 1 year, 11 months ago

Should be A. Windows Hello for businnes > app pasword. This question comes up several times and many users indicate that Windows hello for business is what should be the answer.

upvoted 11 times

hml_2024 Most Recent ⏱ 4 months ago

A for sure

upvoted 1 times

Logitech 1 year, 3 months 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 3 times

dule27 1 year, 6 months ago

Selected Answer: A

A. Windows Hello for Business

upvoted 1 times

ShoaibPKDXB 1 year, 7 months ago

Selected Answer: A

A is correct

upvoted 1 times

Ignaci0s 1 year, 9 months 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 3 times

> **Ruslan23** 1 year, 9 months 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 5 times
>
> > **kmk_01** 1 year, 8 months ago
> >
> > That told Nacho.
> >
> > upvoted 4 times

mayleni 1 year, 11 months ago

Selected Answer: A

WHFB!! Totally

upvoted 1 times

faeem 1 year, 11 months ago

Selected Answer: A

Should be A. Windows Hello for businnes > app pasword. 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 1 year, 11 months ago

Windows Hello for Business

upvoted 3 times

> **chikorita** 1 year, 9 months ago
>
> R? lol
>
> upvoted 4 times

ydecac 1 year, 11 months ago

Selected Answer: A

This question comes up several times and many users indicate Windows hello

upvoted 1 times

Halwagy 1 year, 11 months ago

Selected Answer: A

Windows Hello for Business

upvoted 2 times

Question #39 *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 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

Suggested Answer: *A*

Community vote distribution

B (100%)

Holii Highly Voted 1 year, 6 months ago

WFHB *internal screaming*

upvoted 20 times

gusherinos 1 year, 4 months ago

Best answer!

upvoted 2 times

Nabgre Highly Voted 1 year, 11 months ago

Selected Answer: B

Given response is not correct. The right response is B

upvoted 7 times

dule27 Most Recent 1 year, 6 months ago

Selected Answer: B

B. Windows Hello for Business

upvoted 1 times

Selvaraj_Rajan 1 year, 8 months 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 3 times

Schuiram 1 year, 8 months 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 1 year, 9 months ago

Windows Hello is just the first step to authenticate a User so the answer should be "voice".

upvoted 2 times

Ruslan23 1 year, 9 months 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 1 year, 10 months 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 3 times

Tony416 4 months ago

Where did you read about a landline available in this scenario?

upvoted 1 times

Zak366 1 year, 10 months 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 1 year, 11 months ago

Selected Answer: B

Windows Hello for Business

upvoted 3 times

Oknip 1 year, 11 months ago

Selected Answer: B

Windows Hello for Business

upvoted 2 times

ydecac 1 year, 11 months ago

Selected Answer: B

mobile phone connectivity = No Voice

upvoted 3 times

chikorita 1 year, 9 months ago

upvote maxxxxxxxxxxx

upvoted 1 times

Halwagy 1 year, 11 months ago

Selected Answer: B

Windows Hello for Business

upvoted 2 times

Question #40 *Topic 2*

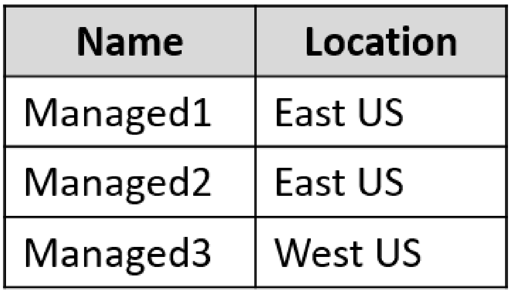
HOTSPOT

-

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.



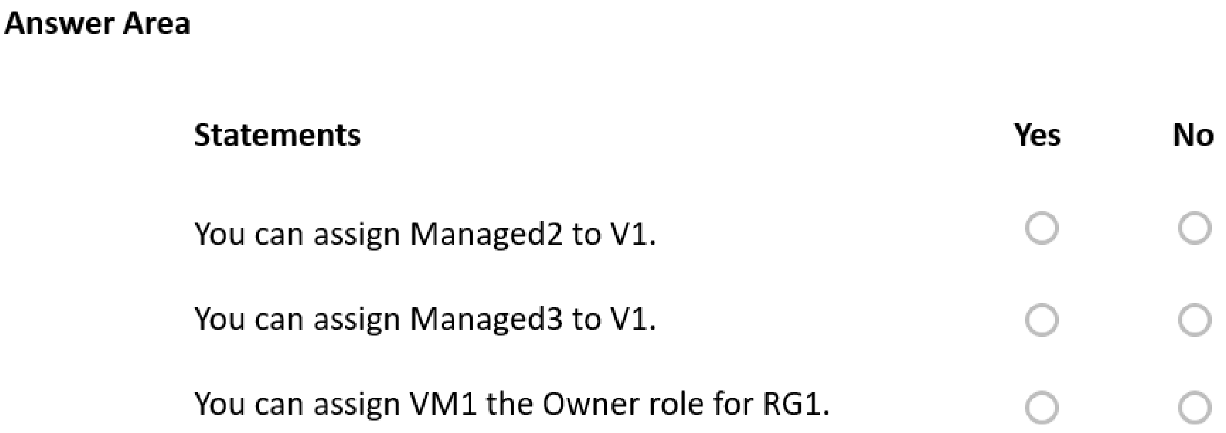
Name	Location
Managed1	East US
Managed2	East US
Managed3	West US

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.

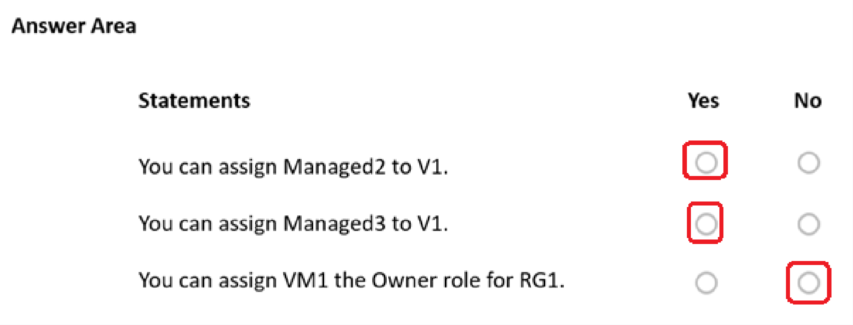
NOTE: Each correct selection is worth one point.



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.	○	○

Suggested Answer:



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.	○	[✓ ○]

⊟ **Markus** Highly Voted 1 year, 5 months ago

YYN.
You can use user assigned managed identities in more than one Azure region.
upvoted 17 times

wooyourdaddy 1 year, 5 months 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 6 times

0byte Highly Voted 8 months, 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 11 times

Nyamnyam 8 months 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

RemmyT Most Recent 3 weeks, 2 days ago
Yes Yes No

VM1 can be assigned the Owner role for RG1 but only with System-assigned managed identity enabled.

If System-assigned managed identity is enabld the role can be assigned to VM directly or to the System-assigned managed identity associated with VM1.

In both cases we only can see the ID of system identity.
upvoted 1 times

RemmyT 3 weeks, 1 day ago
NO
System-assigned managed identity: Disabled
upvoted 1 times

AK_1234 8 months, 3 weeks ago
- Y
- Y
- N
upvoted 2 times

EmnCours 10 months, 3 weeks ago
YES
YES
YES
upvoted 1 times

nils241 11 months, 1 week 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 1 year 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 1 year ago

YES
YES
YES

upvoted 1 times

ITAdmin2019 1 year, 1 month 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 1 year, 3 months 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 3 times

nils241 11 months, 1 week ago

You can add "user assigned identitys" without enable "system assigned" on the VM

upvoted 1 times

chikorita 1 year, 3 months ago

i feel the same too

upvoted 1 times

cris_exam 1 year, 3 months 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 1 year, 3 months ago

can anyone help me understand why 3rd box is marked as NO?
i mean it doesnt 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 1 year, 4 months 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

⊟ **hieverybody** 1 year, 5 months ago

I believe VM1 should be Managed 1 here. So answer is No.

upvoted 1 times

⊟ **natazar** 1 year, 5 months ago

I think it should be YNN

upvoted 1 times

⊟ **kevin_office** 1 year, 5 months 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!

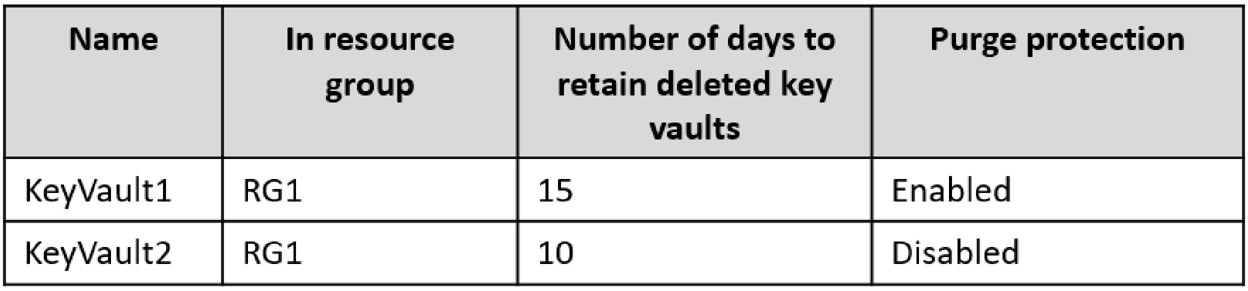
upvoted 49 times

Question #41 *Topic 2*

HOTSPOT

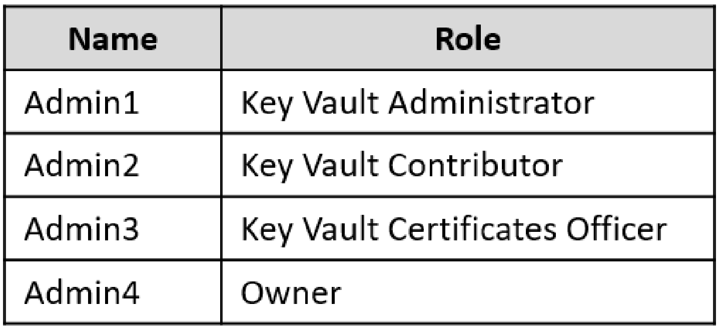
-

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.



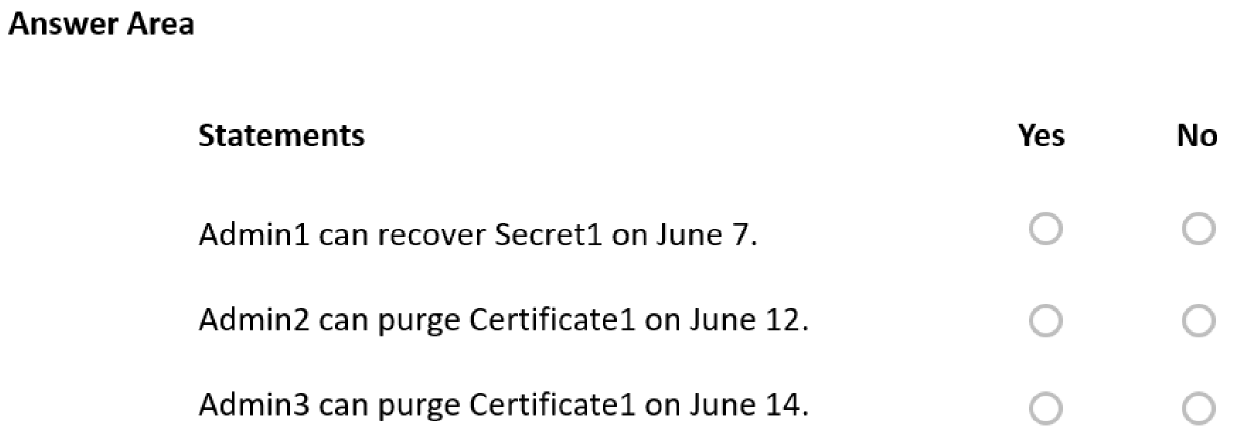
Name	Role
Admin1	Key Vault Administrator
Admin2	Key Vault Contributor
Admin3	Key Vault Certificates Officer
Admin4	Owner

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.

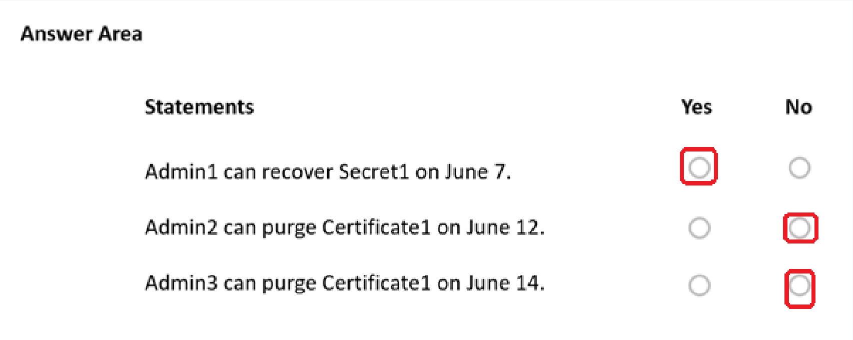
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Admin1 can recover Secret1 on June 7.	○	○
Admin2 can purge Certificate1 on June 12.	○	○
Admin3 can purge Certificate1 on June 14.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
Admin1 can recover Secret1 on June 7.	[✓ ○]	○
Admin2 can purge Certificate1 on June 12.	○	[✓ ○]
Admin3 can purge Certificate1 on June 14.	○	[✓ ○]

wsrudmen Highly Voted 11 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 19 times

Holii 6 months, 3 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 6 months, 3 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 11 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 5 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 3 times

EmnCours 5 months, 2 weeks ago

Is correct
Y
N
N

Generally, only the subscription owner will be able to purge a key vault.

upvoted 3 times

dule27 6 months, 2 weeks ago

YES
NO
NO

upvoted 1 times

⊟ **OK2020** 7 months ago

https://learn.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview

upvoted 2 times

⊟ **OK2020** 7 months ago

https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli

upvoted 1 times

Question #42 *Topic 2*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

ThotSlayer69 Highly Voted 👍 1 year, 5 months 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 23 times

Halwagy Highly Voted 👍 1 year, 5 months ago

Selected Answer: D

Correct

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

upvoted 5 times

emartiy Most Recent ⏲ 3 months, 1 week ago

Selected Answer: D

@ThotSlayer69 shared excellent information.. Please get reference that list.... And and and.. think about difference between User Risk and Risky Sign-in topics..

User Risk : Account base risks. It may be compromised..
Sign-in Risk: Login attempts may come from malicious IP or sources based on collected signals..

upvoted 1 times

AK_1234 8 months, 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 11 months, 2 weeks ago

Selected Answer: D

D. Azure AD threat intelligence

upvoted 1 times

dule27 1 year ago

Selected Answer: D

D. Azure AD threat intelligence

upvoted 1 times

ShoaibPKDXB 1 year, 1 month ago

Selected Answer: D

D correct

upvoted 1 times

wsrudmen 1 year, 5 months ago

Selected Answer: D

Correct

upvoted 2 times

Question #43 *Topic 2*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

Guestie Highly Voted 👍 1 year, 4 months 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 10 times

Matt19 Most Recent ⏲ 1 week, 6 days ago

Selected Answer: D

D - You cannot have MS Authenticator app / Code selected when you have only 1 method to set for SSPR (greyed out now while you configure SSPR). One needs to select at least 2 methods for Authenticator app.

upvoted 1 times

Nyamnyam 8 months 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 2 times

roman_cat 10 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 9 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 11 months, 2 weeks ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

⊟ **dule27** 1 year ago

Selected Answer: B

B. a mobile app code

upvoted 1 times

⊟ **JN_311** 1 year 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 3 times

⊟ **roman_cat** 10 months, 2 weeks ago

question is asking for users, not administrators

upvoted 1 times

⊟ **BigDogAG** 3 months, 2 weeks ago

Yes but in this instance the admin is who put the requirements in place.

upvoted 1 times

⊟ **kanew** 1 year, 1 month 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 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** 1 year, 3 months ago

Selected Answer: B

B is Correct
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks

upvoted 1 times

⊟ **divyakanth** 1 year, 5 months ago

Selected Answer: B

correct explanation by wooyou

upvoted 1 times

⊟ **Halwagy** 1 year, 5 months ago

D also a valid option

upvoted 1 times

⊟ **kevin_office** 1 year, 5 months ago

yeah but D comes when B is not available

upvoted 2 times

⊟ **wooyourdaddy** 1 year, 5 months 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

Question #44 Topic 2

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

Suggested Answer: *A*

Community vote distribution

A (100%)

BRoald Highly Voted 11 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

curtmcgirt 3 weeks, 5 days ago

sign-in risk is correct, but isn't 'leaked credentials' (included in your list of examples) the poster child for user risk, not sign-in risk?

upvoted 5 times

EmnCours Most Recent 5 months, 2 weeks ago

Selected Answer: A

A. a sign-in risk policy

upvoted 1 times

dule27 6 months, 2 weeks ago

Selected Answer: A

A. a sign-in risk policy

upvoted 1 times

ShoaibPKDXB 7 months, 3 weeks ago

Selected Answer: A

A correct

upvoted 1 times

rajbne 8 months, 1 week ago

its "new" tenancy so could be C as well

upvoted 1 times

bda92b3 9 months, 3 weeks ago

Correct

upvoted 1 times

Jotest 11 months, 2 weeks ago

sign-in risk policy seems to be correct

upvoted 2 times

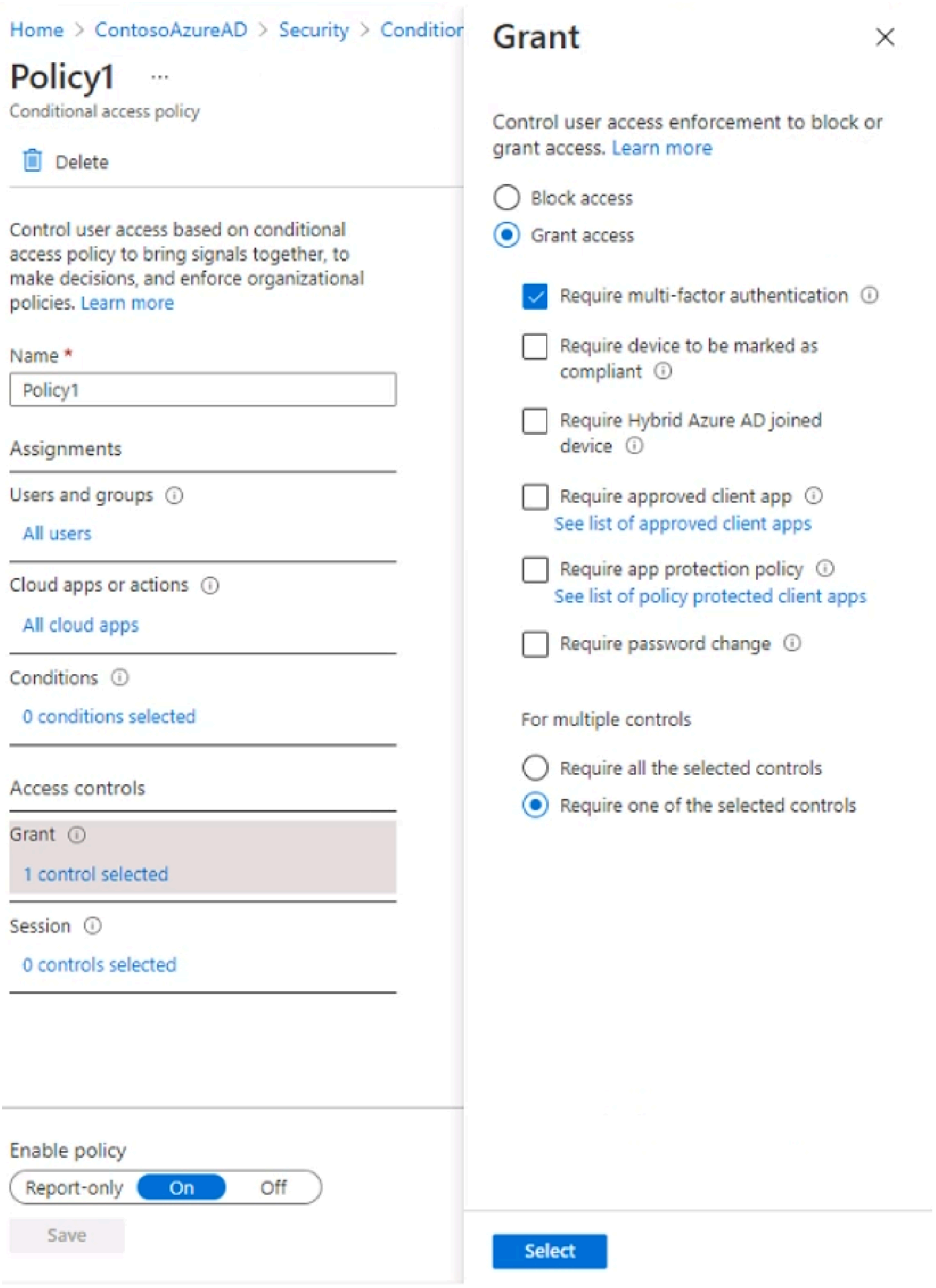
Question #45 *Topic 2*

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 > Conditior

Policy1 ...

Conditional access policy

Delete

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 ⓘ

All users

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Enable policy

Report-only | **On** | Off

Save

Grant ✕

Control user access enforcement to block or grant access. Learn more

○ Block access

● Grant access

☑ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ
See list of approved client apps

☐ Require app protection policy ⓘ
See list of policy protected client apps

☐ Require password change ⓘ

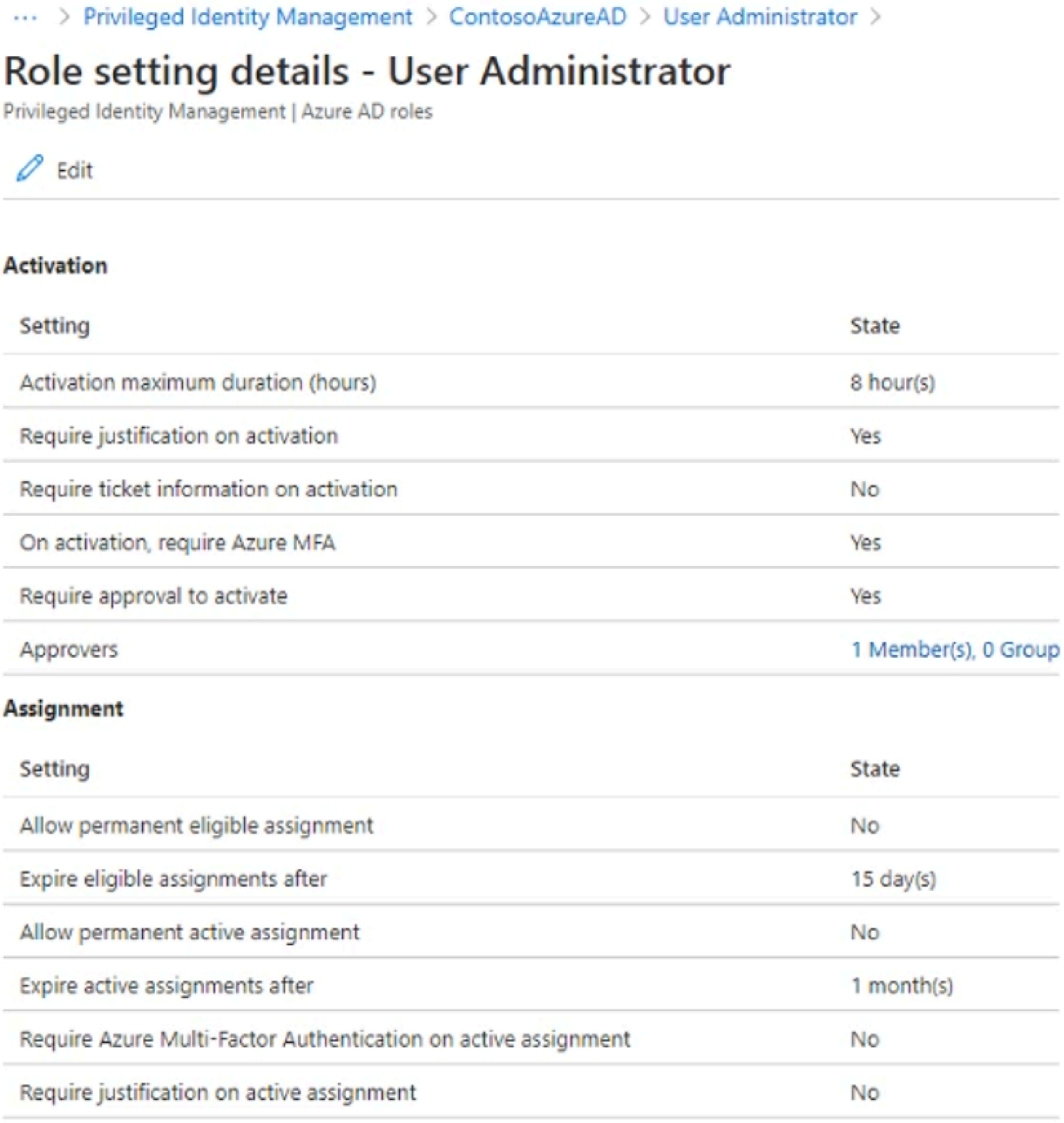
For multiple controls

○ Require all the selected controls

● Require one of the selected controls

Select

You view the User administrator role settings as shown in the Role setting details exhibit. (Click the Role setting details tab.)


… > Privileged Identity Management > ContosoAzureAD > User Administrator >

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

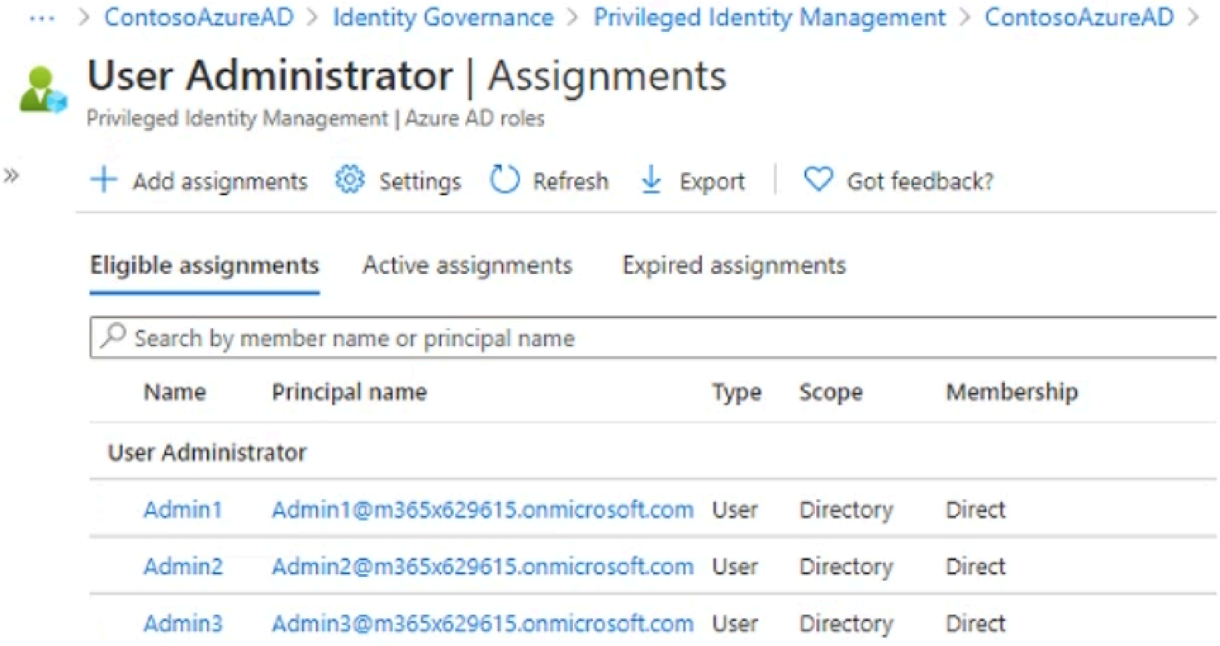
Activation

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.)


… > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

User Administrator | Assignments

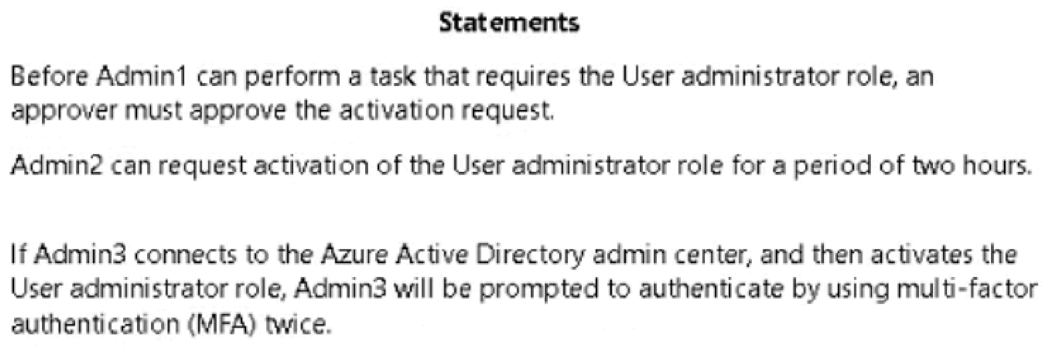
Privileged Identity Management | Azure AD roles

»
+ 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	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

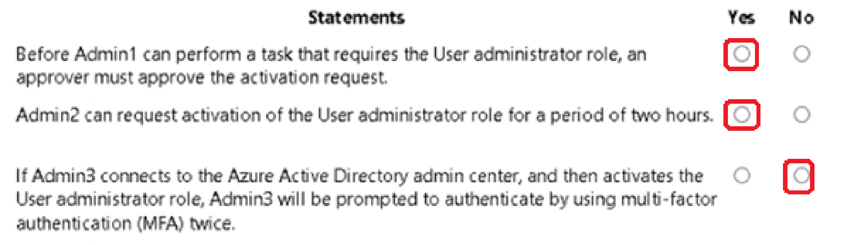
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

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.	○	○
Admin2 can request activation of the User administrator role for a period of two hours.	○	○
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.	○	○

Suggested Answer:



Statements	Yes	No
Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.	[✓ ○]	○
Admin2 can request activation of the User administrator role for a period of two hours.	[✓ ○]	○
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.	○	[✓ ○]

⊟ **Halwagy** Highly Voted 1 year, 11 months ago

Correct

upvoted 17 times

⊟ **SFAY** 11 months, 1 week ago

Tested and verified in the Lab.

YYN

upvoted 3 times

⊟ **chikorita** Highly Voted 1 year, 9 months 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 7 times

⊟ **cris_exam** 1 year, 9 months ago

I would also go with YYY as you explained, it makes sense.

upvoted 1 times

⊟ **cris_exam** 1 year, 9 months ago

take back what I said - Require MFA on Active assignment is set to NO. so it's YYN.

upvoted 3 times

⊟ **chikorita** 1 year, 9 months 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** 1 year, 6 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 5 times

⊟ **Holii** 1 year, 6 months 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 9 times

Ammyg 3 months, 3 weeks ago

Yes, its menitioned in this doc.
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings#on-activation-require-multi-factor-authentication

upvoted 1 times

Siraf Most Recent 1 year ago

Correct Answer is: Yes/Yes/No

On activation, require multifactor authentication:
You can require users who are eligible for a role to prove who they are by using the multifactor authentication feature in Microsoft Entra ID before they can activate. Multifactor authentication helps safeguard access to data and applications. It provides another layer of security by using a second form of authentication.

Users might not be prompted for multifactor authentication if they authenticated with strong credentials or provided multifactor authentication earlier in the session.

The word "might" implies that Yes/Yes/Yes can also be accepted as answer.

https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings#on-activation-require-multi-factor-authentication

upvoted 4 times

Nivos23 1 year, 2 months ago

Correct

upvoted 1 times

EmnCours 1 year, 5 months ago

Yes Yes No

upvoted 3 times

Heshan 1 year, 5 months ago

On the exam, 09/07/2023

upvoted 2 times

dule27 1 year, 6 months ago

Yes
Yes
No

upvoted 3 times

217f3c9 1 year, 8 months 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 6 times

Holii 1 year, 6 months ago

Tested and confirmed. YYN.

upvoted 1 times

f2bf85a 1 year, 8 months 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

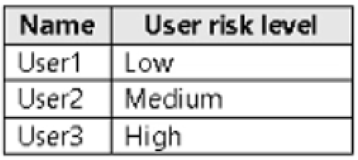
upvoted 4 times

Question #46 *Topic 2*

HOTSPOT

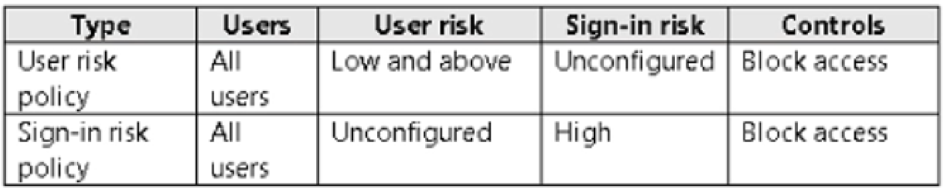
-

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



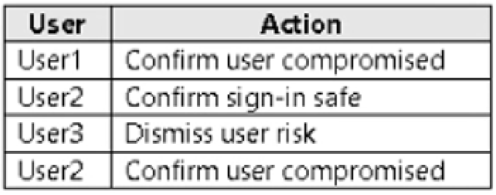
Name	User risk level
User1	Low
User2	Medium
User3	High

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

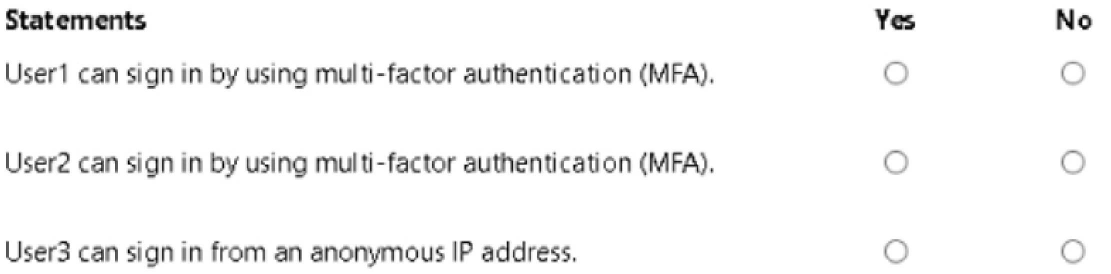
You review the Risky users report and the Risky sign-ins report and perform actions for each user as shown in the following table.



User	Action
User1	Confirm user compromised
User2	Confirm sign-in safe
User3	Dismiss user risk
User2	Confirm user compromised

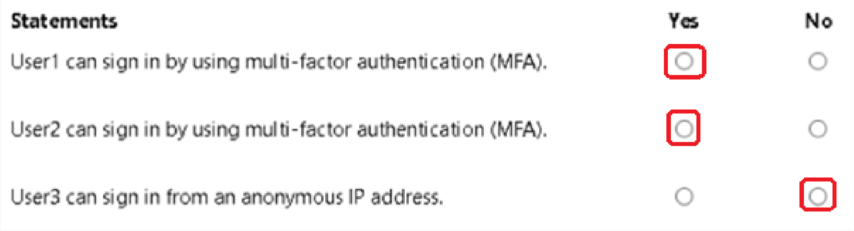
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Statements	Yes	No
User1 can sign in by using multi-factor authentication (MFA).	○	○
User2 can sign in by using multi-factor authentication (MFA).	○	○
User3 can sign in from an anonymous IP address.	○	○

Suggested Answer:



Statements	Yes	No
User1 can sign in by using multi-factor authentication (MFA).	[✓ ○]	○
User2 can sign in by using multi-factor authentication (MFA).	[✓ ○]	○
User3 can sign in from an anonymous IP address.	○	[✓ ○]

doch Highly Voted 1 year, 11 months 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 29 times

⊟ **ExamStudy68** 1 year, 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 6 times

⊟ **c18525f** 1 year, 10 months 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 2 times

⊟ **ThotSlayer69** Highly Voted 1 year, 11 months 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 19 times

⊟ **Nail** 2 months, 1 week ago
Agreed. Link for last answer: "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.
upvoted 1 times

⊟ **naveenbio** Most Recent 3 weeks, 5 days ago
No. Compromised user1, regardless of risk level.
No. Compromised user2, regardless of risk level.
No.User 3, High sign-in risk due to anonymous IP, even with dismissed user risk.
upvoted 1 times

⊟ **RemmyT** 7 months ago
No No No

Made a High Risk Sign policy that block access.
Tried to login from TOR browser with two different accounts.

Error message:
You cannot access this right now
Your sign-in was successful, but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app or location that is restricted by your admin.

Anonymous IP address
Calculated in real-time. This risk detection type indicates sign-ins from an anonymous IP address (for example, Tor browser or anonymous VPN). These IP addresses are typically used by actors who want to hide their sign-in information (IP address, location, device, and so on) for potentially malicious intent.
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#anonymous-ip-address

upvoted 2 times

⊟ **ItzVerified** 8 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 + User 3 has the following action performed on his account : "Dismiss User Risk"

upvoted 1 times

⊟ **ANiMOSiTYOP** 10 months, 1 week ago

No, No, Yes

User1: The User Risk Policy for User1 specifies the User Risk as "Low and above" and the control as "Block Access". Therefore, User1 would not be allowed to sign in even via multi-factor authentication (MFA) since the policy is set to block access.

User2: The User Risk Policy for User2 specifies the User Risk as "Low and above" and once the user is confirmed compromised, the policy as "Block Access" applies. Hence, User2 would not be allowed to sign in even via MFA after being confirmed as compromised.

User3: The User Risk for User3 is dismissed. This means User3 can sign in from any location including anonymously. In case the Sign-in Risk becomes High, then User3 would not be allowed to sign in as per the Sign-in Risk Policy.

upvoted 6 times

⊟ **Shena2021** 1 year, 3 months 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 9 times

⊟ **curtmcgirt** 1 year ago

#2 is No, but not because of "confirm sign in safe." that sign in confirmation is only for the sign-in, and doesn't change user2's *user risk* from medium, and (user risk low and above) is (blocked), even before we confirm user2 compromised two steps after confirming the sign-in safe.

upvoted 1 times

⊟ **Nivos23** 1 year, 2 months ago

I agree, thanks for the explanation

N

N

y

upvoted 2 times

⊟ **Nivos300** 1 year, 1 month ago

I agree

N

N

Y

upvoted 2 times

⊟ **EmnCours** 1 year, 4 months ago

N

N

Y

upvoted 1 times

⊟ **Tweety1972** 1 year, 5 months 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 4 times

⊟ **b233f0a** 1 year, 6 months 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 dfeedback Identity Pritection 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 4 times

⊟ **dule27** 1 year, 6 months ago
No
No
Yes
upvoted 2 times

⊟ **wsrudmen** 1 year, 11 months 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 7 times

⊟ **topzz** 1 year, 9 months ago
agree with this
upvoted 1 times

⊟ **dobriv** 1 year, 10 months ago
OK, but Anonymous IP is Sign-in Risk, not User Risk, so I think the third should be NO.
upvoted 2 times

⊟ **dobriv** 1 year, 8 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 2 times

⊟ **Halwagy** 1 year, 11 months ago

the user risk policy is block access

N N Y

upvoted 5 times

Question #47 *Topic 2*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

doch Highly Voted 👍 1 year, 5 months 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 9 times

Halwagy Highly Voted 👍 1 year, 5 months ago

Selected Answer: D

Correct Answer given

upvoted 5 times

baz Most Recent ⏱ 5 months, 1 week ago

D. Application Administrator - other roles can manage Application Proxy settings

upvoted 2 times

Shena2021 9 months, 3 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 3 times

EmnCours 10 months, 3 weeks ago

Selected Answer: D

D. Application administrator

upvoted 2 times

dule27 1 year ago

Selected Answer: D

D. Application administrator

upvoted 2 times

⊟ **dejo** 1 year, 4 months 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** 7 months ago

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#application-administrator

upvoted 1 times

⊟ **dobriv** 1 year, 4 months 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 12 times

Question #48 *Topic 2*

DRAG DROP

-

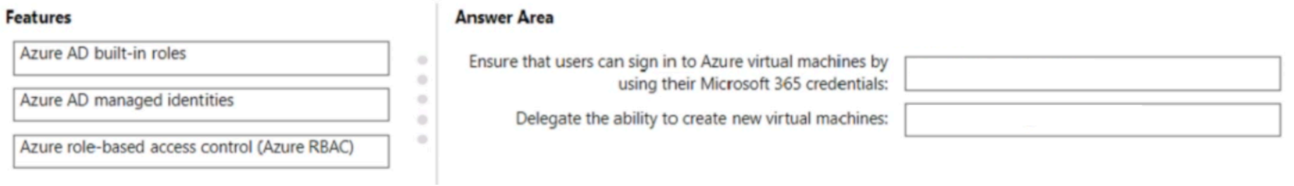
You have a Microsoft 365 E5 subscription and an Azure subscription.

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

Azure AD built-in roles

Azure AD managed identities

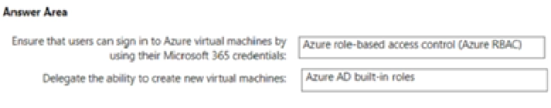
Azure role-based access control (Azure RBAC)

Answer Area

Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials:

Delegate the ability to create new virtual machines:

Suggested Answer:



Answer Area

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 1 year, 8 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 21 times

mancio Highly Voted 1 year, 7 months 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 7 times

Nail 2 months, 1 week ago

Careful. Option 2 is really just Azure RBAC as well. The link for Azure AD built-in roles is this: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference BUT, the answer is Azure RBAC for BOTH.

upvoted 1 times

Hull 1 year, 4 months 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 3 times

RemmyT Most Recent 6 months, 3 weeks ago

RBAC : Virtual Machine User Login

RBAC : VM Contributor

upvoted 1 times

emartiy 9 months, 1 week ago

Both are Azure role-basd access control (RBAC)

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#role-based-access-control-administrator-preview

upvoted 1 times

⊟ **emartiy** 9 months, 1 week ago

What is the difference between Azure roles and Azure AD roles?

1 Answer. Assigned roles are Azure AD administrator roles, for accessing Azure AD and other Microsoft 365 platforms such as Exchange and SharePoint. Azure role assignments (may also be referred to as Azure RBAC roles) are for accessing Azure resources such as virtual machines, storage accounts, subscriptions, etc.11 Kas 2022

upvoted 1 times

⊟ **Foggy31** 1 year, 2 months 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** 1 year, 7 months 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** 1 year, 8 months 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** 1 year, 11 months 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** 1 year, 10 months 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** 1 year, 11 months 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** 1 year, 11 months 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 3 times

⊟ **Halwagy** 1 year, 11 months ago

Azure AD managed Identities

Azure Role-based access control

upvoted 5 times

⊟ **Halwagy** 1 year, 11 months 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 13 times

Question #49 *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 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

Suggested Answer: *D*

Community vote distribution

D (100%)

⊟ **Ikazimirs** Highly Voted 5 months, 2 weeks ago

why is this question repeated so many times - this is the 5th or 6th time im seeing this.

upvoted 11 times

⊟ **Anonymouse1312** Highly Voted 2 months, 3 weeks ago

Hello? Is it this question youre looking for?

upvoted 5 times

⊟ **roman_cat** Most Recent 4 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** 4 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** 5 months, 1 week ago

Selected Answer: D

Correct Answer: D

upvoted 1 times

⊟ **dule27** 6 months, 2 weeks ago

Selected Answer: D

D. Windows Hello for Business

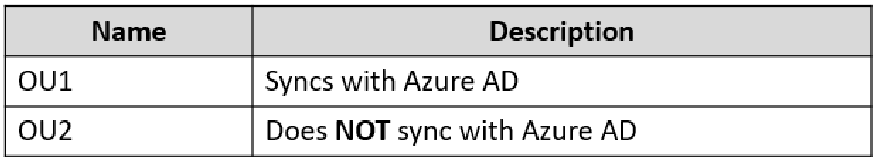
upvoted 3 times

Question #50 *Topic 2*

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.

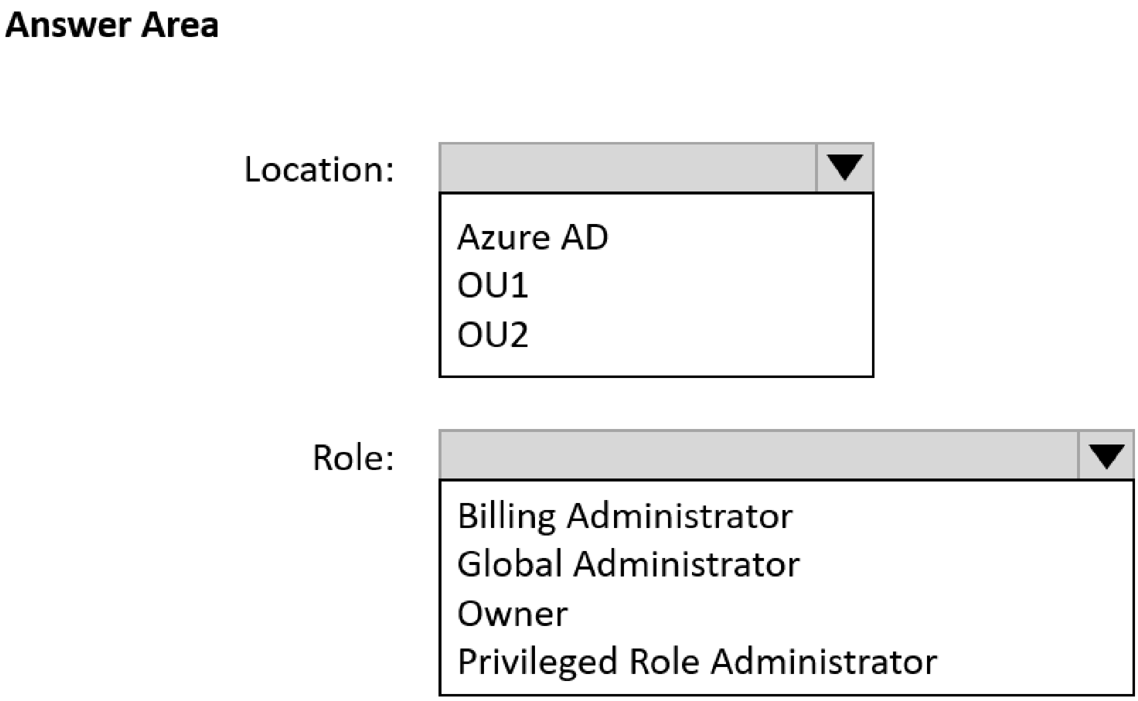


Name	Description
OU1	Syncs with Azure AD
OU2	Does **NOT** sync with Azure AD

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

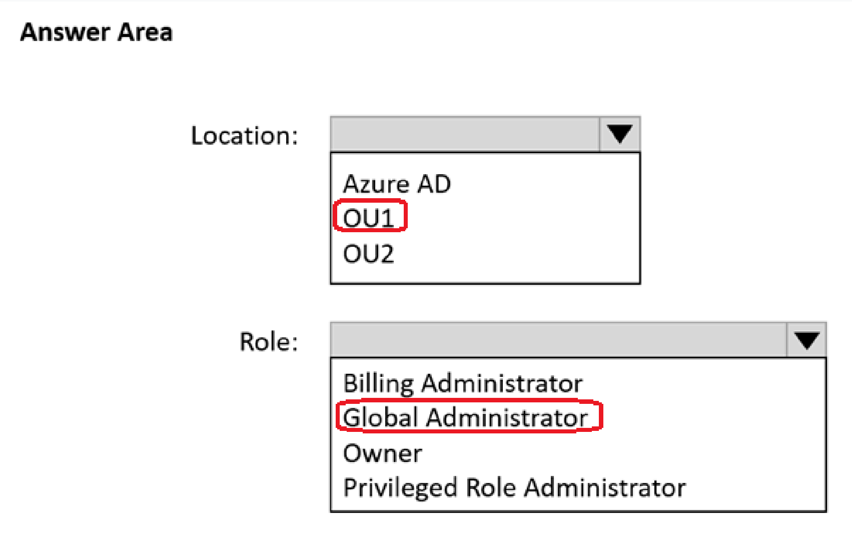
Location:

Azure AD
OU1
OU2

Role:

Billing Administrator
Global Administrator
Owner
Privileged Role Administrator

Suggested Answer:



Answer Area

Location:

Azure AD
[✓ OU1]
OU2

Role:

Billing Administrator
[✓ Global Administrator]
Owner
Privileged Role Administrator

DoMing Highly Voted 1 year, 3 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 39 times

topzz 1 year, 3 months ago

break-glass account = emergency access account

upvoted 6 times

ANiMOSiTYOP 4 months ago

Location: Azure AD

Role: Global Administrator

Explanation: A break-glass account is a highly privileged account meant to be used in emergency situations where normal administration cannot be performed. As such, it should be created directly in Azure AD so it's not dependent on the on-premises AD DS domain. The Global Administrator role will provide the broadest level of permissions to address potential emergency issues. Remember, such accounts should be protected with strong, complex passwords, ideally stored securely off-line, and should only be used for temporary and emergency purposes.

upvoted 2 times

kmk_01 Highly Voted 1 year, 2 months 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 7 times

HartMS Most Recent 3 months ago

Azure AD and Global Admin

upvoted 2 times

emartiy 3 months, 1 week ago

I searched this question and found exact and only one correct answer..

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. Link: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access#create-emergency-access-accounts

Azure AD and Global Admin... chose these options and gain point from exam :)

upvoted 3 times

kijken 7 months, 2 weeks ago

Sorry, but a break glass account for what? For Azure or for on prem AD?

upvoted 1 times

⊟ **norkis97** 8 months ago

Break glass account must be only azure ad account !

Break glass account also must be Global Administrator

upvoted 4 times

⊟ **sherifhamed** 9 months, 2 weeks 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 3 times

⊟ **sgfurgi** 10 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** 10 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** 11 months, 1 week ago

AzureAD and Global Admin

upvoted 2 times

⊟ **dule27** 1 year ago

Azure AD

Global Admin

Break-glass account has emergency access

upvoted 3 times

⊟ **caef525** 1 year, 2 months 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

Question #51 Topic 2

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.

Suggested Answer: *B*

Community vote distribution

B (100%)

kmk_01 Highly Voted 👍 1 year, 2 months 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 8 times

emartiy Most Recent 🕒 3 months, 1 week ago

Selected Answer: B

Access Packages

upvoted 2 times

EmnCours 11 months, 1 week ago

Selected Answer: B

B. Create an access package.

upvoted 1 times

dule27 1 year ago

Selected Answer: B

B. Create an access package.

upvoted 1 times

Question #52 Topic 2

HOTSPOT

-

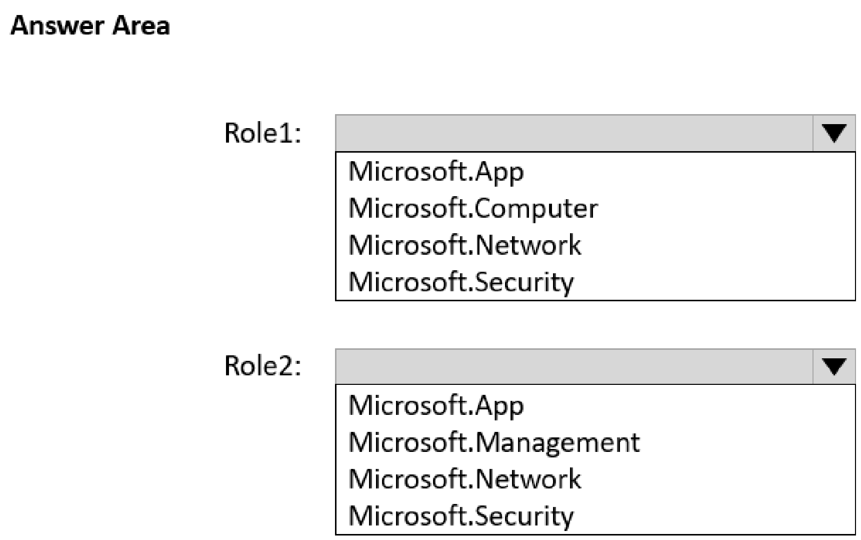
You have an Azure subscription.

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.

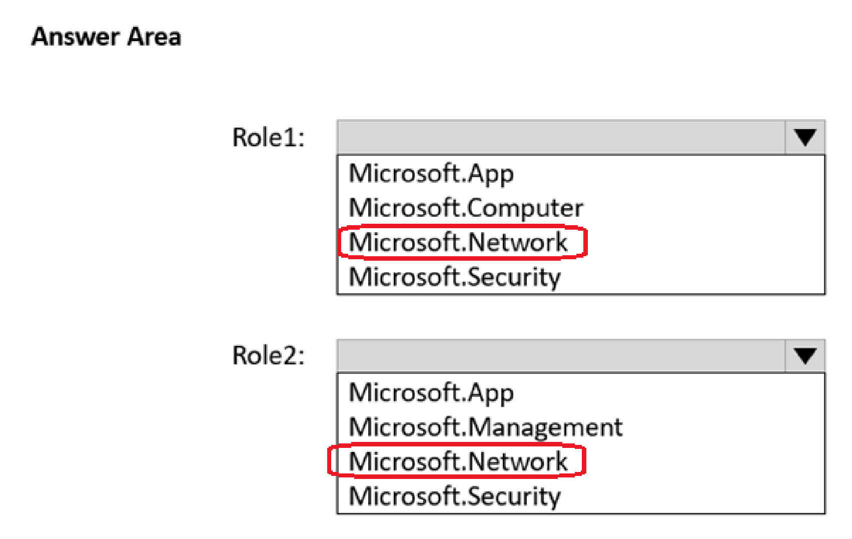


Answer Area

Role1: ▼
Microsoft.App
Microsoft.Computer
Microsoft.Network
Microsoft.Security

Role2: ▼
Microsoft.App
Microsoft.Management
Microsoft.Network
Microsoft.Security

Suggested Answer:



Answer Area

Role1: ▼
Microsoft.App
Microsoft.Computer
[✓ Microsoft.Network]
Microsoft.Security

Role2: ▼
Microsoft.App
Microsoft.Management
[✓ Microsoft.Network]
Microsoft.Security

⊟ DoMing Highly Voted 1 year, 9 months ago
Correct
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork
upvoted 16 times

⊟ Nail 2 months, 1 week ago
Correct. Also: https://learn.microsoft.com/en-us/azure/role-based-access-control/permissions/networking#microsoftnetwork .
"Microsoft.Network/azurefirewalls/write" "Microsoft.Network/applicationSecurityGroups/write"

upvoted 1 times

⊟ **kmk_01** 1 year, 8 months ago

Thanks for providing the link.

upvoted 3 times

⊟ **dvmhike** Most Recent 1 month, 2 weeks ago

This is Correct

https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork

upvoted 1 times

⊟ **EmnCours** 1 year, 5 months ago

Role1: Microsoft.Network

Role2: Microsoft.Network

upvoted 2 times

⊟ **dule27** 1 year, 6 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

Suggested Answer: *D*

Community vote distribution

D (89%) 11%

⊟ **sbettani** Highly Voted 1 year, 7 months ago

wiithout internet ... D? We answer to 10 question with app password. Then B

upvoted 5 times

⊟ **Phax** Most Recent 2 months ago

Answer should be B, theres no internet and phone connectivity, how can the app be working. WHile the only connectivity iniated was the wired connection.

upvoted 1 times

⊟ **emartiy** 9 months, 1 week ago

Selected Answer: D

Adding an authenticator app like Microsoft Authenticator can provide easier verification, and also allows you to sign in even if the verification device is offline.

https://support.microsoft.com/en-us/account-billing/microsoft-account-security-info-verification-codes-bf2505ca-cae5-c5b4-77d1-69d3343a5452

upvoted 2 times

⊟ **aks_exam** 11 months ago

Selected Answer: B

how do you receive verification code without internet...?

i would answer B

upvoted 1 times

⊟ **Tony416** 4 months ago

You don't need Internet Access. It's not a push verification. It's just a Verification Code provided by a Soft Token (App)

upvoted 1 times

⊟ **EmnCours** 1 year, 5 months ago

Selected Answer: D

D. a verification code from the Microsoft Authenticator app

upvoted 1 times

⊟ **dule27** 1 year, 6 months ago

Selected Answer: D

D. a verification code from the Microsoft Authenticator app

upvoted 1 times

ahmedkmicha 1 year, 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 4 times

Question #54

Topic 2

DRAG DROP

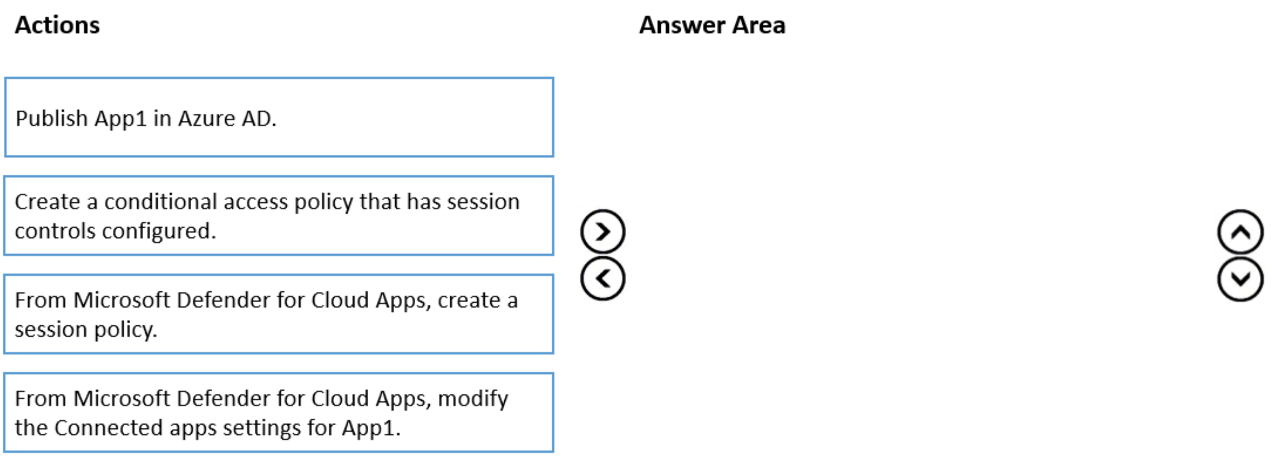
-

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

Publish App1 in Azure AD.

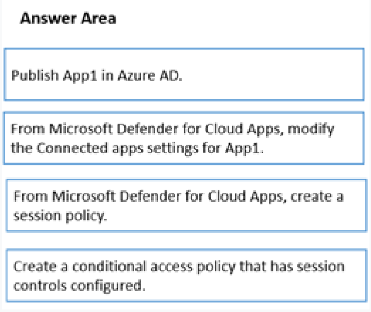
Create a conditional access policy that has session controls configured.

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

Suggested Answer:



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.

DoMing Highly Voted 1 year, 9 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 41 times

HartMS 8 months, 3 weeks ago

correct

upvoted 2 times

hml_2024 Most Recent 4 months ago

To enable real-time session-level monitoring of App1 using Microsoft Defender for Cloud Apps, the actions should be performed in the following order:

Publish App1 in Azure AD.

Create a conditional access policy that has session controls configured.

From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1.

From Microsoft Defender for Cloud Apps, create a session policy.

upvoted 1 times

⊟ **EmnCours** 1 year, 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 2 times

⊟ **dule27** 1 year, 6 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

Question #55 *Topic 2*

HOTSPOT

-

Case Study

-

Overview

-

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

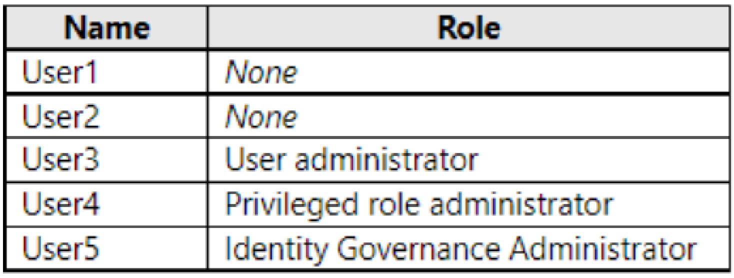
Existing Environment. ADatum Environment

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.

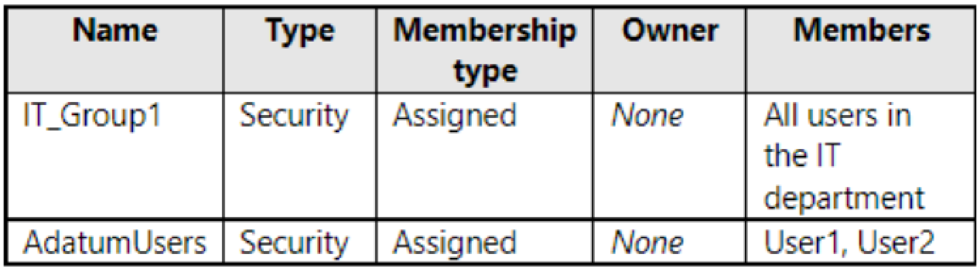
ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

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

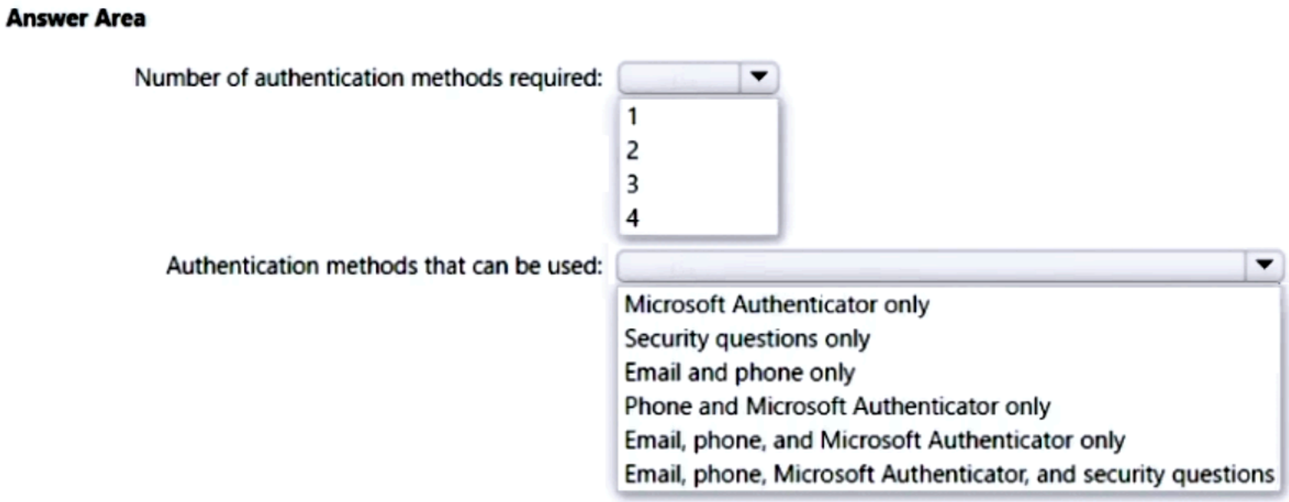
ADatum identifies the following technical requirements:

• 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

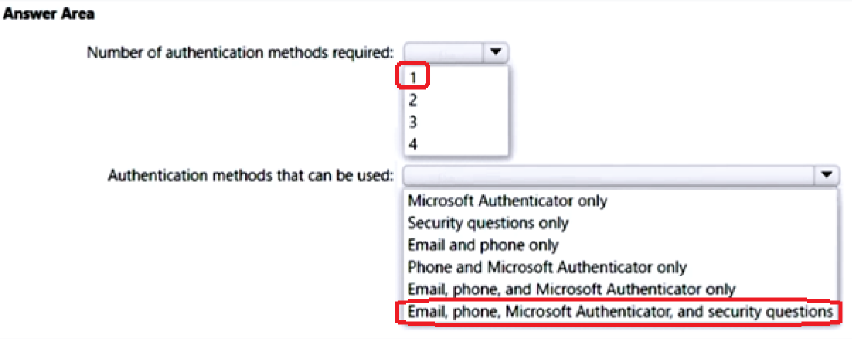
Number of authentication methods required: ▼

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

Suggested Answer:



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]

⊟ **marsot** Highly Voted 1 year, 5 months 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 27 times

⊟ **Shivz0903** 5 months, 1 week ago

It says security defaults are disabled, does this not make a difference?
upvoted 1 times

⊟ **SFAY** 11 months, 2 weeks ago

You have missed the sentence following what you quoted. The full text goes like this - 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.

Therefore, the two gate policy applies to admin roles, is enforced, can't be changed and is independent of the actual policy defined for the users.

Why would you need 2 auth methods when the requirement clearly asks for 1?
upvoted 2 times

⊟ **SFAY** Highly Voted 11 months, 2 weeks ago

I tested and set Auth method as '1' and checked email, phone, MS App Code & security questions as available options for users. However, SSPR presented only one option i.e MS Auth App code for pwd reset. I tested both with a normal user and with 'User Admin' role and the result was same i.e no two gate thing as mentioned in some of the comments.
Therefore, based on my testing and the results I got the answers are '1' & MS App only'. Please test it out yourself before blindly following others.

If you ask why 1 and not 2 auth methods, then please note that the requirement is that:
Users must provide ONE authentication method to reset their password by using SSPR.

If MS Auth is selected as one of the authentication options, then it appears that Azure prefers it over all other possible options.
upvoted 9 times

⊟ **survivor** 1 month, 1 week ago

Exceptions
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 isn't configured (the tenant is using the default *.onmicrosoft.com, which isn't recommended for production use) and Microsoft Entra Connect isn't synchronizing identities.
upvoted 1 times

ANiMOSiTYOP 10 months, 1 week ago
The word "and" in the phrase "Email, Phone, Microsoft Authenticator, and Security Questions" could be potentially misleading. The word "or" would be more appropriate because the users are supposed to choose only one method among these for authentication.

So I'd agree with MS prefers "Microsoft Authenticator only" probably as the best answer.
upvoted 1 times

Arash123 Most Recent 1 month, 2 weeks ago
It has to be 2 methods for admins. This is what I see on Authentication methods blade for SSPR:
These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.
https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy#administrator-password-policy-differences
upvoted 1 times

emartiy 9 months, 1 week ago
1 method since quetion asks for and
Email,Phone,MFA selection can be chosen except Security Questions. Admins can't use it for SSPR.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-security-questions
upvoted 2 times

survivor 1 month, 1 week ago
Exceptions
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 isn't configured (the tenant is using the default *.onmicrosoft.com, which isn't recommended for production use) and Microsoft Entra Connect isn't synchronizing identities.
upvoted 1 times

hw121693 1 year, 5 months ago
I think authen methods should be 2, password + one of those MFA methods
upvoted 1 times

Peeeedor 1 year, 5 months 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 3 times

⊟ **JCkD4Ni3L** 1 year, 2 months ago
You are contradicting yourself :)
upvoted 5 times

⊟ **marsot** 1 year, 5 months 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 7 times

Question #56 *Topic 2*

HOTSPOT

-

Case Study

-

Overview

-

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

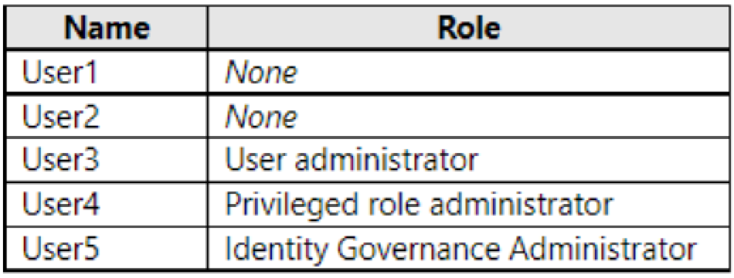
Existing Environment. ADatum Environment

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.

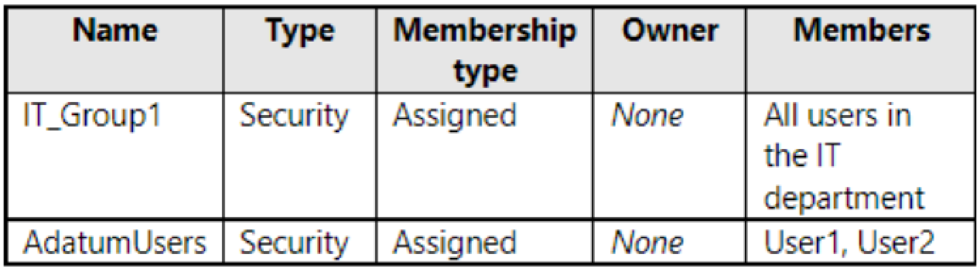
ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

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

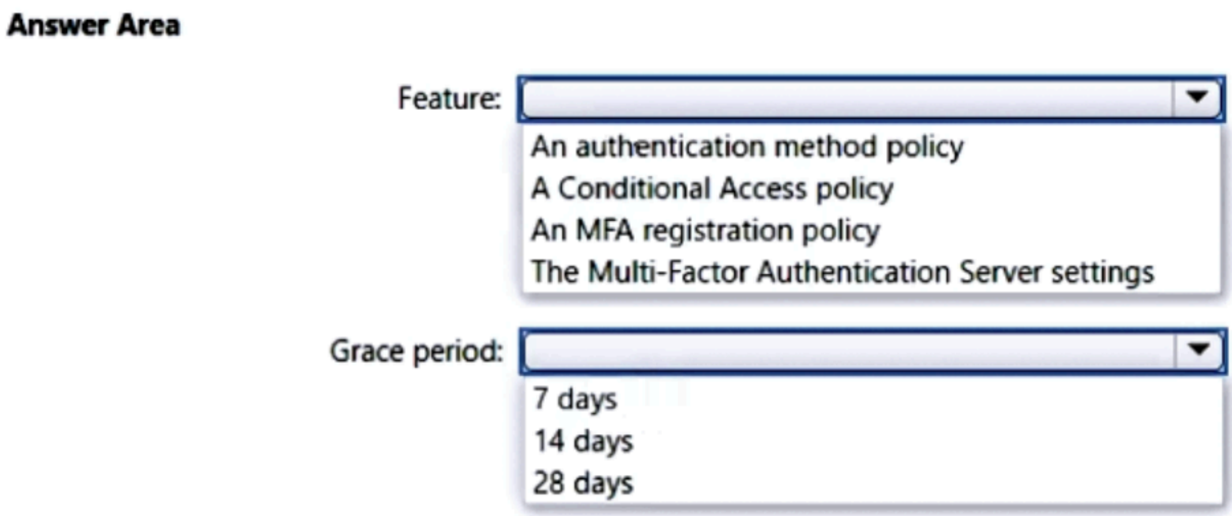
ADatum identifies the following technical requirements:

• 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.

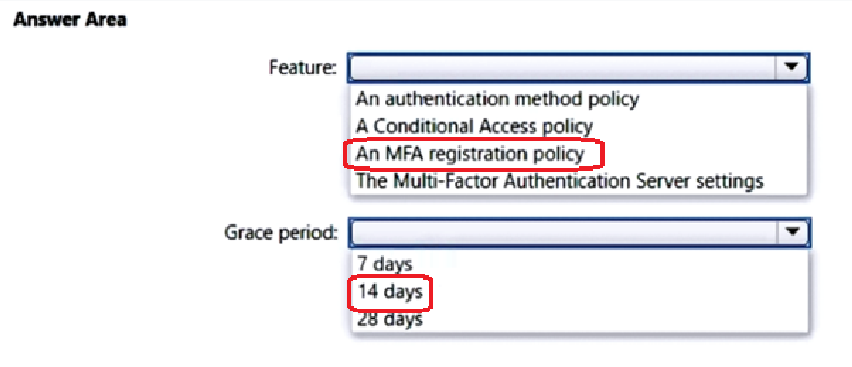


Answer Area

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

Suggested 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

marsot Highly Voted 5 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 11 times

JCkD4Ni3L Highly Voted 2 months, 1 week ago

Answer is Correct !

upvoted 5 times

Question #57 *Topic 2*

DRAG DROP

-

Case Study

-

Overview

-

ADatum Corporation is a consulting company in Montreal.

ADatum recently acquired a Vancouver-based company named Litware, Inc.

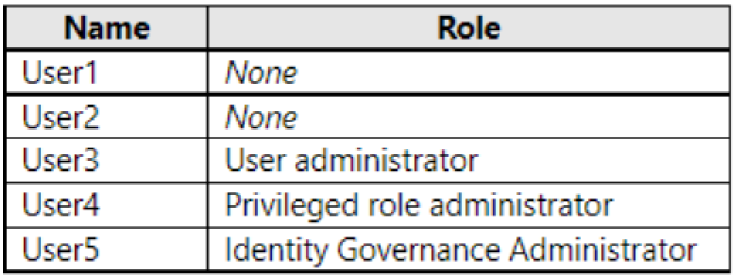
Existing Environment. ADatum Environment

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.

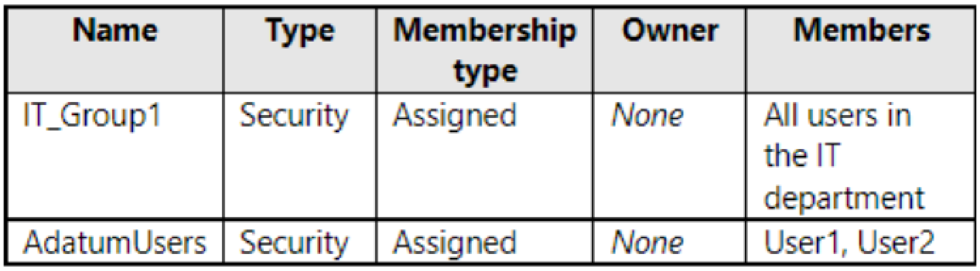
ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

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

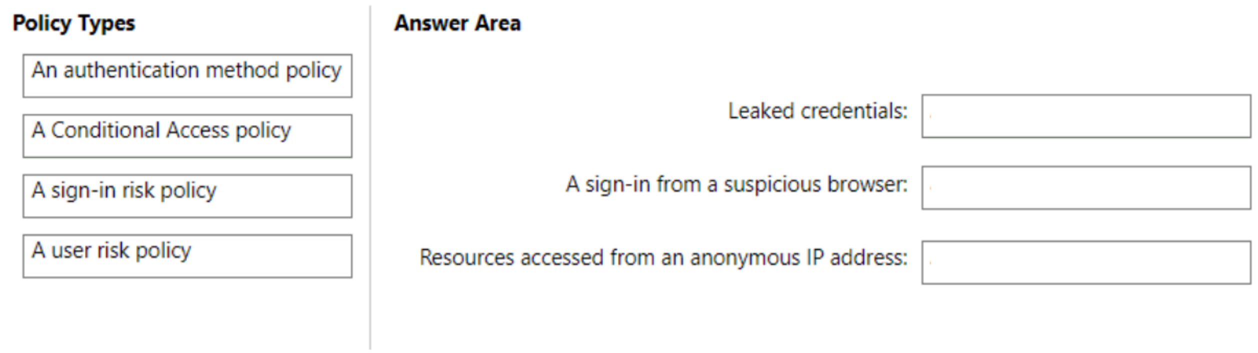
ADatum identifies the following technical requirements:

• 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 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

An authentication method policy

A Conditional Access policy

A sign-in risk policy

A user risk policy

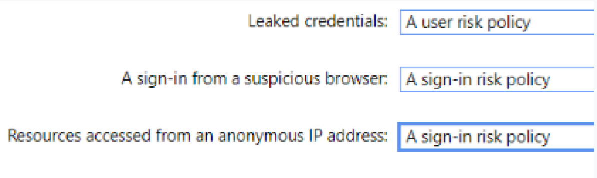
Answer Area

Leaked credentials:

A sign-in from a suspicious browser:

Resources accessed from an anonymous IP address:

Suggested Answer:



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

ACSC Highly Voted 3 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 11 times

thoemes Highly Voted 4 months ago

i think user risk, sign in risk & conditional Access for anonymous IP

upvoted 6 times

1c67a2c Most Recent 5 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 2 months, 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 2 months, 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 asume 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 3 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 3 months, 3 weeks ago

BTW, here's a good video about the subject.
https://youtu.be/zV_MBngLNDo

upvoted 2 times

EmnCours 5 months, 1 week ago

Correct

upvoted 2 times

Question #58 *Topic 2*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

Panama469 5 months, 3 weeks ago

I would agree to check the sign-in logs.
In reality a user can go to security.microsoft.com without an error, they don't have access to much though.
real life... option E: Google the error

upvoted 1 times

emartiy 9 months, 1 week ago

Selected Answer: B

B. sign-in logs (user sign-in failure logs can be reached under user profile > Sign-in logs

upvoted 2 times

ELQUMS 10 months, 1 week ago

Sign-in logs

upvoted 1 times

haazybanj 1 year, 1 month 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

[Removed] 1 year, 2 months ago

Correct , Sign-in Logs for Msft Defender for Cloud Apps

upvoted 1 times

rohitrc8521 1 year, 2 months ago

absolutely correct

upvoted 2 times

ServerBrain 1 year, 4 months ago

Selected Answer: B

Correct

upvoted 3 times

Question #59 *Topic 2*

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.

Suggested Answer: *A*

Community vote distribution

A (83%) D (17%)

Panama469 5 months, 3 weeks ago

Agree. Access Policy which uses conditional access app control.
I see there is also a method with an activity policy but I'm not sure it exactly meets the requirements:

App...equals...'name of app'
Activity - IP address... category...equals... risky
Governance action - suspend user in app

upvoted 2 times

emartiy 9 months, 1 week ago

Selected Answer: A

Create an access policy. based on user risk level!

upvoted 1 times

ELQUMS 10 months, 1 week ago

Access Policy

upvoted 1 times

Nyamnyam 1 year, 1 month 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 confifure Cloud Apps access policy and specify Location, but I cannot specify Yammer as the only target app in scope.

upvoted 1 times

JimboJones99 1 year, 2 months ago

Selected Answer: A

A - Access Policy

upvoted 2 times

Anonymouse1312 1 year, 2 months ago

Selected Answer: D

Anomaly detection
as per:
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy

upvoted 1 times

Anonymouse1312 1 year, 2 months ago

disregard my comment.
Given answer is CORRECT.
Not anomaly detection between that does not prevent users from signing-in! '

upvoted 3 times

ServerBrain 1 year, 4 months ago

Selected Answer: A

correct

upvoted 2 times

1c67a2c 1 year, 5 months ago

seems correct https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad

upvoted 1 times

Anonymouse1312 1 year, 2 months 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

Anonymouse1312 1 year, 2 months ago

disregard my comment.
Given answer is CORRECT.
Not anomaly detection between that does not prevent users from signing-in! '

upvoted 1 times

Question #60

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. SMS

B. email

C. security questions

D. a verification code from the Microsoft Authenticator app

Suggested Answer: *D*

Community vote distribution

D (86%) 14%

ServerBrain Highly Voted 1 year, 4 months ago

Selected Answer: D

i think this is appearing for the 5th time.

upvoted 7 times

NickGhouse Most Recent 1 month, 1 week ago

Selected Answer: D

5th time, if verification code is available that is the answer... otherwise it is email. *shrug*

upvoted 1 times

ELQUMS 10 months, 1 week ago

Verification Code - In Exam

upvoted 2 times

Kronos 11 months ago

Answer is D

upvoted 1 times

MacDanorld 1 year, 1 month ago

Selected Answer: A

The correct answer is A

upvoted 1 times

Question #61 *Topic 2*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

emartiy 3 months, 1 week ago

Selected Answer: D

D. Azure AD threat intedetlligence

Why? A, B, C risk detections are related to Risky Sign-in .. not Risky User..

upvoted 1 times

ELQUMS 4 months, 1 week ago

D - in Exam

upvoted 3 times

ServerBrain 10 months, 1 week ago

Selected Answer: D

corrcet

upvoted 1 times

Charlie33 10 months, 3 weeks ago

Selected Answer: D

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

upvoted 2 times

EmnCours 10 months, 3 weeks ago

Selected Answer: D

Correct Answer: D

upvoted 1 times

Question #62 *Topic 2*

You have a Microsoft Entra tenant.

You need to query risky user activity for the tenant.

How long will the logs of risky user activity be retained?

A. 30 days

B. 60 days

C. 90 days

D. 180 days

Suggested Answer: *A*

Community vote distribution

A (67%) D (33%)

⊟ **Phax** 2 months ago

90 days, logs of risky user activity are usually retained for 90 days...

upvoted 2 times

⊟ **murcao** 2 months ago

The question is not well done, but considering the maximum time is 90 days (Entra P2) I will select the option C
> Microsoft Entra ID Free : 7 days
> Microsoft Entra ID P1: 30 days
> Microsoft Entra ID P2: 90 days

This retention period allows you to monitor and analyze risky user activity over a significant period to ensure security and compliance

More information:
Audit logs
> Microsoft Entra ID Free: Seven days
> Microsoft Entra ID P1: Seven days
> Microsoft Entra ID P2: 30 days

Sign-ins
> Microsoft Entra ID Free: 30 days
> Microsoft Entra ID P1: 30 days
> Microsoft Entra ID P2: 30 days

Microsoft Entra multifactor authentication usage
> Microsoft Entra ID Free: 30 days
> Microsoft Entra ID P1: 30 days
> Microsoft Entra ID P2: 30 days

Based on the link below:
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-reports-data-retention

upvoted 1 times

⊟ **Nail** 2 months, 1 week ago

Selected Answer: C

I'm going with 90. I'm in the portal right now under Identity Protection, Report, Risky Users and I can go back a maximum of 90 days. Almost all of the other questions seem to assume you have P2.

upvoted 3 times

⊟ **Tony416** 3 months, 3 weeks ago

Selected Answer: A

This is a tip found in the MS Book SC-300 Exam Prep:
The risk reports have different log-rotation periods. The Risky Users report tracks risky users since the beginning of time (from the perspective of tenant inception). The Risky Sign-in report tracks with the log rotation period of the sign-in logs (30 days). The Risk Detections report has a log-rotation period of 90 days.

upvoted 2 times

Tony416 4 months ago

Selected Answer: D

This question is entirely nonsensical. I found 90 days. There's no reference to 30 days, even though the log time can be changed.
https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-investigate-risk#how-to-investigate-risky-users

"When administrators select an individual user, the Risky user details pane appears. Risky user details provide information like: user ID, office location, recent risky sign-in, detections not linked to a sign, and risk history. The Risk history tab shows the events that led to a user risk change in the last 90 days."

upvoted 1 times

jarattdavis 5 months, 3 weeks ago

Answer is 90 days.

The Risk history tab also shows all the events that led to a user risk change in the last 90 days. This list includes risk detections that increased the user’
remediation actions that lowered the user’s risk.

Note: Question is not referring to Sign in risk which is 30 days.

https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-investigate-risk#:~:text=The%20Risk%20history%20tab%20also%20shows%20all%20the%20events%20that%20led%20to%20a%20user%20risk%20change%20in%20the

upvoted 1 times

ELQUMS 10 months, 1 week ago

A - in Exam

upvoted 2 times

Sozo 10 months, 2 weeks ago

Selected Answer: A

The retention period for logs of risky user activity in Microsoft Entra varies by report type and license type. For instance, the risky sign-ins report contains filterable data for up to the past 30 days. However, you can retain the audit and sign-in activity data for longer than the default retention period by routing it to an Azure storage account using Azure Monitor.

upvoted 1 times

baz 11 months, 1 week ago

A. The risky sign-ins report contains filterable data for up to the past 30 days (one month)
https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-investigate-risk#risky-users-report

upvoted 4 times

throwaway10188 11 months, 2 weeks ago

This question is trash.

No license specified and even if it did Risky User 'Activity' is retained until the end of time/resolved.

upvoted 3 times

throwaway10188 11 months, 2 weeks ago

https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-reports-data-retention

Risky users No limit No limit No limit
Risky sign-ins 7 days 30 days 90 days
Note

Risky users and workload identities are not deleted until the risk has been remediated.

upvoted 4 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

Suggested Answer: *B*

Community vote distribution

B (100%)

Futfuyfyjfj 1 month, 2 weeks ago

Selected Answer: B

B

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#mobile-app-and-sspr

upvoted 1 times

Siraf 6 months ago

Correct Answer is: B

It is actually the only valid answer in the choices.

upvoted 1 times

Anonymouse1312 8 months, 4 weeks ago

Correct

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#authentication-methods

upvoted 3 times

Question #64 *Topic 2*

HOTSPOT

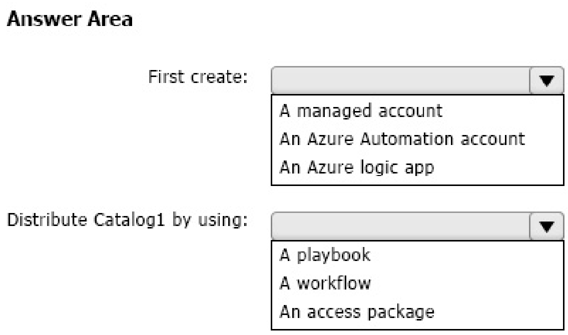
-

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.

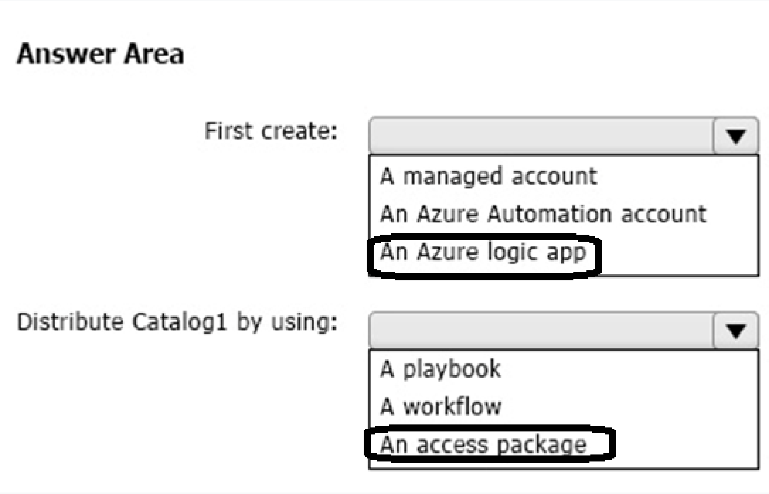


Answer Area

First create: ▼
A managed account
An Azure Automation account
An Azure logic app

Distribute Catalog1 by using: ▼
A playbook
A workflow
An access package

Suggested Answer:



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]

Anonymouse1312 Highly Voted 8 months, 3 weeks ago

Seems to be correct:
https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-logic-apps-integration

upvoted 8 times

OrangeSG 7 months, 4 weeks ago

Demo video on YouTube:
Creating Azure AD Entitlement Management Custom Extensions for Access Packages
https://www.youtube.com/watch?v=tl1GZ_JGMBk&ab_channel=CloudIdentity%7CJefTek

upvoted 3 times

Alcpt 1 month, 4 weeks ago

answer is correct as per MS deployment steps:
https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-logic-apps-integration

upvoted 1 times

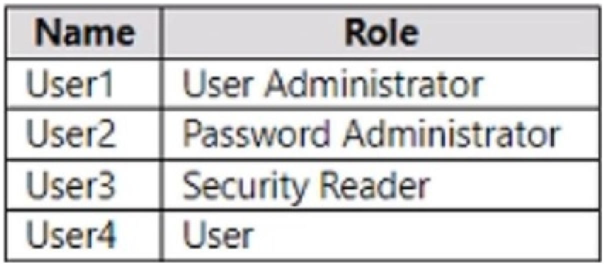
ELQUMS Most Recent 4 months, 1 week ago

Correct answers

upvoted 2 times

Question #65 *Topic 2*

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

Suggested Answer: *B*

Community vote distribution

B (88%) 13%

0byte Highly Voted 8 months, 2 weeks ago

Selected Answer: B

Correct answer.

Basically, some administrative roles, by design can only use strong, two-gate password reset policy, regardles of SSPR settings.

User Administrator and Password Administrator will be always forced to use two methods and cannot use security questions.

Securiry 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 14 times

be9z Most Recent 7 months, 2 weeks 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 2 times

Naya24 7 months, 2 weeks 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 7 months, 2 weeks 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 2 times

Alcpt 1 month, 4 weeks ago

no. Administrator accounts can't use security questions as verification method with SSPR.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-security-questions

upvoted 1 times

AleFerrillo 1 month, 3 weeks ago

Security Reader is not an Admin role subjected to "admin" SSPR rules.

upvoted 1 times

Nivos23 8 months ago

Selected Answer: B

I agree with 0byteThe answer is b

upvoted 1 times

Lekong 8 months, 2 weeks ago

I think it should be Username only

upvoted 1 times

Lekong 8 months, 2 weeks ago

I mean User 4 only. A

upvoted 1 times

Alcpt 1 month, 4 weeks ago

Security Reader account can use security questions as a verification method for Self-Service Password Reset (SSPR). Security questions are not used during sign-in but can be used during the SSPR process to confirm the user's identity. However, it's important to note that while security questions can be enabled for non-administrative roles, they are generally considered less secure than other methods

upvoted 1 times

shuhaidawahab 8 months, 3 weeks ago

Administrator accounts can't use security questions as verification method with SSPR.

upvoted 1 times

Trappie 9 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

Suggested Answer: *B*

Community vote distribution

B (100%)

Siraf 6 months ago

Correct Answer is B

upvoted 1 times

0byte 8 months, 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 4 times

e1ec325 8 months, 4 weeks ago

Selected Answer: B

Correct

upvoted 1 times

Question #67 *Topic 2*

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.

Suggested Answer: *A*

Community vote distribution

A (100%)

Siraf 6 months ago

Answer is A

upvoted 2 times

JimboJones99 8 months, 2 weeks ago

Selected Answer: A

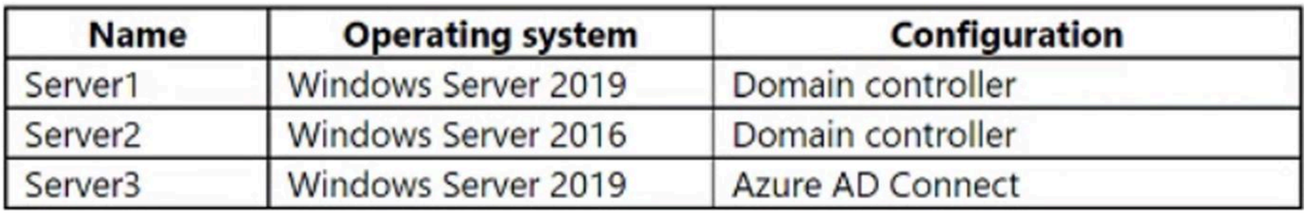
Correct as the tenant is new and security defaults will be on by default.

upvoted 3 times

Question #68 *Topic 2*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

Sozo 4 months, 2 weeks ago

Selected Answer: D

To ensure that Azure AD Password Protection continues to work even if a single server fails, you should implement the Azure AD Password Protection proxy service on Server4. This service is responsible for relaying password validation requests from on-premises Active Directory to Azure AD, which is essential for the Azure AD Password Protection feature to work correctly, especially since your domain controllers do not have internet access. By setting up the proxy service on an additional server, you provide redundancy for this functionality.

upvoted 1 times

0byte 8 months, 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 3 times

JCkD4Ni3L 8 months, 2 weeks ago

Selected Answer: D

Answer is correct.

upvoted 3 times

Question #69 *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 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

Suggested Answer: *D*

Community vote distribution

D (100%)

NickGhouse 1 month, 1 week ago

Selected Answer: D

Ahh.. we meet again

upvoted 3 times

GummyBear95 3 months, 2 weeks ago

Selected Answer: D

Same as all the others

upvoted 1 times

Robin_Cegeka 8 months, 1 week ago

Selected Answer: D

Just like the previous 5 times, a verification code is cached and doesn't need a connection.

upvoted 2 times

JCkD4Ni3L 1 year, 2 months ago

Selected Answer: D

Correct Answer, since there is no internet on mobile devices the only method available is the authenticator code.

upvoted 3 times

Question #69 *Topic 2*

You have an on-premises app named App1.

You have a Microsoft Entra tenant.

You plan to publish App1 by using Microsoft Entra Private Access.

You need to enable the Private access profile.

Which blade should you use in the Microsoft Entra admin center?

A. Remote networks

B. Traffic forwarding

C. Security profiles

D. Connectors

Suggested Answer: *B*

Community vote distribution

B (100%)

Sunth65 4 days, 3 hours ago

Selected Answer: B

Enable the Private Access traffic forwarding profile

Browse to Global Secure Access > Connect > Traffic forwarding. Select the checkbox for Private Access profile.

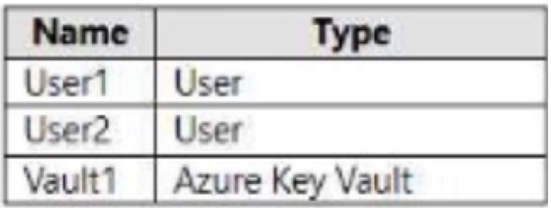
upvoted 1 times

Question #70 *Topic 2*

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:

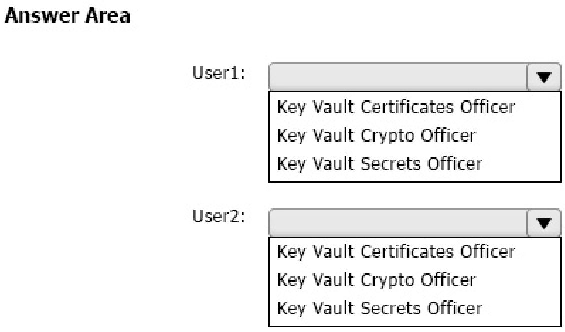
• Ensure that User1 can manage and create keys in Vault1.

• 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

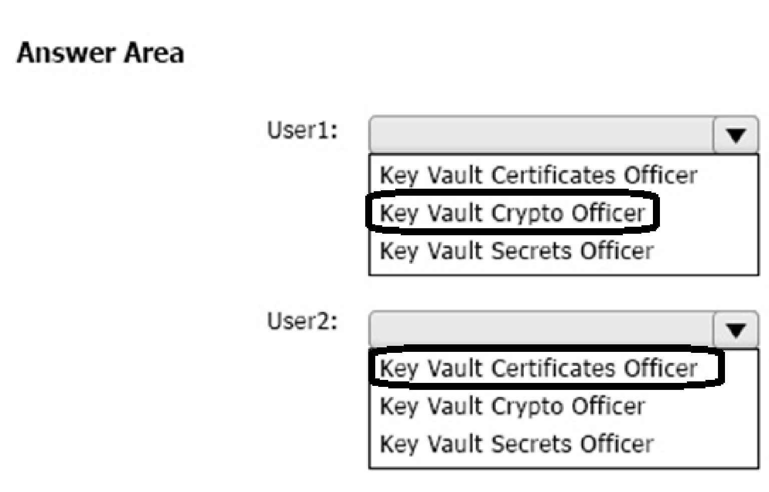
User1:

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

Suggested Answer:



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

Siraf Highly Voted 6 months ago

- Key Vault Crypto Officer
- Key Vault Certificates Officer

Key Vault Crypto Officer: Perform any action on the keys of a key vault, except manage permissions.

Key Vault Certificates Officer: Perform any action on the certificates of a key vault, except manage permissions.

Key Vault Secrets Officer: Perform any action on the secrets of a key vault, except manage permissions.

Ref:

https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli.

upvoted 5 times

⊟ **penatuna** Most Recent ⊙ 8 months, 1 week 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 3 times

⊟ **JCkD4Ni3L** 8 months, 2 weeks ago

Correct

upvoted 1 times

⊟ **AK_1234** 8 months, 4 weeks ago

- Key Vault Crypto Officer
- Key Vault Certificates Officer

upvoted 2 times

⊟ **Julesy** 9 months 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