



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



## **CERTIFICATION TEST**

- [CertificationTest.net](https://CertificationTest.net) - Cheap & Quality Resources With Best Support

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?

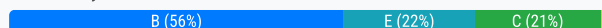
- A. Group1 and Group4 only
- B. Group1, Group2, Group3, Group4, and Group5
- C. Group1 and Group2 only
- D. Group1 only
- E. Group1, Group2, Group4, and Group5 only

**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 4 years 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 95 times

**Acrownit** 9 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 2 times

**klayytech** 1 year, 2 months 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



**Acrownit** 9 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** 10 months ago

Yes but the license here is MS 365 E5  
upvoted 1 times

  **tamisius** 3 years, 6 months 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** 3 years, 5 months ago

Agree - the licenses can be applied to all groups created in Azure AD via portal.  
upvoted 3 times

  **Beitran**  4 years, 1 month ago

Wrong, you can assign licenses to Microsoft 365 groups as well. The correct answer is E  
upvoted 22 times

  **Shaz** 4 years, 1 month ago

The answer is correct, there's only the two groups \*users not devices\* that marked as security.  
upvoted 7 times

  **Borbz** 3 years, 11 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** 9 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

  **Bulldozer** 3 years, 4 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, 8 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

  **CuraPutus**  1 month, 2 weeks ago

 Selected Answer: C

License can be assigned to only security group and users.  
upvoted 1 times

  **AcTiVeGrEnAdE** 2 months ago

 Selected Answer: C

C is the correct answer.

The license in the question cannot be assigned to a dynamic device group.

If group-based licensing is used, there are a few limitations:

- a) it does not support nested groups in which case, only the immediate first level user members will get the license.
- b) The feature can only be used with security groups & M365 groups that have securityEnabled=TRUE.

securityEnabled=TRUE is not set by default on any M365 groups and the question does not specifically mention any of the groups being set so we have to assume false. Therefore, the only groups that can be assigned a license is group 1 & 2.  
upvoted 1 times

  **Tatak\_Manok** 2 months ago

 Selected Answer: B

bing says you can assign a license to dynamic groups of type devices

upvoted 1 times

🗨️ 👤 **krzkrzkra** 2 months, 1 week ago

**Selected Answer: E**

Group-based licensing in Microsoft Entra ID is primarily designed for user accounts. This means that licenses are typically assigned to users, either directly or through their membership in groups. Devices, on the other hand, are not the primary targets for license assignments in this context.

However, there is a specific scenario where devices can be licensed: device-based licensing for Microsoft 365 Apps for enterprise. In this case, you can assign licenses to devices by adding them to a security group in Microsoft Entra ID and then assigning the appropriate licenses to that group. This method is specifically for Microsoft 365 Apps and is not a general approach for all Microsoft services.

learn.microsoft.com

For more detailed information, you can refer to the official Microsoft documentation on <https://learn.microsoft.com/en-us/microsoft-365/apps/licensing-activation/device-based-licensing>

upvoted 1 times

🗨️ 👤 **Yassine1988** 2 months, 2 weeks ago

**Selected Answer: E**

Chat GPT: To determine which groups you can assign a Microsoft Office 365 Enterprise E5 license directly, you need to understand that only Microsoft 365 groups with either:

Assigned membership, or

Dynamic user membership

...are eligible for direct license assignment in Azure AD.

upvoted 1 times

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

**Selected Answer: D**

Answer: D. User1 and User2 only, Users can be added to groups regardless of licence state. Licences assigned through group-based licensing are applied once the user is a member of the group

upvoted 1 times

🗨️ 👤 **Obi\_Wan\_Jacoby** 2 months, 3 weeks ago

**Selected Answer: E**

Answer is E. You cannot assign an E5 license to a device or a device group as they must be assigned to a user only. You can assign other licenses that are device based licensing for certain products (like 365 apps for enterprise) for shared devices so any user can use the apps etc.

upvoted 1 times

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

**Selected Answer: E**

"There are Microsoft 365, Office 365, and Windows licenses - These licenses are assigned to a Microsoft Entra user or group to grant them access to use Office or Windows products. You need one license for each user who needs access to Windows and / or office."

Keywords: user, define identity licensing

Source: <https://learn.microsoft.com/en-us/training/modules/explore-identity-azure-active-directory/11-define-identity-licensing>

upvoted 1 times

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

**Selected Answer: B**

Tested this per 15-03-2025: all groups were created in Entra ID. License assignments however need to be done in the 365 admin center, I could assign a license to all the groups.

However, when the Microsoft 365 groups are created in the M365 admin center, you cannot assigned a license to the group.

sezza\_blunt's post is the most accurate and therefor I would vote for B as well.

upvoted 1 times

🗨️ 👤 **Bojana** 3 months, 3 weeks ago

**Selected Answer: E**



Device groups, such as Dynamic Device groups, are not eligible for license assignments. Licenses can only be assigned to user-based groups like Security Groups, Mail-Enabled Security Groups, and Microsoft 365 Groups.

You can assign a Microsoft Office 365 Enterprise E5 license directly to several types of groups:

Security Groups: These groups are used to manage user and computer access to shared resources.

Mail-Enabled Security Groups: These groups are similar to security groups but also have an email address.

Microsoft 365 Groups: These groups provide collaboration features such as shared mailboxes, calendars, and document libraries  
upvoted 1 times

🗲️ 👤 **Frank9020** 5 months ago

**Selected Answer: E**

E is correct:

Group1 (Security, Assigned) → ✔ Eligible

Group2 (Security, Dynamic User) → ✔ Eligible

Group3 (Security, Dynamic Device) → ✖ Not Eligible (Device groups cannot have licenses)

Group4 (Microsoft 365, Assigned) → ✔ Eligible

Group5 (Microsoft 365, Dynamic User) → ✔ Eligible

upvoted 2 times

🗲️ 👤 **dee1969** 5 months, 1 week ago

**Selected Answer: C**

Group Type:

Security groups: Can have licenses assigned.

Microsoft 365 groups: Can have licenses assigned if securityEnabled = true. (This information is missing in the table, so by default, Microsoft 365 Groups are not considered security-enabled unless explicitly mentioned.)

Membership Type:

Both assigned and dynamic user memberships are supported for license assignment.

Dynamic device memberships are not eligible, as licenses are for users, not devices.

upvoted 2 times

🗲️ 👤 **test123123** 5 months, 3 weeks ago

**Selected Answer: B**

You can assign licenses to any security group.

<https://learn.microsoft.com/en-us/entra/fundamentals/concept-group-based-licensing#features>

<https://learn.microsoft.com/en-us/microsoft-365-apps/licensing-activation/device-based-licensing#steps-to-configure-device-based-licensing-for-microsoft-365-apps-for-enterprise>

upvoted 1 times

🗲️ 👤 **ATimTimm** 6 months, 3 weeks ago

**Selected Answer: E**

You cannot assign license to Dynamic Device group.

upvoted 2 times

🗲️ 👤 **Mole857** 7 months, 1 week ago

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

upvoted 1 times

You have a Microsoft Exchange organization that uses an SMTP address space of contoso.com.  
 Several users use their contoso.com email address for self-service sign-up to Azure 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 4 years 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 33 times

 **avdan16** Highly Voted 1 year, 5 months ago

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

upvoted 8 times

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

**Selected Answer: A**

Set-MsolCompanySettings: Sets company-level configuration settings.

Set-MsolCompanySettings

[-SelfServePasswordResetEnabled <Boolean>]

[-UsersPermissionToCreateGroupsEnabled <Boolean>]

[-UsersPermissionToCreateLOBAppsEnabled <Boolean>]

[-UsersPermissionToReadOtherUsersEnabled <Boolean>]

[-UsersPermissionToUserConsentToAppEnabled <Boolean>]

[-DefaultUsageLocation <String>]

[-AllowAdHocSubscriptions <Boolean>]

[-AllowEmailVerifiedUsers <Boolean>]

[-TenantId <Guid>]

[<CommonParameters>]

e.g. Set-MsolCompanySettings -SelfServePasswordResetEnabled \$True

upvoted 1 times

 **Obi\_Wan\_Jacoby** 2 months, 3 weeks ago

**Selected Answer: A**

Answer = A. However, now that they are pushing Microsoft Graph, try to remember the below.

Connect-MgGraph -Scopes "Policy.ReadWrite.Authorization"

Update-MgDirectorySetting -Id <settingId> -SelfServiceSignUpEnabled \$false

upvoted 1 times

🗳️ 👤 **Obi\_Wan\_Jacoby** 2 months, 3 weeks ago

Can also use the below

Connect-MgGraph -Scopes "Policy.ReadWrite.Authorization"

Update-MgPolicyAuthorizationPolicy -AllowEmailVerifiedUsersToJoinOrganization \$false -AllowedToSignUpEmailBasedSubscriptions \$false

upvoted 2 times

🗳️ 👤 **Labelfree** 8 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** 1 year ago

Correct Ans: A. Set-MsolCompanySettings Most Voted

upvoted 1 times

🗳️ 👤 **dc864d4** 1 year ago

MSOL is EOL

upvoted 1 times

🗳️ 👤 **RahulX** 1 year, 7 months ago

A. Set-MsolCompanySettings.

upvoted 2 times

🗳️ 👤 **sherifhamed** 1 year, 9 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 2 times

🗳️ 👤 **EmnCours** 1 year, 11 months ago

**Selected Answer: A**

A. Set-MsolCompanySettings

upvoted 2 times

🗳️ 👤 **dule27** 2 years, 1 month ago

**Selected Answer: A**

A. Set-MsolCompanySettings

upvoted 2 times

🗳️ 👤 **francescoc** 2 years, 3 months ago

**Selected Answer: A**

The correct answer is A

upvoted 1 times

🗳️ 👤 **jack987** 2 years, 6 months ago

The correct answer is A.

upvoted 1 times



🗳️ 👤 **[Removed]** 2 years, 6 months ago

**Selected Answer: A**

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

together:~:text=How%20do%20the%20controls%20work%20together%3F


upvoted 1 times

  **KrisDeb** 2 years, 7 months ago

**Selected Answer: A**

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

upvoted 1 times

  **clem24** 3 years 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** 3 years, 1 month 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

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

#### Guest user access

##### Guest user access restrictions (Preview) ⓘ

[Learn more](#)

- ☐ Guest users have the same access as members (most inclusive)
- ☒ Guest users have limited access to properties and memberships of directory objects
- ☐ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

#### Guest invite settings

##### Admins and users in the guest inviter role can invite ⓘ

☒ Yes ☐ No

##### Members can invite ⓘ

☒ Yes ☐ No

##### Guests can invite ⓘ

☐ Yes ☒ No

##### Email One-Time Passcode for guests ⓘ

[Learn more](#)

☒ Yes ☐ No

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

[Learn more](#)

☒ Yes ☐ No

#### Collaboration restrictions

- ☒ Allow invitations to be sent to any domain (most inclusive)
- ☐ Deny invitations to the specified domains
- ☐ Allow invitations only to the specified domains (most restrictive)

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

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

Which users will be emailed a passcode?

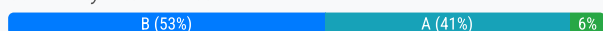
- A. User2 only
- B. User1 only
- C. User1 and User2 only
- D. User1, User2, and User3

#### Suggested Answer: A

Reference:

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

Community vote distribution



**Eltooth** Highly Voted 4 years, 1 month ago

[https://docs.microsoft.com/en-us/active-directory/external-identities/one-time-passcode#when-does-a-guest-user-get-a-one-time-passcode](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 93 times

  **pheb** 3 years, 10 months ago


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

upvoted 51 times

  **RahulX** 1 year ago

Correct I have done the RnD.

upvoted 1 times

  **JN\_311** 2 years 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** 3 years, 1 month ago

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

upvoted 5 times

  **itismadu** 2 years, 6 months 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

  **klayytech** 1 year, 2 months ago

He asking about who will sign with Passcode he not asking about MFA OTP

Passcode only allows for non-entra email users and non-Microsoft accounts like Gmail

upvoted 4 times



  **Alcpt** 1 year, 2 months 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.

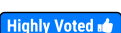
"Even the older \ legacy guest users who redeemed an invitation before email one-time passcode was enabled will continue to use their same authentication method.

upvoted 3 times

  **jack987** 2 years, 6 months ago

I agree the correct answer is A.

upvoted 2 times

  **scotty\_123**  3 years, 4 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 17 times

  **SnottyPudding** 3 years, 3 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 6 times

🗄️ 👤 **AnoG** Most Recent 1 month ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/entra/external-id/one-time-passcode>

According to this link, the answer becomes User 2 only

upvoted 1 times

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

**Selected Answer: A**

"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."

<https://learn.microsoft.com/en-us/entra/external-id/one-time-passcode#when-does-a-guest-user-get-a-one-time-passcode>

upvoted 1 times

🗄️ 👤 **FcoGlezRoy** 1 month, 3 weeks ago

**Selected Answer: A**

Only User2 will be emailed a passcode because User2 is an external user without an existing Microsoft or Azure AD account.

User1 is internal and does not need a passcode.

User3 has an existing account and authenticates normally without a passcode.

upvoted 1 times

🗄️ 👤 **AcTiVeGrEnAdE** 2 months ago

**Selected Answer: A**

Correct answer is A. They could have used a better example for User 2's email address with like a gmail domain, but user 2 is the only one who we be redeeming an invitation or accessing any resources with email OTP.

upvoted 1 times

🗄️ 👤 **dlizz** 2 months, 2 weeks ago

**Selected Answer: A**

Answer is A, The guest user has already registered and that is the method they will continue to use. The only one that would receive the OTP is a newly invited guest.

upvoted 1 times

🗄️ 👤 **noa808a** 3 months, 2 weeks ago

**Selected Answer: A**

OTP is only received by guest users who are accepting invitations for the first time. Therefore it can logically only be User2.

upvoted 1 times

🗄️ 👤 **bubbagump75** 3 months, 3 weeks ago

**Selected Answer: B**

User 2 has never accessed fabrikam.com so WILL receive OTP

upvoted 1 times

🗄️ 👤 **Stifino** 3 months, 3 weeks ago

**Selected Answer: A**

A. User2 Only.  
as User1 and existing users are already past the point of redemption.

upvoted 1 times

🗄️ 👤 **YesPlease** 4 months, 1 week ago

**Selected Answer: A**

Answer) A = User2 only

The only user that will get a One-Time Passcode will be User2 when they try to join the first time. User1 already joined as a guest and would have gotten their OTP back when they first joined and User3 is not a guest and is already apart of the Fabrikam domain.

upvoted 1 times

🗨️ 👤 **01b9a25** 4 months, 2 weeks ago

**Selected Answer: A**

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

🗨️ 👤 **\_marc** 4 months, 3 weeks ago

**Selected Answer: A**

Already existing guest user in fabrikam tenant will not be emailed a password. As an existing guest user they have already gone through the registration process, and because they have an outlook (i.e. microsoft) account, they can use their outlook account password rather than an emailed one

upvoted 1 times

🗨️ 👤 **test123123** 6 months, 1 week 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 2 times

🗨️ 👤 **Frank9020** 6 months, 2 weeks 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

🗨️ 👤 **Frank9020** 5 months ago

I was so very wrong.

User1 (User1@contoso.com) Already a guest user in fabrikam.com.

It does not say anything about if or how User1 authenticates to log in.

If User1 previously signed in using an MSA, Entra ID, or federation, they will NOT receive a passcode.

If User1 has no authentication method available, they WILL receive a one-time passcode.

User2 (User2@outlook.com) Not yet a guest user, but has a Microsoft account (MSA).

When trying to access the SharePoint document library, they will authenticate using their Microsoft account credentials.

Microsoft accounts do not use the email one-time passcode method—they authenticate directly with Microsoft, and won't receive a passcode.

User3 (User3@fabrikam.com) A regular user in fabrikam.com (not a guest).

Will log in normally using Entra ID (Azure AD) and doesn't need a passcode.

upvoted 1 times

🗨️ 👤 **photon99** 6 months, 2 weeks 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** 7 months 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 unknown

User 2, Microsoft Account

User 3 Microsoft Entra

upvoted 3 times

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users. From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 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, 9 months ago

In the exam the cmdlet was Set-MsolUserLicense, the right one!  
upvoted 41 times

🗳️ 👤 **photon99** 6 months, 2 weeks 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 5 times

🗳️ 👤 **Obi\_Wan\_Jacoby** 2 months, 3 weeks ago

This is correct. If on test, go with Set-MgUserLicense using Microsoft Graph using powershell  
upvoted 1 times

🗳️ 👤 **TJ001** 3 years, 5 months ago

just note it only works with Windows Power shell and not Powershell core..  
upvoted 2 times

🗳️ 👤 **Beitran** Highly Voted 4 years, 1 month ago

Correct!  
upvoted 12 times

🗳️ 👤 **3dd21ab** Most Recent 3 weeks, 2 days ago

Selected Answer: C  
c is correct  
upvoted 1 times

🗳️ 👤 **9H3zmT6** 2 months ago

Selected Answer: C  
This question presents three different correct answer patterns as options:  
- Licenses blade in the Microsoft Entra admin center

- Set-MsolUserLicense

- Set-MgUserLicense

upvoted 2 times

🗨️ 👤 **CrazyEyes007** 2 months ago

**Selected Answer: B**

You cannot assign licenses in "Licenses blade in the Azure Active Directory admin center" anymore. In M365 admin center, you will see the message: "You can assign to a maximum of 20 users at a time." So this must be an old question but the answer has to be "Set-MgUserLicense" when assigning licenses to users.

upvoted 1 times

🗨️ 👤 **AcTiVeGrEnAdE** 2 months ago

**Selected Answer: B**

I hope this question is re-worded on the exam as this question leads down the path of stupid. The fastest way to handle license update would be through PowerShell cmdlets. In this case B would be the correct answer but I hope the exam has an option which utilizes the MgGraph PowerShell SDK module.

upvoted 1 times

🗨️ 👤 **Bojana** 3 months, 3 weeks ago

**Selected Answer: B**

The Licenses blade in the Azure Active Directory admin center allows administrators to assign or unassign licenses for up to 20 users at a time<sup>12</sup>. This limitation is in place to ensure efficient management and reduce the risk of errors during bulk operations.

If you need to manage licenses for a larger number of users, you might consider using PowerShell scripts or Azure AD group-based licensing for more efficient bulk operations

upvoted 2 times

🗨️ 👤 **Frank9020** 6 months, 2 weeks 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 2 times

🗨️ 👤 **photon99** 6 months, 2 weeks ago

Unfortunately they have included in exam but the documentation is still incomplete for powershell Module : <https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users.actions/set-mguserlicense?view=graph-powershell-1.0>

upvoted 1 times

🗨️ 👤 **ross9876986** 10 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** 1 year, 4 months 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, 6 months ago

**Selected Answer: C**

correct answer is C

upvoted 1 times

🗨️ 👤 **lojlkdnfvlirez** 1 year, 6 months 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, 6 months 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 3 times

🗨️ 👤 **EmnCours** 1 year, 11 months ago

**Selected Answer: C**

Correct Answer: C

upvoted 1 times

🗨️ 👤 **dule27** 2 years ago

**Selected Answer: C**

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

upvoted 1 times

🗨️ 👤 **Faheem2020** 2 years, 9 months ago

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

```
Set-MgUserLicense -UserId "<Account>" -RemoveLicenses @"(<AccountSkuld1>") -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?](https://learn.microsoft.com/en-us/microsoft-365/enterprise/remove-licenses-from-user-accounts-with-microsoft-365-powershell?source=recommendations&view=o365-worldwide)

[source=recommendations&view=o365-worldwide](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

## HOTSPOT -

You have a Microsoft 365 tenant named contoso.com.

Guest user access is enabled.

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

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

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

### Collaboration restrictions

- ☐ Allow invitations to be sent to any domain (most inclusive)  
☐ Deny invitations to the specified domains  
☒ Allow invitations only to the specified domains (most restrictive)

 Delete

☒ TARGET DOMAINS

☐ Outlook.com

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

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

### Answer Area

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

Box 1: Yes -

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

Box 2: Yes -

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

Box 3. No -

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

🗨️ 👤 **Val\_0** Highly Voted 4 years, 1 month 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 58 times

🗨️ 👤 **reddevil01** 9 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 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 won't even be sent to user 3 mailbox since user settings for collaboration doesn't allow invitation to be sent to adatum.com

upvoted 15 times

🗨️ 👤 **TJ001** 3 years, 5 months ago

very straight forward question and answer

upvoted 5 times

🗨️ 👤 **f2bf85a** 2 years, 2 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 unchecked.

upvoted 1 times

🗨️ 👤 **Frank9020** Most Recent 5 months ago

About User3, the question is very confusing.

If invitations can only be sent to outlook.com, why ask if "User3 can accept the invitation and gain access to the SharePoint site" WHAT INVITATION? if the invitation was blocked, and he did not receive any invitation, there is no invitation to accept.

Also in the collaboration settings, it is only ticked for "Target Domains" and not ticked in the box for "outlook.com", is that why User3 received the invitation?

upvoted 1 times

🗨️ 👤 **m4rv1n** 9 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** 2 years, 2 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 question does not mention that SharePoint and OneDrive integration with Azure AD B2B is enabled, we should assume that it is disabled, as the default setting is so...

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



upvoted 1 times

  **f2bf85a** 2 years, 2 months ago

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


So 3rd question for User3 should be NO

upvoted 1 times

  **HartMS** 1 year, 2 months ago

Answer: YYN

upvoted 1 times

  **RahulX** 1 year, 4 months ago

Ans: Yes, because only user1@outlook.com will receive the invitation as per ext collaboration.

Ans: Yes, User2 already accepted 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, 10 months ago

YES

YES

No

upvoted 1 times

  **dule27** 2 years, 1 month ago

YES

YES

NO

upvoted 1 times

  **JCKd4Ni3L** 2 years, 1 month 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** 2 years, 1 month ago

Yes, yes, No.

Those who are confused at 3rd by assuming that sharepoint and onedrive work differently than B2B, please check the link

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

upvoted 1 times

  **itannajones** 2 years, 3 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** 2 years, 5 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, 6 months ago

Yes, Yes, No


Checked in my tenant

upvoted 4 times

  **BTL\_Happy** 2 years, 7 months ago

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

upvoted 1 times

  **ali\_pin** 2 years, 12 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** 3 years, 2 months ago

YES

YES

No

upvoted 2 times

  **janshal** 3 years, 2 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** 3 years, 3 months ago

what is the right answer?

upvoted 1 times



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

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

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

NOTE: Each correct selection is worth one point.

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

**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 4 years, 2 months ago

correct

upvoted 18 times

🗳️ 👤 **Chwist** Most Recent 5 months, 2 weeks ago

**Selected Answer: AB**

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.

upvoted 2 times

🗳️ 👤 **test123123** 5 months, 3 weeks ago

**Selected Answer: AB**

This is the way.

upvoted 3 times

🗳️ 👤 **AlexBrazil** 8 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 4 times

🗳️ 👤 **sherifhamed** 9 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** 1 year ago

Correct Ans:

A. email address

B. redirection URL

upvoted 1 times

🗄️ 👤 **grimrodd** 1 year, 1 month ago

**Selected Answer: AB**

correct

upvoted 1 times

🗄️ 👤 **RahulX** 1 year, 4 months ago

A. email address

B. redirection URL

upvoted 1 times

🗄️ 👤 **RahulX** 1 year, 7 months ago

A. email address

B. redirection URL

upvoted 1 times

🗄️ 👤 **EmnCours** 1 year, 10 months ago

**Selected Answer: AB**

A. email address

B. redirection URL

upvoted 1 times

🗄️ 👤 **dule27** 2 years, 1 month ago

**Selected Answer: AB**

A. email address

B. redirection URL

upvoted 1 times

🗄️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

**Selected Answer: AB**

AB are correct.

upvoted 1 times

🗄️ 👤 **jojoseph** 2 years, 5 months ago

**Selected Answer: AB**

correct

upvoted 1 times

🗄️ 👤 **Jhill777** 2 years, 7 months 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, 11 months ago

**Selected Answer: AB**

correct

upvoted 1 times

🗄️ 👤 **gwerin** 3 years, 4 months ago

**Selected Answer: AB**

Correct

upvoted 1 times

🗄️ 👤 **GPerez73** 3 years, 4 months ago

**Selected Answer: AB**

Correct. Just download the template and you can see it

upvoted 1 times

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

Name	Type	Directly assigned license
User1	User	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?

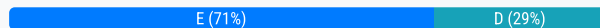
- A. User2 and Group2 only
- B. User2, Group1, and Group2 only
- C. User1, User2, Group1 and Group2
- D. User1 and User2 only
- E. User2 only

**Suggested Answer: E**

Reference:

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

Community vote distribution



**Cheguevarax** Highly Voted 4 years, 1 month ago

The answer is Use2 only. I just tested. You can't assign the users with no license. 100% upvoted 88 times

**loukyexamtopic** 11 months, 1 week ago

did you tested this in 365 admin centre or AAD  
upvoted 1 times

**hhaywood** 4 years ago

Agreed, also tested. However I found you can assign 'equipment users' e.g. Projectors with no license - odd one.  
upvoted 4 times

**lime568** 3 years, 3 months ago

because the equipments have a mailbox  
upvoted 7 times

**Arjanussie** 2 years, 4 months ago

Test it also You can't assign the users with no license / mailbox  
upvoted 1 times

**Discuss4certi** 3 years, 9 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 MESSG. But if you go to the user you can add a membership to the group.  
upvoted 6 times

**007Ali** 3 years, 5 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 2 times

**mackypatio** 3 years, 1 month 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, 6 months ago

**Selected Answer: E**



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

upvoted 21 times

  **xupiter** 3 years, 5 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, 9 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, 9 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, 8 months ago

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

upvoted 4 times

  **Chris7910** 2 years, 1 month 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

  **Nosajgnat87**  2 months ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/entra/fundamentals/concept-learn-about-groups>

Some groups can't be managed in the Azure portal or Microsoft Entra admin center.

Groups synced from on-premises Active Directory can only be managed on-premises.

Distribution lists and mail-enabled security groups can only be managed in the Exchange admin center or the Microsoft 365 admin center. You must sign in and have the appropriate permissions for that admin center to manage those groups.

upvoted 1 times

  **AcTiVeGrEnAdE** 2 months ago

**Selected Answer: D**

Mail enabled security groups does not support group nesting so any answer with a group listed is out.

User 1 and User 2 are able to be a member of mail enabled security group. Licensed user does not matter.

upvoted 1 times

  **Obi\_Wan\_Jacoby** 2 months, 3 weeks ago

**Selected Answer: D**

I was able (from the 365 admin center) to go to the unlicensed user, go to their group listings and add them to the mail enabled security group. However, I could not add the user while going to the group itself and trying to add the member that way. As from Entra, it does not tie down to a license for memberships, so it should also allow. So answer is D. Microsoft may want answer E, but this is the real world and the real world shows D.

upvoted 1 times

  **Obi\_Wan\_Jacoby** 2 months, 3 weeks ago

Answer is still D, but I wanted to update. Within Entra I could neither add the group via the user properties nor add the users via the group properties. So the only way you can do this is via the Admin center. I also tried this from the azure portal and had the same issue as in Entra.

upvoted 1 times

  **noa808a** 3 months, 2 weeks ago

**Selected Answer: D**

Correct answer is D.

Only users & service principals are able to be added to mail-enabled security groups (groups cannot be nested). Being added to a security group does not depend on licensing, so both users are eligible.

upvoted 3 times

🗳️ 👤 **Oskarma** 5 months, 2 weeks ago

**Selected Answer: D**

I've just added a user without license to a mail enabled security group in my tenant. And you can't add security groups to mail enabled security groups: <https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-groups#:~:text=Adding%20security%20groups%20as%20members%20of%20mail%2Denabled%20security%20groups.>

upvoted 1 times

🗳️ 👤 **test123123** 5 months, 3 weeks ago

**Selected Answer: E**

To get an email you need the licence:D

Cannot add Security groups that may have users without licenses duh.! ^^

upvoted 2 times

🗳️ 👤 **Frank9020** 5 months ago

You could not be more wrong, Entra ID does not require users to be licensed to be added to a mail-enabled security group.

Unlicensed users can still be added as members because group membership management in Entra ID is independent of licensing.

upvoted 1 times

🗳️ 👤 **saha241108** 5 months, 3 weeks ago

**Selected Answer: C**

become a member of mail enabled security group there has no pre-requisite like license user or not. you can add user as well as group as a member of group. So, the correct answer should be C

upvoted 1 times

🗳️ 👤 **Matt19** 6 months, 1 week ago

**Selected Answer: D**

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

upvoted 3 times

🗳️ 👤 **door88** 8 months, 2 weeks ago

**Selected Answer: D**

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

upvoted 3 times

🗳️ 👤 **MaxLily** 9 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** 11 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** 1 year, 2 months ago

No license - No Money

upvoted 2 times

  **HartMS** 1 year, 2 months ago

**Selected Answer: E**

User2 Only

upvoted 2 times

  **penatuna** 1 year, 4 months 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 Exchange portal.

upvoted 3 times

  **RahulX** 1 year, 4 months ago

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

Tested

upvoted 1 times

## DRAG DROP -

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

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

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

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

**Actions**

Sign in to the Microsoft 365 admin center.

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

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

Respond to the Become the admin message.

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

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

**Answer Area****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, 7 months ago

Seems correct judging by the link.

upvoted 24 times

**slayer78** Highly Voted 3 years, 2 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 20 times

  **test123123** 5 months, 3 weeks ago

Steps

1. Create a self-signed user account in the Azure AD tenant.
2. Sign in to the M365 admin center.
3. Respond to the Become the admin Message.
4. From The M365 admin center, add the domain name.

upvoted 1 times

  **casti** 3 years, 1 month ago

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

upvoted 3 times

  **007Ali** 2 years, 11 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 9 times

  **Jhill777** 2 years, 1 month ago

Yessir. Had to do this many times.

upvoted 1 times

  **AcTiVeGrEnAdE**  2 months ago

I agree with the suggested answer but WOW, what a horribly worded question.

upvoted 1 times

  **Rackup** 4 months ago

Sign in to the Microsoft 365 admin center with an account outside that tenant.

Add the contoso.com domain from the Microsoft 365 admin center.

Create a TXT record in the DNS zone for contoso.com to prove domain ownership.

Respond to the 'Become the admin' prompt in the admin center once verification completes.

upvoted 1 times

  **RahulX** 10 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

  **lojlkdnfvirez** 1 year 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** 1 year, 4 months 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, 7 months 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, 7 months 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, 9 months ago

Given answer is correct IMO.

upvoted 1 times

🗨️ 👤 **saadnadir** 2 years, 10 months ago

Create a Self Signed user account in azure AD tenant

Sign in to the Microsoft 365 admin center

respond to the become the admin message

create a txt record in the contoso.com DNS zone

upvoted 1 times

🗨️ 👤 **casti** 3 years, 2 months ago

i think:

1 sign 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** 3 years, 2 months ago

After thinking about it again, I think that:

i think:

1 Create a self signed user account

2 sign in the admin center

3 From the 365 admin center add the domain name

4 Create TXT record

upvoted 3 times

🗨️ 👤 **Ibukun** 3 years ago

This is a mistake

upvoted 1 times

🗨️ 👤 **Mohammad\_Alomari** 2 years, 5 months ago

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

upvoted 1 times

🗨️ 👤 **Domza** 3 years, 6 months ago

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

Tooof, these kinda questions

upvoted 4 times

🗨️ 👤 **jilly78** 2 years, 7 months ago

yes it lacks context

upvoted 1 times

## HOTSPOT -

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

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

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

Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

GroupA:

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

GroupB:

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

### Answer Area

Suggested Answer:

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 3 years, 7 months ago

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

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

upvoted 92 times

AmazingKies 3 years, 3 months ago

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

upvoted 7 times

  **lime568** 2 years, 9 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 24 times

  **GryffindorOG**  2 years, 4 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 7 times

  **Jhill777** 2 years, 1 month 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** 2 years, 4 months ago

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

upvoted 3 times

  **AcTiVeGrEnAdE**  2 months ago

Group A: User1, Group1, Group2 and Group3 Only

Group B: User1 Only

upvoted 1 times



  **Maxo\_Roken** 2 months, 3 weeks ago

I created the exact same scenario in my Entra tenant. The result is that Group A can contain Group 1, Group 2, Group 3 and a User 1. That is because, Security Group can have device, user, or a service principal as its members while M365 can have only users as its members.

while Group B can only contain User1 as its member - Groups (either Security or M365 type) cannot be added to Group B (M365 group type).

So, the correct answer is E for Group A and A for Group B

upvoted 1 times

  **krutesh** 4 months, 1 week ago



Group A: User1, Group1, Group2 and Group3 Only

Group B: User1 Only

Adding Microsoft 365 groups to security groups or other Microsoft 365 groups is not supported.

Adding security groups to Microsoft 365 groups is not supported.

upvoted 1 times

  **RahulX** 10 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** 1 year, 3 months ago

As of today when I tested with my tenant.

Group A: can include users and security groups but no MS365 groups.

Group B: can include only users but no groups.

upvoted 3 times

🗨️ 👤 **EmnCours** 1 year, 4 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 1 times

🗨️ 👤 **dule27** 1 year, 7 months ago

Group A - User1, Group1, Group2 and Group3

Group B - User1 only

upvoted 3 times

🗨️ 👤 **ShoaibPKDXB** 1 year, 7 months ago

Correct

Group A - User1, Group1, Group2 and Group3

Group B - User1 only

upvoted 1 times

🗨️ 👤 **anaSH** 2 years ago

Answer is correct, tested in my tenant

upvoted 4 times

🗨️ 👤 **cameron0485** 2 years, 1 month ago

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

upvoted 1 times

🗨️ 👤 **ANDRESCB1988** 2 years, 1 month ago

Correct.

GroupA allow add users, Dynamic User, Dynamic Devices.

GroupB only permit add users.

upvoted 2 times

🗨️ 👤 **sapien45** 2 years, 6 months ago

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

We don't currently support:

Adding Microsoft 365 groups to Security groups or other Microsoft 365 groups.

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

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

upvoted 1 times

🗨️ 👤 **observador081** 2 years, 7 months ago

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

User1 has a Department set to Sales and a Country set to US

User2 has a Department set to Marketing and a Country set to US

User3 has a Department set to Sales and a Country set to Germany

User4 has a Department set to Marketing and a Country set to Germany

You create a group called Group1 that has the following dynamic membership rule.

`user.country -eq "USA" -and user.department -eq "Marketing" -or user.department -eq "Sales"`

Which users are members of Group1?

Please select only one answer.

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** 2 years, 1 month ago

To answer your question above - B

upvoted 1 times

  **bleedinging** 2 years, 7 months ago

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

upvoted 2 times

  **thiennp1982** 2 years, 7 months ago

Correct

upvoted 1 times

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

You have an Active Directory forest that syncs to an Azure 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, 11 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 21 times

 **glazdub** 2 years, 3 months ago

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

upvoted 2 times


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

**Selected Answer: B**

Password writeback allows password changes in the cloud to be written back to an on-premises directory in real time by using either Microsoft Entra Connect or Microsoft Entra Connect cloud sync. When users change or reset their passwords using SSPR in the cloud, the updated passwords also written back to the on-premises AD DS environment.

Azure AD Connect with Pass-through Authentication (PTA) ensures that authentication requests are validated against on-premises Active Directory, so when an account is disabled, it is immediately reflected in Azure AD.

upvoted 1 times

 **test123123** 5 months, 3 weeks ago

**Selected Answer: B**

Agree.

upvoted 1 times

 **EmnCours** 10 months, 3 weeks ago

**Selected Answer: B**

Correct Answer: B

upvoted 1 times

 **dule27** 1 year, 1 month ago

**Selected Answer: B**

B. No is correct

upvoted 1 times

  **ShoaibPKDXB** 1 year, 1 month ago

**Selected Answer: B**

B is correct

upvoted 1 times

  **ANDRESCB1988** 1 year, 7 months ago



correct, answer is No

upvoted 1 times

  **bleedinging** 2 years, 1 month ago

Objection, your honor: Irrelevant.

upvoted 4 times

  **WMG** 2 years, 3 months ago

**Selected Answer: B**

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

upvoted 2 times

  **Iamjudeicon** 2 years, 6 months ago

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

upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant. You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes. You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.

Solution: You configure pass-through authentication.

Does this meet the goal?

A. Yes

B. No




**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, 11 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 18 times

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



Selected Answer: A  
Pass-through Authentication (PTA) allows Azure AD to validate user credentials directly against on-premises Active Directory in real time  
upvoted 1 times

  **RITIK1000** 5 months, 2 weeks ago

Selected Answer: B  
But just disabling the account will not work because of the sync cycle between AD and AAD so we need to implement CAE(Continuous access evaluation) or conditional access policies for the immediate enforcement of account disablement so correct answer should be B  
upvoted 2 times

  **AlexBrazil** 8 months ago

Selected Answer: A  
Microsoft Entra pass-through authentication can solve this issue.  
upvoted 2 times

  **RahulX** 1 year, 4 months ago



Yes, Pass-through Authentication and ADFS uses on-premises account policy at the time of sign-in in M365.  
upvoted 2 times

  **EmnCours** 1 year, 10 months ago

Selected Answer: A  
Correct Answer: A  
upvoted 3 times

  **dule27** 2 years, 1 month ago

Selected Answer: A  
A: YES - pass-through authentication.  
upvoted 2 times

  **ANDRESCB1988** 2 years, 7 months ago  
correct, answer is yes




upvoted 2 times

  **shine98** 3 years ago

On the exam - June 12, 2022


upvoted 1 times

  **DemekeAd** 3 years, 2 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, 6 months ago

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

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an 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, 11 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 3 years, 1 month ago

Correct (B - No)  
upvoted 7 times

 **test123123** Most Recent 5 months, 3 weeks ago

**Selected Answer: B**  
CA has nothing to do with this :D  
upvoted 1 times

 **Stevo74** 10 months, 2 weeks ago

Basically, you can configure a conditional policy for every disabled acc or group of acc (if you're disabling more of them at once). In policy you can block access to all cloud apps for this specific user or users and that will do, but this is not a permanent solution because you will need to do this every time, so that's why answer is B.  
upvoted 2 times

 **EmnCours** 10 months, 3 weeks ago

**Selected Answer: B**  
Correct (B - No)  
upvoted 2 times

 **dule27** 1 year, 1 month ago

**Selected Answer: B**  
B. No is the correct answer  
upvoted 2 times

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

**Selected Answer: B**  
No is the correct answer.  
upvoted 2 times

 **ANDRESCB1988** 1 year, 7 months ago

correct, answer is NO  
upvoted 1 times

🗨️ 👤 **Tokiki** 2 years ago

B is correct

upvoted 1 times

🗨️ 👤 **Fico** 2 years, 1 month ago

**Selected Answer: B**

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

upvoted 2 times

🗨️ 👤 **WMG** 2 years, 3 months ago

**Selected Answer: B**

Conditional Access will not help.

upvoted 1 times

🗨️ 👤 **glazdub** 2 years, 3 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** 3 years, 1 month ago

Agreed - answer is no.

upvoted 3 times

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, 11 months ago

The answer is simple. Answer is correct. Why? Because nested group do not inherit licenses.  
upvoted 66 times

🗳️ 👤 **jt63** 3 years, 6 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced#limitations-and-known-issues>  
upvoted 8 times

🗳️ 👤 **Dobby\_41** Highly Voted 4 years ago

Group 4 cannot be a member of group 1.  
upvoted 34 times

🗳️ 👤 **sapien45** 3 years ago

Good catch  
upvoted 5 times

🗳️ 👤 **YesPlease** Most Recent 4 months, 1 week ago

Selected Answer: B

Answer B) 2

It is a bad question because Group 1 is technically not possible because you are not allowed to add 365 Group to Security group. But, for sake of answering this question.... Licensing only applies to first tier users and not to nested groups.  
upvoted 1 times

🗳️ 👤 **test123123** 5 months, 3 weeks ago

Selected Answer: B

Nested group do not inherit licenses.  
upvoted 1 times

🗳️ 👤 **AlexBrazil** 8 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** 10 months, 3 weeks ago

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

contraduction with Topic1-Question9

upvoted 2 times

🗳️ 👤 **[Removed]** 1 year ago

the answer is 2. Very simple char

upvoted 1 times

🗳️ 👤 **BigDogAG** 1 year, 4 months ago

But why is it 2 and not 1?

upvoted 1 times

🗳️ 👤 **Futfuyfyfj** 1 year, 2 months ago

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

upvoted 1 times

🗳️ 👤 **RahulX** 1 year, 4 months 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, 9 months ago

**Selected Answer: B**

2 licenses

upvoted 1 times

🗳️ 👤 **EmnCours** 1 year, 10 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, 11 months ago

**Selected Answer: B**

Answer is correct.

upvoted 1 times

🗳️ 👤 **dule27** 2 years, 1 month ago

**Selected Answer: B**

B: 2 licenses

upvoted 2 times

🗳️ 👤 **f2bf85a** 2 years, 2 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** 2 years, 4 months ago

**Selected Answer: B**

agree it is b

upvoted 1 times

🗳️ 👤 **jojoseph** 2 years, 5 months ago

B. nested group do not inherit licenses

upvoted 3 times

🗳️ 👤 **ANDRESCB1988** 2 years, 7 months ago

correct, nesting is not support to assing license

upvoted 1 times

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

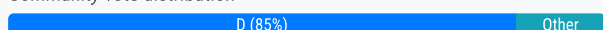
- A. Run the New-AzADUser cmdlet.
- B. Configure the External collaboration settings.
- C. Add a WS-Fed identity provider.
- D. Create a guest user account in contoso.com.

**Suggested Answer: D**

Reference:

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

Community vote distribution



**Jt909** Highly Voted 3 years, 9 months ago

Probably in the exam the cmdlet New-AzureADMSInvitation is proposed and correct  
upvoted 25 times

**AS007** Highly Voted 4 years ago

Looks good given external collaboration is allowed/ default settings  
upvoted 9 times

**WMG** 3 years, 3 months ago

Unless noted, all MS questions assume default settings.  
upvoted 4 times

**test123123** Most Recent 5 months, 3 weeks ago

**Selected Answer: D**

Invite user as guest, so a guest user :D  
upvoted 1 times

**Labelfree** 8 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** 8 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](https://aad.portal.azure.com) link redirects to Entra.

upvoted 2 times

  **bardock100** 1 year, 2 months ago

**Selected Answer: C**

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

upvoted 1 times

  **bardock100** 1 year, 2 months 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.

labeledzkis

upvoted 1 times

  **Labelfree** 8 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 provider<sup>1</sup>.

upvoted 1 times

  **belyo** 1 year, 4 months 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** 1 year, 4 months 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** 1 year, 5 months ago


shouldnt D say invite the user not create it?

upvoted 2 times

  **ak4exams** 1 year, 3 months ago

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



upvoted 1 times

  **EmnCours** 1 year, 11 months ago

**Selected Answer: D**

Answer is correct.

upvoted 1 times

  **LOEG** 2 years, 1 month 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** 2 years, 2 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** 2 years, 1 month 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** 2 years 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** 2 years 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** 2 years, 2 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** 2 years, 5 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** 2 years 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 2 times

🗨️ 👤 **Jhill777** 2 years, 7 months ago

**Selected Answer: D**

Correct, given external collaboration is set to defaults

upvoted 1 times

🗨️ 👤 **ANDRESCB1988** 2 years, 7 months ago

correct option D

upvoted 1 times

🗨️ 👤 **Magis** 2 years, 8 months ago

**Selected Answer: D**

Correct. B2B is the only option in this scenario.

upvoted 2 times



Your network contains an Active Directory forest named contoso.com that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com by using Azure AD Connect. You need to prevent the synchronization of users who have the extensionAttribute15 attribute set to NoSync. What should you do in Azure AD Connect?

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

**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** Highly Voted 8 months, 3 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 5 times

🗳️ **RahulX** Most Recent 10 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 3 times

🗳️ **EmnCours** 1 year, 4 months ago

**Selected Answer: C**

C is correct

upvoted 2 times

🗳️ **dule27** 1 year, 7 months ago

**Selected Answer: C**

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

upvoted 1 times

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

**Selected Answer: C**

C is correct

upvoted 1 times

🗳️ **m4rv1n** 1 year, 8 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, 11 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** 2 years 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** 2 years, 1 month ago

this came out in my test.

upvoted 2 times

🗳️ 👤 **palito1980** 2 years, 2 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** 2 years, 3 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** 2 years, 2 months ago

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

upvoted 1 times

🗳️ 👤 **Geolem** 2 years, 5 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** 2 years, 3 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, 6 months ago

C is correct

upvoted 1 times

🗳️ 👤 **Sh1rub10** 2 years, 9 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, 9 months ago

**Selected Answer: C**

upvoted 4 times

🗳️ 👤 **hwoarang** 2 years, 11 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** 3 years 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

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, 11 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 38 times

**AmazingKies** Highly Voted 3 years, 9 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

🗨️ 👤 **Yassine1988** Most Recent 2 months, 2 weeks ago

**Selected Answer: A**

User1 (Cloud-only user):

Authenticates directly against Azure AD (no dependency on on-premises infrastructure).

Can sign in.

User2 (Synced user):

Normally authenticates via PTA, which fails due to lost connectivity.

Cannot sign in (unless PHS is used as a fallback, but PTA takes precedence here).

User3 (Guest user):

Authenticates via their home tenant (no dependency on on-premises infrastructure).

Can sign in.

upvoted 2 times

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

**Selected Answer: A**

Microsoft FAQ states: "No. Pass-through Authentication doesn't automatically failover to password hash synchronization. To avoid user sign-in failures, you should configure Pass-through Authentication for high availability."

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta-faq#does-password-hash-synchronization-act-as-a-fallback-to-pass-through-authentication->

upvoted 1 times

🗨️ 👤 **krutesh** 4 months, 1 week ago

**Selected Answer: C**

Pass-through Authentication (PTA) validates users' passwords directly against on-premises Active Directory. It ensures on-premises security policies are enforced and does not store passwords in the cloud.

Password Hash Synchronization (PHS) synchronizes a hash of user's password from on-premises Active Directory to Azure AD. It allows users to sign in to Azure AD using the same password they use on-premises.

If both methods are enabled, PTA will take precedence for authentication. PHS can act as a backup, allowing users to sign in even if the PTA agent is temporarily unavailable.

upvoted 1 times

🗨️ 👤 **Frank9020** 5 months, 2 weeks ago

**Selected Answer: C**

User1: Can sign in because they are not directory-synced and their account exists solely in Azure AD.

User2: Can sign in because Password Hash Sync is enabled, allowing authentication to Azure AD even without on-premises connectivity.

User3: Can sign in because guest accounts authenticate directly with their own identity provider and do not rely on the on-premises domain.

upvoted 2 times

🗨️ 👤 **test123123** 5 months, 3 weeks ago

**Selected Answer: C**

By enabling Password Hash sync, you ensure that password hashes are synchronized to Azure AD, allowing users to authenticate even if the on-premises environment is unavailable. Password Hash sync is enabled, so answer is C.

upvoted 2 times

🗨️ 👤 **test123123** 5 months, 3 weeks ago

if your Azure AD Connect sync status shows "Password Hash Sync Enabled" and "Pass-Through Authentication Enabled," it means that users can still log on to Microsoft 365 even if the on-premises Active Directory loses internet connection.

upvoted 1 times

🗨️ 👤 **SebArgy** 6 months, 1 week ago

**Selected Answer: C**

Reponse C.

1 - The password is sync

2 - TPHA 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** 8 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 2 times

🗨️ 👤 **Olami** 8 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** 9 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, 9 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** 9 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 Password Hash Synchronization is enabled.

upvoted 6 times

🗨️ 👤 **Tuvshinjargal** 1 year, 4 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** 1 year, 4 months 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]** 9 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 2 times

🗨️ 👤 **simonseztech** 9 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 2 times

🗨️ 👤 **f2bf85a** 9 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 2 times

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

I got correct answer, but maybe my logic is off? All users work remotely, so wouldn't 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** 1 year, 4 months ago

A. User1 and User3 only correct ans.

upvoted 1 times

🗨️ 👤 **RahulX** 1 year, 4 months ago

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

upvoted 1 times

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

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

Solution: You configure Azure AD Password Protection.

Does this meet the goal?

A. Yes

B. No

**Suggested Answer: B**

Community vote distribution


B (100%)

 **kijken**  1 year, 7 months 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 13 times

 **melatocaroca**  3 years, 11 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


 **Fijii**  4 months, 1 week ago

**Selected Answer: B**

Only answer is PTA (Pass-Through Authentication).

Entra ID Password Protection is for... password protection ! Used to verify passwords against global or custom banned password lists

upvoted 1 times

 **[Removed]** 9 months, 1 week ago

**Selected Answer: B**

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

upvoted 2 times

 **kalyankrishna1** 1 year, 9 months ago

**Selected Answer: B**

PTA is the only thing that'll work

upvoted 2 times

 **dule27** 2 years, 1 month ago

**Selected Answer: B**

B: NO is the correct answer

upvoted 1 times

 **OrangeSG** 2 years, 5 months ago

**Selected Answer: B**



Answer is No.



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

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

upvoted 4 times

  **ANDRESCB1988** 2 years, 7 months ago

correct, is NO

upvoted 1 times

  **Jawad1462** 2 years, 7 months ago

**Selected Answer: B**

Is the correct answer

upvoted 1 times

  **Iamjudeicon** 3 years, 6 months ago

NO NO NO

The Given Answer Is Correct!!!

upvoted 2 times

  **sapien45** 3 years 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** 4 years ago

very clearly no - the given answer is correct

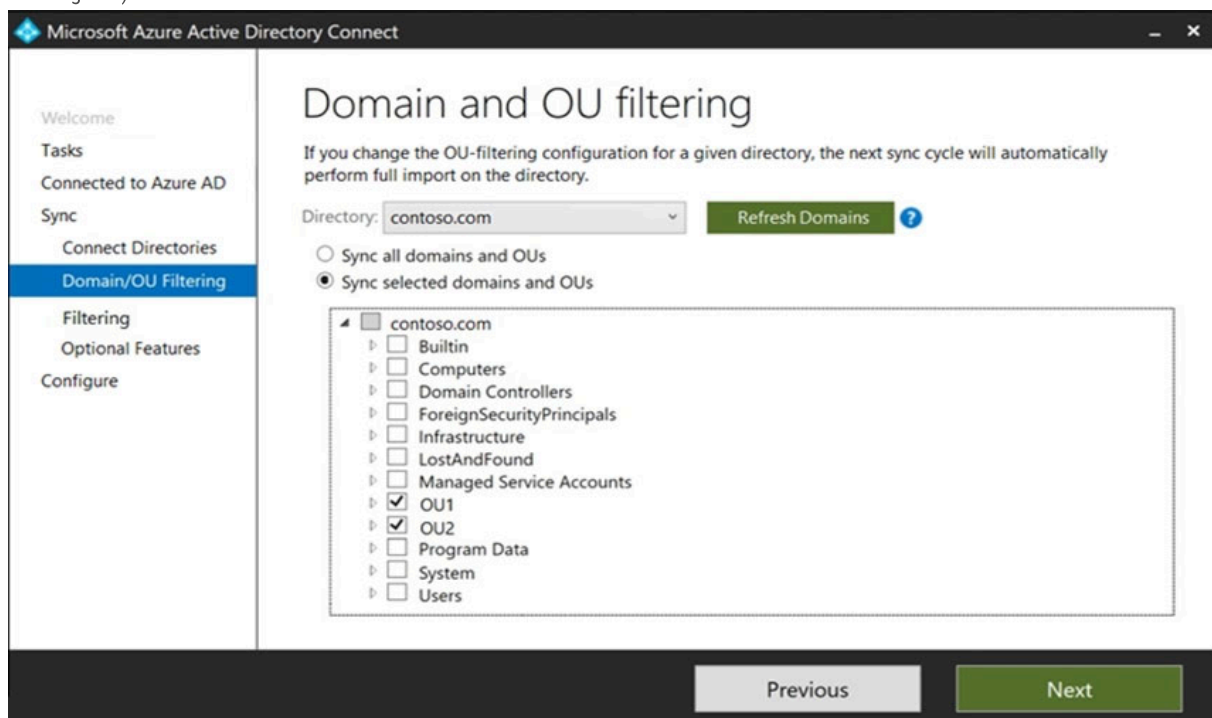
upvoted 1 times

## HOTSPOT -

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

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

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



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

Microsoft Azure Active Directory Connect

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

## Filter users and devices

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

☐ Synchronize all users and devices
☒ Synchronize selected ?

FOREST

contoso.com

GROUP

CN=Group1,OU=OU2,DC=contoso,DC=com

Resolve

Previous
Next

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

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

### Answer Area

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

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 2 years, 1 month 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 34 times

🗨️ 👤 **its\_tima** 1 year, 11 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, 11 months ago

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

upvoted 2 times

🗨️ 👤 **DrMe** Highly Voted 3 years, 2 months ago

Correct:

[https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-](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%20)

[custom#:~:text=When%20you%20add%20a%20group%20as%20a%20member%2C%20only%20the%20group%20itself%20is%20added.%20Its%20members%20](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%20)

upvoted 22 times

🗨️ 👤 **RahulX** Most Recent 10 months, 3 weeks ago

YES

NO

YES

upvoted 2 times

🗨️ 👤 **Nivos23** 1 year, 1 month ago

YES

NO

YES

upvoted 1 times

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

Correct:

[https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-](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%20)

[custom#:~:text=When%20you%20add%20a%20group%20as%20a%20member%2C%20only%20the%20group%20itself%20is%20added.%20Its%20members%20](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%20)

upvoted 1 times

🗨️ 👤 **dule27** 1 year, 7 months ago

YES

NO

YES

upvoted 1 times

🗨️ 👤 **Efficia** 2 years, 5 months ago

The given answer is correct.

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

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

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

upvoted 5 times

🗨️ 👤 **Tokiki** 2 years, 6 months ago

Correct, YNY

upvoted 1 times

🗨️ 👤 **rachee** 2 years, 6 months ago

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

upvoted 2 times

🗨️ 👤 **RandomNickname** 2 years, 7 months 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 because it's a direct member of G1, however any nested, for example, members of G2 will not be synced, so direct users or groups of G1 will.

For reference see below excerpt from MS article

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

upvoted 10 times

🗨️ 👤 **TP447** 2 years, 8 months ago

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

upvoted 4 times

🗨️ 👤 **SnottyPudding** 2 years, 9 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 3 times

🗨️ 👤 **kanew** 1 year, 8 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, 9 months ago

Group 2 is Nested and it will be ignored.

Y, N, N is the correct.

upvoted 4 times

🗨️ 👤 **SnottyPudding** 2 years, 9 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, 9 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, 11 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, 10 months ago

OU1 doesn't sync to the AAD, just Group1 and OU2

upvoted 1 times

🗨️ 👤 **GPerez73** 2 years, 9 months ago



It is true, you are right.

upvoted 1 times

🗨️ 👤 **teriaavibes** 2 years, 9 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

  **bt\_k\_1** 2 years, 11 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, 11 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, 11 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

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, 6 months ago  
Correct.

To take advantage of MAU billing, your Azure AD tenant must be linked to an Azure subscription.  
<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing#what-do-i-need-to-do>  
upvoted 9 times

 **WS\_21** Highly Voted 3 years, 3 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 9 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** 9 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** 1 year, 4 months ago  
C. a linked subscription Mo  
upvoted 1 times

 **EmnCours** 1 year, 10 months ago  
Selected Answer: C  
C. a linked subscription  
upvoted 1 times

🗨️ 👤 **dule27** 2 years, 1 month ago

**Selected Answer: C**

C. a linked subscription

upvoted 1 times

🗨️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

C Linked Subscription

upvoted 1 times

🗨️ 👤 **KennethYY** 3 years, 6 months ago

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

upvoted 3 times

🗨️ 👤 **zaqwsx** 3 years, 10 months ago

it looks correct, from docs:

An Azure AD tenant already linked to a subscription?

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

upvoted 3 times



## DRAG DROP -

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

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

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

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

**Actions**

Delete the contoso.onmicrosoft.com domain.

Add a custom domain name of contoso.com.

Set the domain to primary.

Create a new TXT record in DNS.

Successfully verify the domain name.

**Answer Area****Suggested Answer:****Actions**

Delete the contoso.onmicrosoft.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**  3 years, 2 months ago


Correct!!!

upvoted 26 times

 **3dd21ab**  3 weeks ago

correct

upvoted 1 times

 **oenyabine** 6 months, 3 weeks ago

correct

upvoted 1 times

 **EmnCours** 1 year, 5 months ago

Correct!!!

upvoted 2 times

 **EmnCours** 1 year, 4 months 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, 7 months 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** 2 years, 1 month ago

correct

upvoted 1 times

🗨️ 👤 **pete26** 2 years, 2 months ago

The answer given is correct!

upvoted 1 times

🗨️ 👤 **TJ001** 2 years, 11 months ago

Correct !!

upvoted 1 times

🗨️ 👤 **Iamjudeicon** 3 years ago

CORRECT!!!

upvoted 2 times

## HOTSPOT -

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

| Name   | Role                       |
|--------|----------------------------|
| Admin1 | Cloud device administrator |
| Admin2 | Device administrator       |
| User1  | None                       |

You have the Device Settings shown in the following exhibit.

Devices | Device settings ...

Default Directory - Azure Active Directory

<< Save Discard Got feedback?

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

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.                                                          | <input type="radio"/> | <input type="radio"/> |
| Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to <b>Yes</b> . | <input type="radio"/> | <input type="radio"/> |
| Admin2 is a local administrator on Device3.                                                                             | <input type="radio"/> | <input type="radio"/> |

Suggested Answer:

### Answer Area

| Statements                                                                                                              | Yes                              | No                               |
|-------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 can join four additional Windows 10 devices to Azure AD.                                                          | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to <b>Yes</b> . | <input type="radio"/>            | <input checked="" type="radio"/> |
| Admin2 is a local administrator on Device3.                                                                             | <input type="radio"/>            | <input checked="" type="radio"/> |

Box 1: Yes -

Users may join 5 devices to Azure AD.

Box 2: No -

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

Box 3: No -

An additional local device administrator has not been applied

Reference:

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

  **DrMe**  3 years, 8 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%20registered,context=azureportal>  
upvoted 86 times

  **NotanAdmin** 1 year, 1 month ago

You are correct that : The limit applies to devices that are Microsoft Entra joined or Microsoft Entra registered, with some exceptions. <https://learn.microsoft.com/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 additional devices", so No, because no matter what devices, he already has 5 joined OR registered.

upvoted 1 times

  **Menard001** 1 year, 3 months 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** 1 year ago


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

upvoted 1 times

  **Futfuyfjffj** 1 year, 2 months 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, 12 months ago

100% agreed and tested, these answer are correct:

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

upvoted 15 times

  **phony** 3 years, 3 months ago

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

upvoted 1 times

  **phony** 3 years, 3 months ago



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

upvoted 11 times

  **kanew** 2 years, 2 months ago

exactly!

upvoted 1 times

  **xurxosan**  3 years, 3 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, 6 months 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**  8 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** 9 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** 10 months, 4 weeks 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** 1 year 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** 1 year, 2 months ago

NO

YES

NO

upvoted 1 times

🗨️ 👤 **jtlucas99** 1 year, 2 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** 1 year, 4 months 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** 1 year, 4 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** 1 year, 4 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** 1 year, 5 months 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, 7 months ago

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

upvoted 2 times

🗨️ 👤 **amurp35** 1 year, 10 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, 10 months ago

Correction:

NO

YES

NO

upvoted 1 times

🗨️ 👤 **dule27** 2 years, 1 month ago

NO

NO

NO

upvoted 1 times

  **dule27** 1 year, 12 months ago



Correction:

NO

YES

NO

upvoted 1 times

  **kanew** 2 years, 2 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

  **Holli** 2 years 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** 2 years, 2 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

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%)

🗳️ 👤 **3dd21ab** 3 weeks ago

**Selected Answer: C**

Thats correct!

upvoted 1 times

🗳️ 👤 **test123123** 5 months, 3 weeks ago

**Selected Answer: C**

Checked myself, this is the way.

upvoted 1 times

🗳️ 👤 **5f2afa7** 6 months ago

**Selected Answer: C**

Entra > User experiences > Company Branding > Add browser language

upvoted 3 times



DRAG DROP -

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

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

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

Which portal should you use to configure each user? To answer, drag the appropriate portals to the correct users. Each portal may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

### Portals

### Answer Area

Azure Active Directory admin center

Exchange admin center

Microsoft 365 compliance center

Microsoft Endpoint Manager admin center

SharePoint admin center

User1:

User2:

User3:

Suggested Answer:

### Portals

### Answer Area

Azure Active Directory admin center

Exchange admin center

Microsoft 365 compliance center

Microsoft Endpoint Manager admin center

SharePoint admin center

User1:


User2:

User3:

Azure Active Directory admin center

Exchange admin center

Microsoft Endpoint Manager admin center

 **sergioandreslq** Highly Voted 2 years, 5 months ago

Answer:

User 1: Azure AD Admin center

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

and compliance center) SCC roles have evolved from Exchange role groups design to MS Purview.

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

upvoted 40 times

🗨️ 👤 **jack987** 2 years 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 12 times

🗨️ 👤 **Nyamnyam** 1 year, 1 month 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, 8 months ago

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

upvoted 2 times

🗨️ 👤 **dhenrique1555** Highly Voted 🍌 2 years, 8 months ago

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

upvoted 13 times

🗨️ 👤 **jilly78** 2 years, 7 months ago

currently true

upvoted 3 times

🗨️ 👤 **Holii** 1 year, 6 months ago

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

upvoted 4 times

🗨️ 👤 **RahulX** Most Recent 🔔 10 months, 3 weeks ago

Azure AD Admin Center (Microsoft Entra ID Admin Center)

\* User Administrator Role

\* Device Administrator 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 7 times

🗨️ 👤 **mikekrt** 1 year, 3 months ago

New names:

User 1: Entra ID Admin center

User 2: Microsoft Purview admin center

User 3: Intune admin center

upvoted 7 times

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

🗨️ 👤 **EmnCours** 1 year, 5 months ago

Correct Answer

upvoted 1 times

🗨️ 👤 **MatthewMeng** 1 year, 6 months 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, 7 months 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, 6 months 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** 1 year, 5 months ago

User 2: Microsoft Purview Compliance portal

upvoted 1 times

🗨️ 👤 **AmplifiedStitches** 1 year, 8 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, 11 months ago

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

upvoted 1 times

🗨️ 👤 **ANDRESCB1988** 2 years, 1 month ago

correct

upvoted 1 times

🗨️ 👤 **VinciTheTechnic1an** 2 years, 6 months ago

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

upvoted 2 times

🗨️ 👤 **bleedinging** 2 years, 7 months ago

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

upvoted 4 times

🗨️ 👤 **slick\_orange** 2 years, 4 months ago

Or maybe the question was not up to date.

upvoted 2 times

🗨️ 👤 **kanew** 1 year, 8 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, 8 months ago

Answer is partly wrong:

Correct answers below:

- 1) Azure AD Admin Center
  - 2) Microsoft Purview Portal > Permissions & Roles > Purview Roles (Old name was "Microsoft 365 Compliance Portal")
  - 3) Microsoft Endpoint Manager Admin Center
- upvoted 4 times

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

A corporate security policy states the following:

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

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

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

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

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

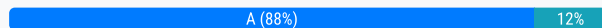
- A. Server4
- B. Server2
- C. Server1
- D. Server3

**Suggested Answer:** A

Reference:

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

Community vote distribution



🗳️ 👤 **Nilz76** Highly Voted 👍 2 years, 8 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 20 times

🗳️ 👤 **krisbla** Highly Voted 👍 11 months, 1 week ago

On Exam in January 2024!

upvoted 8 times

🗳️ 👤 **AcTiVeGrEnAdE** Most Recent 🕒 2 months ago

**Selected Answer:** A

PTA is installed on the Entra connect sync server if configured so if you are looking for PTA failover, the safest approach would be to install the agent on an additional member server.

upvoted 1 times

🗳️ 👤 **onelove01** 1 year ago

**Selected Answer:** A

On exam 12/15/2023.

upvoted 2 times

🗳️ 👤 **EmnCours** 1 year, 5 months ago

**Selected Answer:** A

Answer A.

upvoted 1 times

🗳️ 👤 **dule27** 1 year, 7 months ago

**Selected Answer:** A

A: Server 4

upvoted 1 times

- 🗨️ 👤 **yakuzasm** 1 year, 10 months ago  
server 4 is correct, tested and worked  
upvoted 2 times
- 🗨️ 👤 **ANDRESCB1988** 2 years, 1 month ago  
Server 4 is correct  
upvoted 1 times
- 🗨️ 👤 **slick\_orange** 2 years, 4 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** 2 years, 5 months ago  
**Selected Answer: A**  
Answer A.  
upvoted 1 times
- 🗨️ 👤 **Zubairr13** 2 years, 5 months ago  
On the exam, 7/23/2022.  
upvoted 2 times
- 🗨️ 👤 **Tokiki** 2 years, 6 months ago  
Agree. A  
upvoted 2 times
- 🗨️ 👤 **shine98** 2 years, 6 months ago  
On the exam - June 12, 2022  
upvoted 1 times
- 🗨️ 👤 **bleedinging** 2 years, 7 months ago  
Gotta be A. Server 3 has it already and if it goes down they won't be able to authenticate.  
upvoted 4 times
- 🗨️ 👤 **Xyz\_40** 2 years, 6 months ago  
correct...  
upvoted 1 times
- 🗨️ 👤 **Davidf** 2 years, 7 months ago  
Server 4 since DCs cannot talk to the internet and server 3 already has it presumably  
upvoted 6 times
- 🗨️ 👤 **Nilz76** 2 years, 8 months ago  
**Selected Answer: A**  
This question was in the exam 28/April/2022  
upvoted 3 times
- 🗨️ 👤 **Nilz76** 2 years, 8 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, 8 months ago  
Correction, wrong vote on Selected Answer, Should be Selected Answer A.  
upvoted 1 times

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

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

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

What should you do?

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

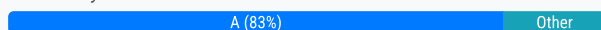
#### Suggested Answer: A

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



**Jacquesvz** Highly Voted 2 years, 10 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 27 times

**Hot\_156** Highly Voted 2 years, 9 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, 10 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 1 year 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** 1 year 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** 1 year, 2 months 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, 7 months 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, 11 months ago

**Selected Answer: A**

A. Run the New-AzureADMSInvitation cmdlet.

upvoted 1 times

🗨️ 👤 **vietnam** 1 year, 11 months ago

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

upvoted 1 times

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

by inviting him you ensure he gets access, so A

upvoted 1 times

🗨️ 👤 **dule27** 2 years, 1 month ago

**Selected Answer: A**

A. Run the New-AzureADMSInvitation cmdlet.

upvoted 1 times

🗨️ 👤 **AMDf** 2 years, 6 months ago

**Selected Answer: A**

A is correct

upvoted 4 times

🗨️ 👤 **pikapin** 2 years, 9 months ago

In exam 29/Sep

upvoted 1 times

🗨️ 👤 **DeepMoon** 2 years, 9 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 2 times

🗨️ 👤 **Holii** 2 years 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, 11 months ago



**Selected Answer: B**

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

upvoted 3 times

  **kangtamo** 2 years, 11 months ago

**Selected Answer: A**


I would go with A.

upvoted 1 times

  **Tokiki** 3 years ago

A is answer

upvoted 1 times



  **Mike8899** 3 years 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** 2 years, 2 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** 3 years 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

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 3 years, 1 month ago

The Set-MsolUserLicense cmdlet is deprecated. You'd use Set-MgUserLicense now.  
upvoted 15 times

🗳️ **sapien45** 2 years, 12 months ago  
Not yet deprecated

The Set-MsolUserLicense and New-MsolUser (-LicenseAssignment) cmdlets are scheduled to be retired. Please migrate your scripts to the Microsoft Graph SDK's Set-MgUserLicense cmdlet as described above  
upvoted 6 times

🗳️ **JimboJones99** Highly Voted 1 year, 8 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

🗳️ **klayytech** 1 year, 2 months ago  
Set-MgUserLicense  
upvoted 2 times

🗳️ **AlexBrazil** Most Recent 8 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** 10 months, 2 weeks ago

Question in Aug 2024

upvoted 2 times

🗳️ 👤 **jtlucas99** 1 year, 1 month 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, 9 months ago

But isn't it true that,

The Set-MsolUserLicense cmdlet is a valid PowerShell cmdlet used for managing license assignments for individual users in Microsoft 365. It allows you to add, remove, or modify licenses for a specific user.

upvoted 2 times

🗳️ 👤 **EmnCours** 1 year, 10 months ago

**Selected Answer: D**

D. the Set-MsolUserLicense cmdlet

upvoted 2 times

🗳️ 👤 **dule27** 2 years ago

**Selected Answer: D**

D. the Set-MsolUserLicense cmdlet

upvoted 2 times

🗳️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

**Selected Answer: D**

D: Set-MsolUserLicense

upvoted 3 times

🗳️ 👤 **[Removed]** 2 years, 6 months ago

**Selected Answer: D**

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

upvoted 1 times

🗳️ 👤 **giver** 2 years, 11 months ago

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

upvoted 1 times

🗳️ 👤 **martinods** 2 years, 9 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, 6 months ago

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

upvoted 1 times

🗳️ 👤 **rachee** 2 years, 11 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** 3 years ago

D is correct

upvoted 1 times

🗳️ 👤 **Benkyoujin** 3 years, 1 month 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

You have a Microsoft Entra tenant named contoso.com that contains an 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. Implement Microsoft Entra Connect sync.
- B. Add a custom domain name to contoso.com.
- C. Implement Microsoft Entra Application Proxy.
- D. Run the New-MgInvitation cmdlet.

**Correct Answer:** D



  **test123123** 5 months, 3 weeks ago

**Selected Answer:** D

Invite the user using the mggraph powershell module. New-mginvitation. Ref

<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mginvitation?view=graph-powershell-1.0>

upvoted 1 times

  **lxRs451** 5 months, 3 weeks ago

**Selected Answer:** D

Answer: D

It is the new cmdlet replacing New-AzureADMSInvitation

upvoted 4 times

## HOTSPOT -

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

One-time password:

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

User details:

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

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>

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 38 times

  **Waris\_khan8623**  10 months, 1 week ago

B2C identity provider and user flow under B2c Tenant. The answer is correct.  
upvoted 4 times

  **RahulX** 10 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 4 times

  **EmnCours** 1 year, 5 months 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** 1 year, 4 months ago

One-Time Password: an Identity Provider


User Details: a user flow

upvoted 3 times

  **venumurki** 1 year, 6 months 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, 6 months ago

One-Time Password: an Identity Provider


User Details: a user flow

upvoted 2 times

  **ShoaibPKDXB** 1 year, 7 months ago

Correct. An Identity provider and User flow

upvoted 1 times



  **f2bf85a** 1 year, 8 months ago

Why Box 1 should be "An Identity Provider"??

You first have to enable self-service sign-up from the "External Collaboration Settings".

If you do that, "Email one-time passcode" identity provider is already added and enabled by default...

upvoted 4 times

  **Holii** 1 year, 6 months 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, 6 months 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** 8 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** 2 years, 1 month 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** 2 years, 1 month ago

Correct.

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

upvoted 2 times



  **TheMCT** 2 years, 2 months ago

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

Box 1 -> Identity Provider

Box 2 -> User Flow

upvoted 4 times

  **Moezey** 2 years, 2 months ago

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

upvoted 2 times

  **Holii** 1 year, 6 months 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** 2 years ago



I think guest setting, refer question 3

upvoted 2 times

  **taer** 2 years, 3 months ago

correct

upvoted 1 times

You have an Azure Active Directory (Azure AD) Azure AD tenant.  
 You need to bulk create 25 new user accounts by uploading a template file.  
 Which properties are required in the template file?

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

**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 1 year, 2 months 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 9 times

 **Nyamnyam** Highly Voted 1 year, 7 months ago

Has anyone paid 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 8 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, 10 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, 11 months ago

**Selected Answer: C**

Correct Answer: C

upvoted 2 times

 **dule27** 1 year, 12 months ago

**Selected Answer: C**

C. accountEnabled, displayName, userPrincipalName, and passwordProfile


upvoted 1 times

 **ShoaibPKDXB** 2 years, 1 month ago

**Selected Answer: C**

Correct. C

upvoted 1 times

 **kerimnl** 2 years, 8 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, 9 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, 9 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, 9 months ago

**Selected Answer: C**

You can see it in the Template

upvoted 2 times

🗨️ 👤 **zed026** 2 years, 10 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, 6 months ago

So basically, none of the provided answers is correct.

upvoted 1 times

🗨️ 👤 **ThotSlayer69** 2 years, 5 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** 2 years, 5 months ago

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

upvoted 3 times

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. Users sign in to computers that run Windows 10 and are joined to the domain. You plan to implement Azure AD Seamless Single Sign-On (Azure AD Seamless SSO). You need to configure the Windows 10 computers to support Azure AD Seamless SSO. What should you do?

- A. Configure Sign-in options from the Settings app.
- B. Enable Enterprise State Roaming.
- C. Modify the 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**  3 years, 8 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**  2 years, 10 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**  8 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** 1 year, 4 months 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, 11 months ago

**Selected Answer: C**

Correct Answer: C

upvoted 1 times

 **dule27** 1 year, 12 months ago

**Selected Answer: C**

C. Modify the Intranet Zone settings.

upvoted 2 times

 **ShoaibPKDXB** 2 years, 1 month ago

**Selected Answer: C**

Correct: C

upvoted 1 times

🗨️ 👤 **Zubairr13** 2 years, 11 months ago

On the exam, 7/23/2022.

upvoted 3 times

🗨️ 👤 **ali\_pin** 2 years, 12 months ago

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

upvoted 2 times

🗨️ 👤 **shine98** 3 years ago

On the exam - June 12, 2022

upvoted 3 times

🗨️ 👤 **petercorn** 3 years ago

**Selected Answer: C**

Answer in Step 3: Roll out the feature

upvoted 1 times

🗨️ 👤 **POOUAGA** 3 years, 1 month ago

Agree the answer is C

upvoted 1 times

🗨️ 👤 **Nilz76** 3 years, 2 months ago

This question was in the exam 28/April/2022

upvoted 1 times

🗨️ 👤 **Miguelin11** 3 years, 3 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** 3 years, 3 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** 3 years, 3 months ago

On the exam - March 28, 2022

upvoted 1 times

🗨️ 👤 **Sh1rub10** 3 years, 3 months ago

**Selected Answer: C**

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

upvoted 1 times

## HOTSPOT -

Your on-premises network contains an Active Directory Domain Services (AD DS) domain. The domain contains computers that run Windows 11.

You have a Microsoft 365 E5 subscription.

You plan to enable hybrid join and enroll the computers in Microsoft Intune.

You need to recommend the software that should be deployed to the domain, and the actions that should be performed in Intune.

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

NOTE: Each correct selection is worth one point.

## Answer Area

Domain:   
 Microsoft Entra Connect  
 The Microsoft Entra provisioning agent

Intune:   
 Modify the mobile device management (MDM) user scope.  
 Modify the Windows Information Protection (WIP) user scope.

## Correct Answer:

## Answer Area

Domain:   
 Microsoft Entra Connect  
 The Microsoft Entra provisioning agent

Intune:   
 Modify the mobile device management (MDM) user scope.  
 Modify the Windows Information Protection (WIP) user scope.

**Frank9020** Highly Voted 4 months, 4 weeks ago

1: Domain= Entra Connect - Required for hybrid Azure AD join

1: Intune= Modify the mobile device management (MDM) user scope Enables automatic enrollment into Intune  
 upvoted 6 times

**noa808a** Most Recent 3 months, 2 weeks ago

Domain = Entra Connect, Intune = Modify MDM.  
 upvoted 1 times

**noa808a** 3 months, 2 weeks ago

I should also note, Intune connector for AD is partially correct, but is not the best answer to what the question is asking (steps for hybrid joining devices). Modifying the WIP user scope is also partially correct, however this would come after modifying the MDM scope, and is therefore not the best answer.

upvoted 2 times

**Waiuku2123** 5 months, 1 week ago

1. Entra Connect (provisioning agent does not support devices)

2. Modify MDM User Scope to allow all (or some) users to enrol devices

Autopilot not mentioned in the question, it is simply configuring Entra ID hybrid join for on premises devices

upvoted 2 times

**northgaterebel** 5 months, 1 week ago


Answer seems correct.

1. Intune Connector for AD.

2. Modify the MDM user scope.

<https://learn.microsoft.com/en-us/autopilot/windows-autopilot-hybrid>

upvoted 1 times

  **Phil\_79** 2 weeks ago

Autopilot is a provisioning solution meant to provision new computer from the out-of-the-box experience. To hybrid join a client to Entra, you just work on the Connect and on Intune tenant-side

upvoted 1 times

## DRAG DROP -

You need to resolve the recent security incident issues.

What should you configure for each incident? To answer, drag the appropriate policy types to the correct issues. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

**Policy Types**

An authentication method policy

A Conditional Access policy

A sign-in risk policy

A user risk policy

**Answer Area**

Leaked credentials:

A sign-in from a suspicious browser:

Resources accessed from an  
anonymous IP address:

**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 sign-in from a suspicious browser:

Resources accessed from an  
anonymous IP address:

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>

  **Obyte**  2 years, 2 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 23 times



  **rvln7** 4 months ago

1. A user risk policy

2. A sign in risk policy

3. A conditional access policy- "resources ACCESSED from an anonymous IP address"- if something is ACCESSED, it has nothing to do with a sign-in policy.

upvoted 2 times

  **chikorita** 1 year, 9 months ago

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

upvoted 1 times

  **Holii** 1 year, 6 months 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, 9 months ago

Today I would solve all over Conditional Access.

upvoted 14 times

  **S60** 6 months, 1 week 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 2 times

  **syougun200x** 1 year, 3 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

  **AcTiVeGrEnAdE** Most Recent 2 months ago

1. A user risk policy / conditional access policy
2. A sign in risk policy / conditional access policy
3. A sign in risk policy / conditional access policy

Each answer can have more than 1 solution. Most tenants will just use risk-based conditional access policies to cover these scenarios but there is more than 1 way to get the desired results.



upvoted 1 times

  **noa808a** 3 months, 2 weeks ago

As of Mar 2025:



1. User Risk Policy
2. Sign In Risk Policy
3. Conditional Access Policy

upvoted 2 times

  **Frank9020** 5 months, 2 weeks ago

1. A user risk policy
2. A sign in risk policy
3. A conditional access policy

upvoted 3 times

  **RahulX** 10 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** 1 year, 4 months ago

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

upvoted 2 times

  **dule27** 1 year, 6 months ago



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



upvoted 3 times

  **ShoaibPKDXB** 1 year, 7 months ago

Correct

upvoted 1 times

  **den5\_pepito83** 2 years, 1 month ago  
ON EXAM 14/11/2022  
upvoted 4 times

  **Vaerox** 11 months, 3 weeks ago  
But was it correct?  
upvoted 1 times

## 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, 9 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 98 times

🗨️ 👤 **mb0812** 1 year, 3 months ago

Agree. We cannot set job title in Azure for a user synced from on-premise AD

upvoted 3 times

🗨️ 👤 **Magis** 2 years, 8 months ago

Agree. This answer is correct for sure.

upvoted 5 times

🗨️ 👤 **kanew** 2 years, 1 month ago

Agree 100% and tested.

upvoted 6 times

🗨️ 👤 **Silusha** 1 year, 9 months ago

Did you try to change the job title of User3?

upvoted 1 times

🗨️ 👤 **sbnpj** 2 years, 2 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, 10 months ago

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

upvoted 21 times

🗨️ 👤 **Fcnet** 2 years, 8 months ago

Job Title : only user2 & user3

Usage Location can be changed for U1,U2,U3

upvoted 1 times

🗨️ 👤 **SvenHorsheim** 2 years, 7 months 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** 2 years 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

🗨️ 👤 **AcTiVeGrEnAdE** Most Recent 2 months ago

I disagree with the provided answers. In my experience, no attributes may be modified in Entra Id for directory synced users and usage location is still controlled from ADDS for synced users. The question asks about making these changes in Entra ID. This can only be done for User 2 & User 3.

Maybe in a commercial tenant you are able to change usage location but I bet the sync engine will revert the changes on its next sync. In GCCH, you can try and change an attribute but it will just error out in the portal saying the user is directory synced.

upvoted 1 times

  **MicrosoftAdminUser** 2 months, 3 weeks ago

For cloud-only users, you can edit user properties directly in Azure AD. For synced users, properties must be managed in the on-premises directory, Microsoft Entra admin centre > Identity > Users > Select a Guest user >

Display name ✓

Email ✓

User principal name ✓


Job title ✕ (greyed out, cannot edit)

Usage location ✕ (greyed out, cannot edit)

Department ✕ (greyed out)

Company name ✕ (greyed out)

upvoted 1 times

  **Frank9020** 5 months, 2 weeks ago

Job title: Can be changed in Azure AD for non-synchronized members (User2).

Cannot be changed for synchronized members (User1) or guests (User3).

Usage location:


Can be changed in Azure AD for all users (User1, User2, and User3), regardless of synchronization status.

upvoted 1 times

  **BRZSZCL** 8 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** 9 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** 1 year, 4 months 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, 6 months ago

1. User2 and User3

2. User1, 2, 3

upvoted 1 times



  **JCKD4Ni3L** 1 year, 8 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, 9 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, 8 months ago

Correct answer:

- U2 and U3

- U1, U2 and U3

upvoted 1 times

  **StarMe** 1 year, 10 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, 10 months ago

1. User2 and User3 only



2. User1, User2 and User3

upvoted 1 times

  **Heshan** 1 year, 11 months ago

On the exam, 09/07/2023

upvoted 3 times

  **Sango** 1 year, 12 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** 2 years ago

Job Title : User2 and User3 only

Usage Location: User1,User2 and User3

upvoted 1 times

  **ShoaibPKDXB** 2 years, 1 month ago

Correct: 1. User2 and User3 only

2. User1, User2 and user3

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.  
 You need to ensure that User1 can create new catalogs and add resources to the catalogs they own.  
 What should you do?

- A. From the Roles and administrators blade, modify the Groups administrator role.
- B. From the Roles and administrators blade, modify the Service support administrator role.
- C. From the Identity Governance blade, modify the Entitlement management settings.
- D. From the Identity Governance blade, modify the roles and administrators for the General catalog.

**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.

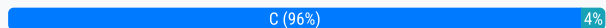
\* Service Support Administrator

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



**Hot\_156** Highly Voted 2 years, 9 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 22 times

**RahulX** 1 year, 4 months 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

**syogun200x** 1 year, 9 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, 10 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

**Aikendrum** Most Recent 2 weeks ago

**Selected Answer: C**

Its C

Sign in to the Azure portal. Use an account that has the necessary administrator rights (typically Global Administrator or a role with equivalent



permissions).

Navigate to Azure Active Directory. In the left-hand menu, select "Azure Active Directory".

Access Identity Governance and Entitlement Management. In the AAD pane, select "Identity Governance". Then, under Identity Governance, choose "Entitlement Management".

Locate Catalog Settings. Within Entitlement Management, find the settings related to catalog creation. (Depending on your portal view, this might be under a "Settings" or "Catalogs" section.)

Enable self-service catalog creation. Look for the option or toggle labeled "Self-service catalog creation" or similar. Switch it to the Enabled state.

Save Your Changes. Confirm and save the settings.

upvoted 1 times

🗲️ 👤 **Frank9020** 5 months, 2 weeks ago

**Selected Answer: D**

Option D correctly identifies the need to modify roles and administrators for the General catalog, enabling User1 to perform the required actions. In Azure Active Directory (Azure AD), the ability to manage catalogs and add resources to them is controlled through Identity Governance. Specifically:

Catalogs are used in Azure AD Entitlement Management to group resources and policies.

To allow a user to create new catalogs and manage them, you must assign them the appropriate role within the Identity Governance settings.

upvoted 1 times

🗲️ 👤 **csi\_2025** 4 months ago

D doesn't make sense since you want the user to modify his own catalogs not (just) the general one. It has to be C.

upvoted 1 times

🗲️ 👤 **Frank9020** 5 months ago

It is C: to create new catalog, has to be C

upvoted 1 times

🗲️ 👤 **ColdCut** 7 months, 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** 8 months ago

**Selected Answer: D**

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

upvoted 2 times

🗲️ 👤 **EmnCours** 1 year, 11 months ago

**Selected Answer: C**

[https://portal.azure.com/#view/Microsoft\\_AAD\\_ERM/DashboardBlade/~/\\_elmSetting](https://portal.azure.com/#view/Microsoft_AAD_ERM/DashboardBlade/~/_elmSetting)

Correct. C

upvoted 1 times

🗨️ 👤 **dule27** 1 year, 12 months ago

**Selected Answer: C**

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

upvoted 1 times

🗨️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

**Selected Answer: C**

Correct. C

upvoted 1 times

🗨️ 👤 **eleazarrrd** 2 years, 2 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** 2 years, 3 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, 6 months ago

**Selected Answer: C**

Correct answer is C.

upvoted 1 times

🗨️ 👤 **Imee** 2 years, 9 months ago

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

upvoted 3 times

🗨️ 👤 **Hot\_156** 2 years, 9 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, 9 months ago

The Answer is D my Friend

upvoted 1 times

🗨️ 👤 **Hot\_156** 2 years, 9 months ago

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

upvoted 3 times

🗨️ 👤 **Ltf** 2 years, 9 months ago

Seems it's D

upvoted 3 times

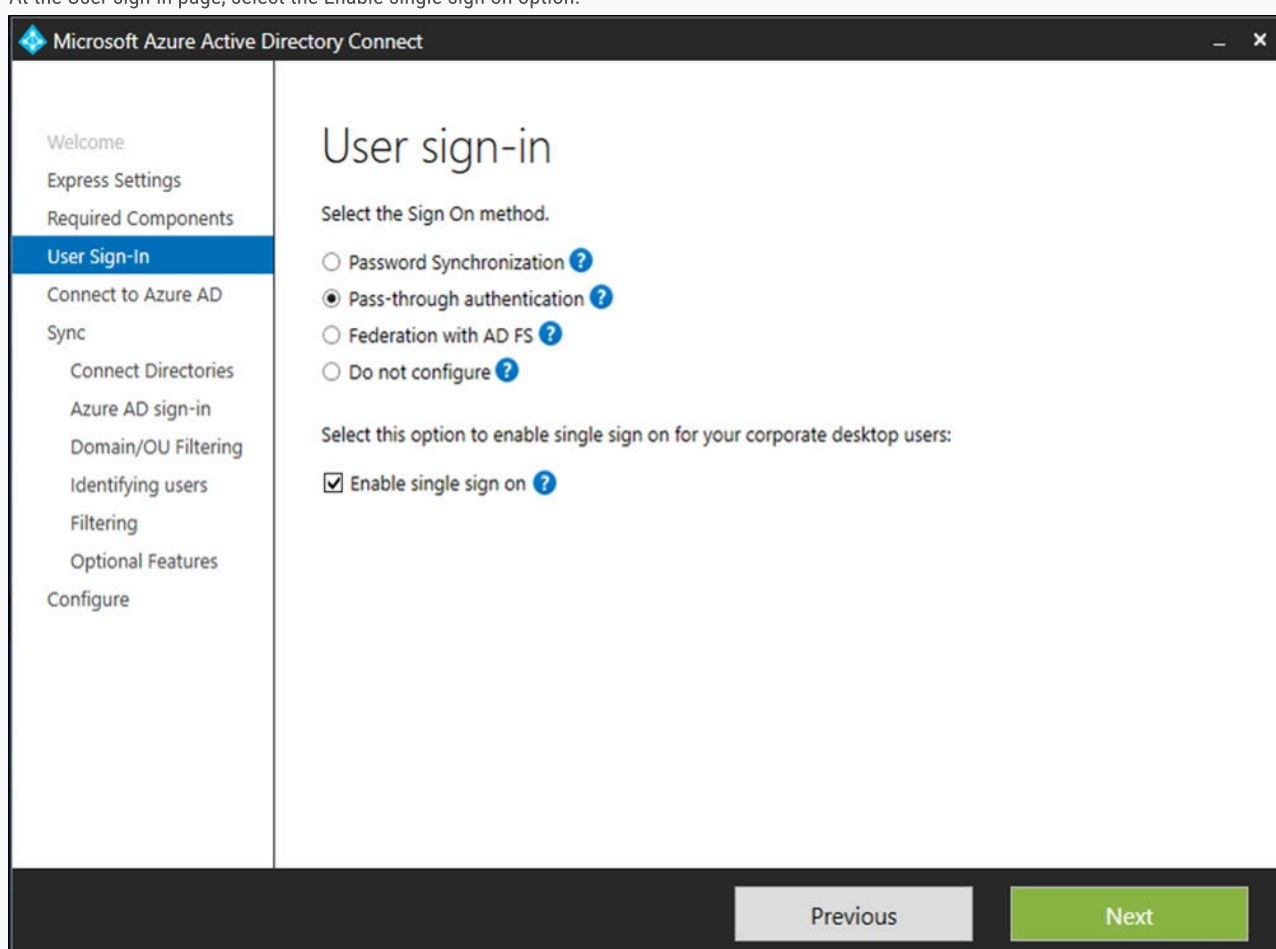
Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. Users sign in to computers that run Windows 10 and are joined to the domain. You plan to implement Azure AD Seamless Single Sign-On (Azure AD Seamless SSO). You need to configure the Windows 10 computers to support Azure AD Seamless SSO. What should you do?

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

**Suggested Answer: A**

Enable Seamless SSO through Azure AD Connect.

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



Note:

The option will be available for selection only if the Sign On method is Password Hash Synchronization or Pass-through Authentication. Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods.

Reference:

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

Community vote distribution

C (100%)

 **Shinolgarashi** Highly Voted 2 years, 9 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 30 times

🗨️ 👤 **jack987** 2 years, 6 months ago

I agree, the correct answer is C.

upvoted 2 times

🗨️ 👤 **Taigr** 2 years, 4 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** 2 years, 4 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 2 times

🗨️ 👤 **ColdCut** Most Recent 7 months, 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 3 times

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

Selected Answer: C

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

upvoted 1 times

🗨️ 👤 **Er\_01** 1 year, 5 months 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, 8 months ago

Answer is C

upvoted 1 times

🗨️ 👤 **BenLam** 1 year, 8 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, 8 months ago

**Selected Answer: C**

As in the previous page, answer is C.

upvoted 2 times

🗨️ 👤 **sherifhamed** 1 year, 9 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-ss.com>. This will allow the browser to send the Kerberos ticket to Azure AD and enable Seamless SSO

upvoted 2 times

🗨️ 👤 **sherifhamed** 1 year, 9 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** 1 year, 2 months 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, 10 months ago

**Selected Answer: C**

Answer is C

upvoted 1 times

🗨️ 👤 **EmnCours** 1 year, 11 months ago

**Selected Answer: C**

I agree, the correct answer is C.

upvoted 1 times

🗨️ 👤 **dule27** 1 year, 12 months ago

**Selected Answer: C**

C. Modify the Local intranet Zone settings.

upvoted 1 times

🗨️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

**Selected Answer: C**

C is correct

upvoted 1 times

🗨️ 👤 **DCT** 2 years, 3 months ago

walao, answer is C la, sohai

upvoted 1 times

🗨️ 👤 **mayleni** 2 years, 5 months ago

**Selected Answer: C**

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

upvoted 2 times

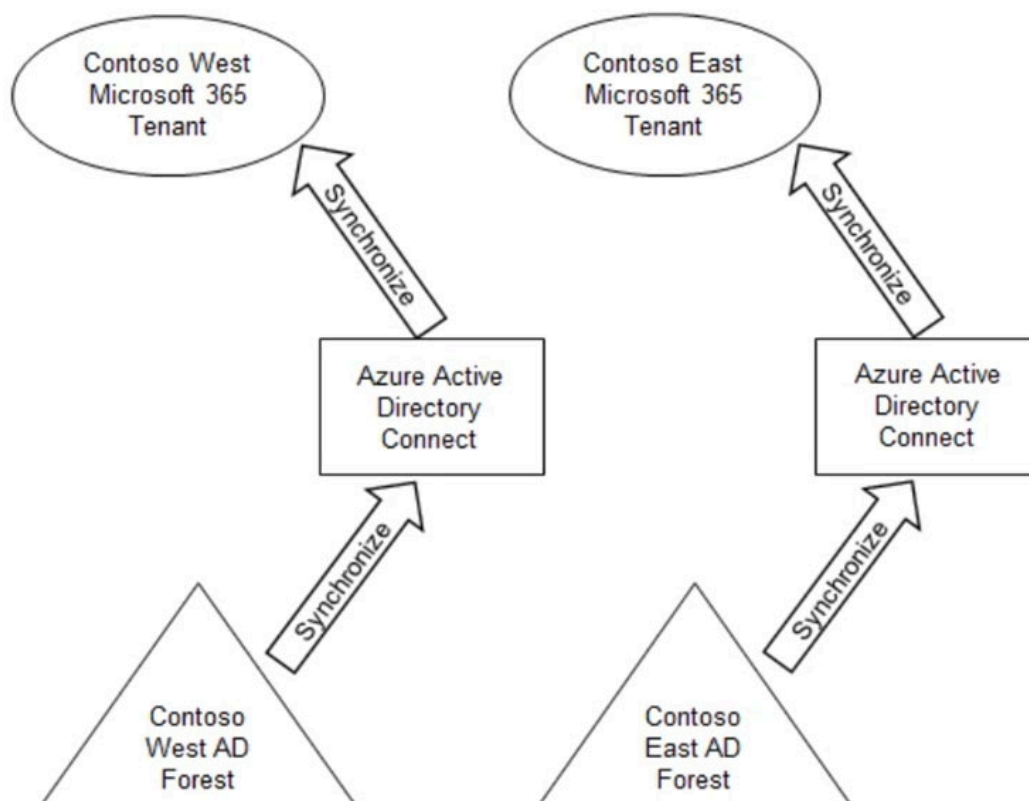
  **Halwagy** 2 years, 5 months ago

**Selected Answer: C**

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

upvoted 2 times

Your company has two divisions named Contoso East and Contoso West. The Microsoft 365 identity architecture for both divisions is shown in the following exhibit.



You need to assign users from the Contoso East division access to Microsoft SharePoint Online sites in the Contoso West tenant. The solution must not require additional Microsoft 365 licenses.

What should you do?

- A. Configure Azure AD Application Proxy in the Contoso West tenant.
- B. Invite the Contoso East users as guests in the Contoso West tenant.
- C. Deploy a second Azure AD Connect server to Contoso East and configure the server to sync the Contoso East Active Directory forest to the Contoso West tenant.
- D. Configure the existing Azure AD Connect server in Contoso East to sync the Contoso East Active Directory forest to the Contoso West tenant.

**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, 7 months ago

it should be stated as answer: configure cross-tenant access settings  
upvoted 8 times

**Holii** 2 years 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 2 times

  **ColdCut** Highly Voted 7 months, 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 6 times

  **RahulX** Most Recent 1 year, 4 months ago



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

upvoted 2 times

  **EmnCours** 1 year, 11 months ago

Correct Answer: B

upvoted 1 times

  **dule27** 1 year, 12 months ago

Selected Answer: B

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

upvoted 1 times

  **haskelatchi** 2 years, 1 month ago

B for Bob

upvoted 1 times

  **ShoaibPKDXB** 2 years, 1 month ago

Selected Answer: B

B is correct



upvoted 1 times

  **[Removed]** 2 years, 6 months ago

Selected Answer: B

B is the correct answer. No further licensing is required here. As LHADUK suggested though, cross-tenant access should be configured.

upvoted 3 times

  **taer** 2 years, 9 months ago

Selected Answer: B

Correct Answer: B

upvoted 5 times



DRAG DROP

-

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You need to ensure that User1 can create access reviews for groups, and that User2 can review the history report for all the completed access reviews. The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

### Roles

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**  2 years, 5 months ago

User 1 : User Administrator

User 2 : Security Reader

upvoted 61 times

 **klayytech** 1 year, 2 months 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 5 times

 **klayytech** 1 year, 3 months 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 5 times

  **HaubeRR89** 6 months, 2 weeks 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 4 times

  **Phil\_79** 1 week ago

Bro, the link you posted lists Security Readers among those who can read the history reports...

upvoted 1 times

  **oscarpopi** 2 years, 5 months ago

Correct

upvoted 3 times

  **doch**  2 years, 5 months ago

User Admin

Security Reader

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

upvoted 29 times

  **oscarpopi** 2 years, 5 months ago

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

upvoted 4 times

  **AcTiVeGrEnAdE**  2 months ago

The suggested answer is correct in regards to "least-privilege"

User 1 : User Administrator

User 2 : Security Reader

upvoted 1 times

  **Sir\_Miky** 2 months, 1 week ago


Following the least privilege principle, I believe that the Reports Reader role is the correct choice for User2 based on the specific requirement to review access review history reports. The Security Reader role is not necessary for this task as it focuses on security alerts and policies, which are not relevant to the requirement.

Therefore:

User 1: User Administrator

User 2: Reports Reader

upvoted 1 times

  **Bojana** 3 months, 3 weeks ago

User 1: User Administrator

User 2: Report Reader



To achieve this while adhering to the principle of least privilege, you can assign the following roles to User1 and User2:

User1: Assign the User Administrator role. This role allows User1 to create access reviews for groups.

User2: Assign the Reports Reader role. This role allows User2 to review the history report for all completed access reviews.

By assigning these specific roles, you ensure that each user has only the permissions necessary to perform their tasks, adhering to the principle of least privilege.

upvoted 1 times

  **krutesh** 4 months, 1 week ago

User1: User Administrator

User2: Reports Reader

The least privileged role that can create access reviews for groups in Azure Active Directory (Azure AD) is the "User Administrator" role. This role provides the necessary permissions to manage users and groups, including creating access reviews.

The least privileged role that can review the history report for all completed access reviews in Azure Active Directory (Azure AD) is the "Report

Reader" role. This role allows users to view various reports, including access review history reports, without granting them broader administrative permissions.

upvoted 2 times

🗨️ 👤 **Frank9020** 6 months, 2 weeks 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 2 times

🗨️ 👤 **ColdCut** 7 months, 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** 8 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 2 times

🗨️ 👤 **BRZSZCL** 8 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 4 times

🗨️ 👤 **hml\_2024** 9 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 groups<sup>1</sup>.

- \*\*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 permissions<sup>2</sup>.

upvoted 1 times

🗨️ 👤 **cluocal** 10 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** 10 months, 3 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** 1 year, 2 months 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** 12 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** 1 year, 2 months ago

User 1 : User Administrator

User 2 : Security Reader

upvoted 3 times

🗨️ 👤 **jtlucas99** 1 year, 2 months 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** 1 year, 3 months 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

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:

Role2:

 **dejo**  2 years, 5 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 31 times




 **ThotSlayer69**  2 years, 5 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 11 times

  **ColdCut**  7 months, 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 3 times

  **Labelfree** 7 months, 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** 8 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** 9 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** 1 year, 4 months ago

Role1: Microsoft.App (for containers).

Role2: Microsoft.Security.

upvoted 2 times

🗨️ 👤 **Siraf** 1 year, 6 months 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, 9 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, 10 months ago

It should 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, 11 months ago

Role 1: Microsoft.App

Role 2 : Microsoft.Security

upvoted 3 times

🗨️ 👤 **dule27** 2 years ago

Role 1: Microsoft.App

Role 2 : Microsoft.Security

upvoted 2 times

🗨️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

Correct: 1. Microsoft.Apps

2. Microsoft.Security

upvoted 3 times

🗨️ 👤 **kanew** 2 years, 1 month ago

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

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

upvoted 4 times

🗨️ 👤 **sbnpj** 2 years, 2 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** 2 years, 2 months ago

ChatGPT says its:

Role 1: Compute

Role 2: Network

upvoted 1 times

  **thadeus** 2 years, 2 months ago

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

upvoted 1 times

  **Holii** 2 years 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** 2 years, 4 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** 2 years 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



## 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:

Role:

**Suggested Answer:**

Object type:

Role:


 **Halwagy** Highly Voted 2 years, 5 months ago

Correct Answer:

Object Type: Administrative Unit

Role: Authentication administrator

upvoted 81 times

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

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

upvoted 33 times

 **Davito** Most Recent 7 months, 4 weeks 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 the AU (executives).

Therefore the answer is: Administrative Unit & Authentication Administrator  
upvoted 5 times

🗨️ 👤 **BRZSZCL** 8 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** 6 months, 4 weeks 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** 9 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 3 times

🗨️ 👤 **MISCOLO** 1 year ago

no such thing as a custom admin role

upvoted 2 times

🗨️ 👤 **SamuelPerezMartin** 11 months, 2 weeks ago

Microsoft Entra allows you to create custom admin roles.

upvoted 3 times

🗨️ 👤 **HartMS** 1 year, 2 months ago

AU

Authentication Administrator

upvoted 3 times

🗨️ 👤 **b0tag** 1 year, 10 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, 8 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 Passwords and regarding least privileg this IS the best role

upvoted 5 times

🗨️ 👤 **EmnCours** 1 year, 11 months ago

Object Type: Administrative Unit

Role: Authentication administrator

upvoted 4 times

🗨️ 👤 **dule27** 1 year, 11 months ago

Object Type: An Administrative Unit

Role: Authentication Administrator

upvoted 4 times

🗨️ 👤 **b233f0a** 2 years 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** 2 years ago

Object Type: An administrative unit

Role: Authentication administrator

upvoted 6 times

🗨️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

Correct: Object Type: An Administrative Unit

Role: Authentication Administrator

upvoted 2 times

🗨️ 👤 **rajbne** 2 years, 2 months ago

Please update final answer

upvoted 3 times

🗨️ 👤 **Remus999** 2 years, 2 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 3 times

🗨️ 👤 **Akakentavr** 2 years, 5 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** 2 years, 5 months ago

Object Type: Administrative Unit

Role: Authentication administrator

upvoted 1 times

🗨️ 👤 **ExamStudy68** 2 years, 2 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

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**  2 years, 5 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 40 times

 **CloudRat**  2 years, 5 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 7 times

 **test123123**  5 months, 3 weeks ago

**Selected Answer: D**

D. User2 and User3 only.

When you add a group to an administrative unit, only the group itself is brought into the management scope of the administrative unit, not the individual members of the group

upvoted 3 times

 **Labelfree** 7 months, 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** 8 months ago

**Selected Answer: D**

Respuesta correcta D

upvoted 1 times

🗨️ 👤 **Futfuyfyjfj** 1 year, 1 month 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** 1 year, 3 months ago

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

upvoted 3 times

🗨️ 👤 **haazybanj** 1 year, 8 months ago

Why is User1 not included?

upvoted 2 times

🗨️ 👤 **Nyamnyam** 1 year, 7 months ago

Because of what Halwagy has quoted and referenced above ;)

upvoted 2 times

🗨️ 👤 **EmnCours** 1 year, 10 months ago

**Selected Answer: D**

User2 and User3 only

upvoted 2 times

🗨️ 👤 **Husterix** 2 years 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** 2 years ago

**Selected Answer: D**

User2 and User3 only

upvoted 2 times

🗨️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

**Selected Answer: D**

D is correct

upvoted 1 times

🗨️ 👤 **oscarpopi** 2 years, 5 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** 2 years, 5 months ago

can i say that AU is also a Group and since adding a group in to an existing group will not make the root users a set of the master group(nested group). and hence the user1 will not be added and the other users were directly added and so the admin can act on them

upvoted 1 times

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

| Name  | Usage location | Department | Job title |
|-------|----------------|------------|-----------|
| User1 | United States  | Sales      | Associate |
| User2 | Finland        | Sales      | SalesRep  |
| User3 | Australia      | Sales      | Manager   |

You create a dynamic user group and configure the following rule syntax.

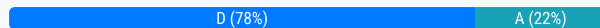
```
user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager") -or (user.jobTitle -eq "SalesRep")
```

Which users will be added to the group?

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

**Suggested Answer:** D

Community vote distribution



**ydecac** Highly Voted 2 years, 5 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 38 times
```

**[Removed]** 2 years, 2 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 19 times

**Nyamnyam** 1 year, 7 months 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 4 times

**Er\_01** 1 year, 4 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 4 times

**Justin0020** 1 year, 2 months 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 2 years, 5 months ago


**Selected Answer: D**

D is correct

always resolve according to precedence, first all the -and operators, only after that the -or operators.

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

upvoted 22 times

 **BRoald** 2 years, 3 months ago

D is wrong because User 2 is located in Finland and cannot be added to the dynamic group. I tested this and I'm 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 16 times

 **Holii** 2 years 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** 7 months, 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 5 months, 1 week ago

**Selected Answer: D**

User1 & User2

upvoted 1 times

 **Frank9020** 6 months, 2 weeks 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 5 times

🗨️ 👤 **Labelfree** 6 months, 3 weeks 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** 6 months, 3 weeks 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** 6 months, 4 weeks ago

**Selected Answer: D**

-and without brackets men's that only one condition is taken to -and  
upvoted 1 times

🗨️ 👤 **PrismaConsultores** 8 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** 8 months, 2 weeks ago

D (User1 and user2) is the correct answer. Confirmed in a Test Lab.  
upvoted 1 times

🗨️ 👤 **Chiragtrapasiya** 12 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** 1 year, 1 month ago

Tested this day :  
Answer D  
upvoted 1 times

🗨️ 👤 **vladi72** 1 year, 2 months 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** 1 year, 2 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** 1 year, 4 months 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, 6 months 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, 6 months ago

Correct Answer is D.

upvoted 1 times

🗨️ 👤 **Alscoran** 1 year, 7 months ago

**Selected Answer: D**

Because of the Or statement

upvoted 1 times

You have an Azure AD tenant that contains a user named User1.

User1 needs to manage license assignments and reset user passwords.

Which role should you assign to User1?

- A. Helpdesk administrator
- B. Billing administrator
- C. License administrator
- D. User administrator

**Suggested Answer:** D

Community vote distribution

D (100%)

BRZSZCL **Highly Voted** 8 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 8 times

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

**Selected Answer: D**

To enable User1 to manage license assignments and reset user passwords, you should assign the User Administrator role. This role provides the necessary permissions for both tasks.

upvoted 1 times

test123123 5 months, 3 weeks ago

**Selected Answer: D**

D. User Administrator

upvoted 1 times

jsca 1 year, 1 month ago

Correct Answer: D

upvoted 2 times

EmnCours 1 year, 11 months ago

Correct Answer: D

upvoted 1 times

dule27 2 years ago

**Selected Answer: D**

D. User administrator

upvoted 1 times

JN\_311 2 years ago

Selected Answer: D

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

upvoted 3 times

🗨️ 👤 **SwitchKat** 2 years, 1 month 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** 2 years 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** 2 years ago

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

upvoted 1 times

🗨️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

Selected Answer: D

correct D

upvoted 1 times

🗨️ 👤 **itismadu** 2 years, 2 months ago

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

upvoted 1 times

🗨️ 👤 **chikorita** 2 years, 3 months ago

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

upvoted 2 times

🗨️ 👤 **Aquintero** 2 years, 5 months ago

Administrador de Usuarios

upvoted 3 times

🗨️ 👤 **jojoseph** 2 years, 5 months ago

Selected Answer: D

User Administrator

upvoted 2 times

🗨️ 👤 **Halwagy** 2 years, 5 months ago

Selected Answer: D

User Administrator

upvoted 3 times

🗨️ 👤 **CloudRat** 2 years, 5 months ago

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

upvoted 3 times

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all users.

You 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%

 **shuhaidawahab** Highly Voted 1 year, 8 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 6 times

 **mohamedbenamor** Highly Voted 8 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

 **BRZSZCL** Most Recent 8 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** 9 months, 2 weeks ago

what the hell is going on with these answers?

upvoted 3 times

🗳️ 👤 **criminal1979** 1 year, 2 months ago

**Selected Answer: A**

Set-MsolUserLicense is the only way between the proposed answers

upvoted 2 times

🗳️ 👤 **Nyamnyam** 1 year, 7 months ago

**Selected Answer: A**

A. is the correct answer

upvoted 2 times

🗳️ 👤 **Sandipmcr** 1 year, 8 months ago

**Selected Answer: A**

Set-MsolUserLicense is the only way between the proposed answers

upvoted 2 times

🗳️ 👤 **morit2578** 1 year, 10 months ago

**Selected Answer: A**

Set-MsolUserLicense is the only way between the proposed answers

upvoted 2 times

🗳️ 👤 **amurp35** 1 year, 10 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, 10 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, 10 months ago

**Selected Answer: B**

A. the Set-MsolUserLicense cmdlet

upvoted 2 times

🗳️ 👤 **mali1969** 2 years 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** 2 years 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** 2 years ago

**Selected Answer: A**

A. the Set-MsolUserLicense cmdlet

upvoted 1 times

🗳️ 👤 **HOTDOGG** 2 years, 1 month 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** 2 years, 1 month 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** 2 years, 1 month ago

**Selected Answer: A**

Set-MsolUserLicense

upvoted 3 times

  **Aquintero** 2 years, 5 months ago

**Selected Answer: A**

A. el cmdlet Set-MsolUserLicense

upvoted 1 times

## HOTSPOT -

You have a Microsoft Entra tenant that contains a user named User1.

An administrator deletes User1.

You need to identify the following:

- What is the maximum number of days for which you have the option to restore the User1 account?
- Which is the least privileged role that can be used to restore User1?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Number of days:

  
15  
30  
90  
180

Role:

  
User Administrator  
Network Administrator  
Helpdesk Administrator  
Domain Name Administrator**Answer Area**


Number of days:

  
15  
30  
90  
180

**Correct Answer:**

Role:

  
User Administrator  
Network Administrator  
Helpdesk Administrator  
Domain Name Administrator

 **070dc8c** 3 months, 3 weeks ago

<https://learn.microsoft.com/en-us/entra/fundamentals/users-restore>

upvoted 2 times

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to a group that includes all the users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the Set-AzureADGroup cmdlet
- B. the Identity Governance blade in the Azure Active Directory admin center
- C. the Set-WindowsProductKey cmdlet
- D. the Set-MsolUserLicense cmdlet

**Suggested Answer: B**

Community vote distribution

D (100%)

🗳️ 👤 **SynnerG** 9 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** 9 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** 1 year ago

**Selected Answer: D**

Opcion D

upvoted 1 times

🗳️ 👤 **jsca** 1 year, 1 month ago

D. the Set-MsolUserLicense cmdlet

upvoted 2 times

🗳️ 👤 **jtlucas99** 1 year, 2 months ago

\*Add

Set-MsolUserLicenses cmdlet is deprecated. 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, 7 months 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, 8 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, 9 months ago

**Selected Answer: D**

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

upvoted 3 times

🗲️ 👤 **sherifhamed** 1 year, 9 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 Skuld>"
```

```
}
```

upvoted 4 times

🗲️ 👤 **dule27** 2 years ago

**Selected Answer: D**

D. the Set-MsolUserLicense cmdlet

upvoted 2 times

🗲️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

**Selected Answer: D**

D is correct

upvoted 2 times

🗲️ 👤 **AmplifiedStitches** 2 years, 2 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** 2 years, 2 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

🗲️ 👤 **AArif098** 2 years, 4 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** 2 years, 4 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** 2 years, 5 months ago

**Selected Answer: D**

D. el cmdlet Set-MsolUserLicense

upvoted 2 times

🗨️ 👤 **mayleni** 2 years, 5 months ago

**Selected Answer: D**

the same question again! Is D

upvoted 2 times

You have a Microsoft Entra tenant named contoso.com that contains an 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-MgUser cmdlet.
- B. Run the New-MgInvitation cmdlet.
- C. Configure the External collaboration settings.
- D. Implement Microsoft Entra Connect sync.

**Correct Answer: B**

  **Fijii** 4 months, 1 week ago


**Selected Answer: B**

Graph command invitation is the right answer (New-MgInvitation)  
upvoted 4 times

  **\_marc** 4 months, 2 weeks ago

**Selected Answer: C**

'that you can provide access'. External collab settings are there so you 'can' provide access. The command for invitation is when you 'do' provide access  
upvoted 1 times

  **Sunth65** 4 months, 2 weeks ago

**Selected Answer: B**

B. Run the New-MgInvitation cmdlet is the correct command !  
upvoted 3 times

HOTSPOT

-

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

You need to configure Azure AD Connect to meet the following requirements:

- User sign-ins to Azure AD must be authenticated by an Active Directory domain controller.
- Active Directory domain users must be able to use Azure AD self-service password reset (SSPR).

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

NOTE: Each correct selection is worth one point.

### Answer Area

Authentication by the domain controller:

Federation with Active Directory Federation Services (AD FS)  
Pass-through authentication  
Password hash synchronization

SSPR:

Device writeback  
Group writeback  
Password hash synchronization  
Password writeback

### Answer Area


Authentication by the domain controller:

Federation with Active Directory Federation Services (AD FS)  
**Pass-through authentication**  
Password hash synchronization

SSPR:

Device writeback  
Group writeback  
Password hash synchronization  
**Password writeback**

Suggested Answer:

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

pass- through auth  
password write back  
upvoted 24 times

 **naveenbio** Most Recent 6 months, 3 weeks 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** 10 months, 2 weeks ago

pass- through auth  
password write back  
upvoted 4 times

🗨️ 👤 **AMZ** 1 year ago  
Question valid - 06/23  
upvoted 4 times

🗨️ 👤 **mali1969** 1 year 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** 10 months, 2 weeks ago  
For 2nd requirement, it should be password write back. PHS doesn't help with SSPR  
upvoted 2 times

🗨️ 👤 **dule27** 1 year ago  
1. Pass- through authentication  
2. Password writeback  
upvoted 2 times

🗨️ 👤 **DoMing** 1 year, 2 months ago  
PTA and Password hash synchronization  
upvoted 1 times

🗨️ 👤 **kmk\_01** 1 year, 2 months 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** 1 year, 5 months 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** 1 year, 5 months ago  
The Answer is Correct  
upvoted 4 times

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all users.

You needed to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the Groups blade in the Azure Active Directory admin center
- B. the Set-AzureADGroup cmdlet
- C. the Identity Governance blade in the Azure Active Directory admin center
- D. the Set-MsolUserLicense cmdlet

**Suggested Answer:** D

Community vote distribution

D (100%)

🗳️ 👤 **Martyss** Highly Voted 2 years ago

At least they got it right on the 4th try lol  
upvoted 30 times

🗳️ 👤 **babadook13** 1 year, 5 months ago

:) good one  
upvoted 1 times

🗳️ 👤 **Labelfree** 7 months, 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 3 times

🗳️ 👤 **haskelatchi** Highly Voted 2 years, 1 month 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 13 times

🗳️ 👤 **070dc8c** Most Recent 3 months, 3 weeks ago

Selected Answer: A

Groups Blade as Set-Msoluserlicense is deprecated. <https://learn.microsoft.com/en-us/answers/questions/1371693/is-there-a-way-to-troubleshoot-an-unknown-error-wh>  
upvoted 1 times

🗳️ 👤 **noa808a** 3 months, 2 weeks ago

Incorrect. The E3 Licenses are assigned individually; therefore the groups blade will not be of assistance.  
upvoted 1 times

🗳️ 👤 **krisbla** 7 months, 2 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** 7 months, 3 weeks ago

lol, how many times is this question going to be asked?  
upvoted 3 times

🗳️ 👤 **sojorow324** 10 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** 11 months, 1 week ago

lol , how many times we have to answer it

upvoted 2 times

🗨️ 👤 **rajatn** 1 year ago

Same question is having different answer which is correct

upvoted 1 times

🗨️ 👤 **jtlucas99** 1 year, 2 months ago

Set-MgGroupLicense cmdlet

upvoted 1 times

🗨️ 👤 **shuhaidawahab** 1 year, 8 months ago

same as question before

upvoted 1 times

🗨️ 👤 **Firefarther** 1 year, 11 months ago

Set-MsolUserLicense would be correct but it is deprecated

upvoted 2 times

🗨️ 👤 **dule27** 2 years ago

**Selected Answer: D**

D. the Set-MsolUserLicense cmdlet

upvoted 2 times

🗨️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

**Selected Answer: D**

D is correct

upvoted 2 times

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

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

You have an Active Directory forest that syncs to an Azure 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** 8 months, 3 weeks ago

same as question before

upvoted 1 times

🗳️ 👤 **EmnCours** 10 months, 2 weeks ago

**Selected Answer: B**

B. No is correct answer

upvoted 3 times

🗳️ 👤 **mali1969** 1 year 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** 1 year ago

**Selected Answer: B**

B. No is correct answer

upvoted 2 times

🗳️ 👤 **haskelatchi** 1 year, 1 month ago

Another repeat question. The answer is obviously C

upvoted 1 times

🗳️ 👤 **kanew** 1 year, 1 month ago

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

upvoted 3 times



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

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

You have a Microsoft 365 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.

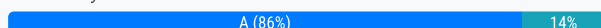
Does this meet the goal?

A. Yes

B. No

**Suggested Answer: A**

Community vote distribution



**AMZ** Highly Voted 1 year, 2 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 20 times

**kmk\_01** 1 year, 2 months ago

Thanks for the link.

upvoted 4 times

**RoelvD** Highly Voted 7 months, 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 8 times

**Frank9020** Most Recent 6 months, 2 weeks 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 2 times

**shuhaidawahab** 8 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** 11 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** 1 year 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 6 times

🗳️ 👤 **mali1969** 1 year 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** 1 year 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** 1 year ago

**Selected Answer: A**

A. Yes is the correct answer  
upvoted 1 times

🗳️ 👤 **ShoaibPKDXB** 1 year, 1 month ago

**Selected Answer: A**

correct  
upvoted 1 times

🗳️ 👤 **ShoaibPKDXB** 1 year, 1 month ago

**Selected Answer: B**

B is correct  
upvoted 1 times

  **LeonLau** 1 year, 1 month ago

No, A is the correct answer.

Only the following 4 role can update identity secure score

Global administrator

Security administrator

Exchange administrator

SharePoint administrator

upvoted 1 times

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

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

You have a Microsoft 365 E5 subscription.

You create a user named User1.

You need to ensure that User1 can update the status of Identity Secure Score improvement actions.

Solution: You assign the User Administrator role to User1.


Does this meet the goal?

- A. Yes
- B. No

**Suggested Answer: B**

Community vote distribution

B (100%)

 **Labelfree** 6 months, 3 weeks 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** 8 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** 1 year, 1 month 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, 11 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, 12 months ago

**Selected Answer: B**

B. NO is the correct answer  
upvoted 1 times

🗨️ 👤 **m4rv1n** 2 years, 1 month 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 4 times

🗨️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

**Selected Answer: B**

Correct B

upvoted 1 times

🗨️ 👤 **boapaulo** 2 years, 2 months ago

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

upvoted 1 times

## HOTSPOT

-

## Case Study

-

## Overview

-

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

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

## Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso\_Resources. The Contoso\_Resources OU contains all users and computers.

The contoso.com Active Directory domain contains the relevant users shown in the following table.

| Name   | Office   | Department |
|--------|----------|------------|
| Admin1 | Montreal | Helpdesk   |
| User1  | Montreal | HR         |
| User2  | Montreal | HR         |
| User3  | Montreal | HR         |
| Admin2 | London   | Helpdesk   |
| User4  | London   | Finance    |
| User5  | London   | Sales      |
| User6  | London   | Sales      |
| Admin3 | Seattle  | Helpdesk   |
| User7  | Seattle  | Sales      |
| User8  | Seattle  | Sales      |
| User9  | Seattle  | Sales      |

Contoso also includes a marketing department that has users in each office.

## Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

- Microsoft Office 365 Enterprise E5
- Enterprise Mobility + Security E5
- Windows 10 Enterprise E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- The users in the London office have the Microsoft 365 Phone System license unassigned.
- The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

#### Existing Environment. Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

#### Requirements. Planned Changes

-

Contoso plans to implement the following changes:

- Implement self-service password reset (SSPR).
- Analyze Azure audit activity logs by using Azure Monitor.
- Simplify license allocation for new users added to the tenant.
- Collaborate with the users at Fabrikam on a joint marketing campaign.
- Configure the User administrator role to require justification and approval to activate.
- Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

#### Requirements. Technical Requirements

Contoso identifies the following technical requirements:

- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

You need to meet the technical requirements for license management by the help desk administrators.

What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Object to create for each branch office:

An administrative unit  
A custom role  
A Dynamic User security group  
An OU

Tool to use:

Azure Active Directory admin center  
Active Directory Administrative Center  
Active Directory module for Windows PowerShell  
Microsoft Purview Compliance portal

### Answer Area

Object to create for each branch office:

An administrative unit  
A custom role  
A Dynamic User security group  
An OU


Suggested Answer:

Tool to use:

Azure Active Directory admin center  
Active Directory Administrative Center  
Active Directory module for Windows PowerShell  
Microsoft Purview Compliance portal

 **kijken** Highly Voted 1 year, 7 months 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 19 times

 **mikekrt** Highly Voted 1 year, 9 months ago

correct  
upvoted 11 times

 **dann\_S** Most Recent 9 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 presented use case). Otherwise I would have definitely agreed with an AU and Entra (Azure) admin center.

Box 4 = an OU

Box 2 = Active Directory Administrative Center

upvoted 3 times

 **test123123** 5 months, 3 weeks ago


You manage the licences in the cloud, not onprem.  
upvoted 1 times



☐  **Sunth65** 6 months ago

Correct answer

upvoted 1 times

☐  **jsca** 1 year, 1 month ago

answer is correct


upvoted 2 times

☐  **haazybanj** 1 year, 8 months ago

box1= Dynamic group

box = Azure admin center

upvoted 2 times

☐  **kijken** 1 year, 7 months ago

first is administrative unit, please read what that is

upvoted 3 times

☐  **haazybanj** 1 year, 7 months ago

You're right

upvoted 3 times

☐  **haazybanj** 1 year, 7 months ago

Box1= Administrative unit

upvoted 1 times

☐  **hw121693** 1 year, 11 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, 11 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, 11 months ago

you cannot apply a role to a dynamic security group - tested

upvoted 4 times

## Case Study -

## Overview -

ADatum Corporation is a consulting company in Montreal.

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

## Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

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

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | None                              |
| User2 | None                              |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner | Members                        |
|-------------|----------|-----------------|-------|--------------------------------|
| IT_Group1   | Security | Assigned        | None  | All users in the IT department |
| AdatumUsers | Security | Assigned        | None  | User1, User2                   |

## Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

## Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

## Requirements. Planned Changes -

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

## Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You need to resolve the issue of 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**  10 months 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 7 times

  **penatuna** 10 months 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

  **test123123** Most Recent 5 months, 3 weeks ago

**Selected Answer: A**

It sounds like the sales department users are hitting the default device limit set in Azure AD. To resolve this issue, you can increase the maximum number of devices that each user can join to Azure AD. Here's how you can do it:

Sign in to the Azure portal:

Go to Azure portal and sign in with your admin account.

Navigate to Azure Active Directory:

In the left-hand navigation pane, select Azure Active Directory.

Go to Devices:

Under Manage, select Devices.

Configure Device Settings:

Select Device settings.

Under Maximum number of devices per user, increase the limit to a higher number that suits your organization's needs.

Save the changes:

Click Save to apply the new device limit.

By increasing the device limit, users in the sales department will be able to join more devices to Azure AD without needing to contact the support department.

upvoted 1 times

  **ELQUMS** 10 months, 1 week ago

**Selected Answer: A**

Answer A



upvoted 2 times

  **Siraf** 1 year ago

Answer is A

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

upvoted 3 times

  **marsot** 1 year, 5 months 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** 1 year, 5 months ago

**Selected Answer: A**

Correct. Issue is:

"Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit."

Within Device settings, you can increase maximum number of devices a user can join/register to Azure AD.  
upvoted 4 times

## Case Study -

## Overview -

ADatum Corporation is a consulting company in Montreal.

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

## Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

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

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | None                              |
| User2 | None                              |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner | Members                        |
|-------------|----------|-----------------|-------|--------------------------------|
| IT_Group1   | Security | Assigned        | None  | All users in the IT department |
| AdatumUsers | Security | Assigned        | None  | User1, User2                   |

## Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

## Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

## Requirements. Planned Changes -

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

## Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You need to resolve the issue of IT\_Group1.

What should you do first?

- A. Change Membership type of IT\_Group1 to Dynamic User.
- B. Recreate the IT\_Group1 group.
- C. Change Membership type of IT Group1 to Dynamic Device.
- D. Add an owner to IT\_Group1.

**Suggested Answer: B**

*Community vote distribution*

B (100%)

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

And when recreating, set isAssignableToRole. <https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept>  
upvoted 17 times

 **AlexBrazil** Highly Voted 8 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 8 times

  **Studytime2023** Most Recent 1 year, 7 months 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, 7 months 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, 7 months 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, 10 months ago

**Selected Answer: B**

recreate group, set isAssignableToRole

upvoted 3 times

  **mali1969** 1 year, 10 months ago

Correct answer is "Add an owner to IT\_Group1"

upvoted 1 times

  **mali1969** 1 year, 10 months ago

and also answer A is corrected

A. Change Membership type of IT\_Group1 to Dynamic User

upvoted 1 times



## Case Study -

## Overview -

ADatum Corporation is a consulting company in Montreal.

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

## Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

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

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | 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**  1 year, 9 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 16 times

🗄️ 👤 **Alcpt** 1 year, 1 month ago

i had to do some research but its definitely A as per MS video at 1:45.

<https://youtu.be/9T6IKEloq0Q>

upvoted 2 times

🗄️ 👤 **Obyte** Highly Voted 👍 1 year, 9 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 10 times

🗄️ 👤 **AlexBrazil** Most Recent 🕒 7 months, 4 weeks 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** 1 year, 5 months 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, 6 months 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, 9 months ago

Selected Answer: A

No trust = Cloud sync

upvoted 6 times

🗄️ 👤 **ServerBrain** 1 year, 10 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, 10 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, 11 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, 11 months ago

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

upvoted 4 times

You have the Azure resources shown in the following table.

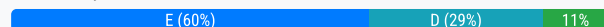
| Name   | Description                                               |
|--------|-----------------------------------------------------------|
| User1  | User account                                              |
| Group1 | Security group that uses the Dynamic user membership type |
| VM1    | Virtual machine with a system-assigned managed identity   |
| App1   | Enterprise application                                    |
| RG1    | Resource group                                            |

To which identities can you assign the Contributor role for RG1?

- A. User1 only
- B. User1 and Group1 only
- C. User1 and VM1 only
- D. User1, VM1, and App1 only
- E. User1, Group1, VM1, and App1

**Suggested Answer: E**

Community vote distribution



**pokr26** Highly Voted 1 year, 6 months 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 and to those groups you can't assign role. So answer is:

User1, VM1, App1  
upvoted 17 times

**sabas4** 1 year, 5 months 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 10 times

**j11v0sud** Highly Voted 1 year, 9 months ago

**Selected Answer: E**

Tested in-lab, FYI user-assigned managed identity works also  
upvoted 8 times

**AcTiVeGrEnAdE** Most Recent 2 months ago

**Selected Answer: D**

D is the only answer that fits here. You CANNOT assign an Azure resource role to a group that has dynamic group membership. What does qualify for role assignments are users, groups, service principals, and managed identities.  
upvoted 1 times

**Bojana** 3 months, 3 weeks ago

**Selected Answer: D**

Dynamic groups cannot be assigned roles in Azure RBAC. Only static groups, individual users, service principals, and managed identities are supported for role assignments.  
upvoted 1 times

**YesPlease** 4 months, 1 week ago

Selected Answer: E

Answer) E

In Azure, you can assign the Contributor role to users, groups, service principals, or managed identities. This means you can give a user, a group of users, an application (service principal), or a system-assigned identity the ability to create and manage most Azure resources within a specified scope.

upvoted 1 times

🗨️ 👤 **JohnnyChimpo** 5 months, 1 week ago

Selected Answer: E

Tested in my tenant. Dynamically assigned groups allow CONTRIBUTOR assignment for Azure resources. It is only AzureAD roles that are not allowed for dynamically assigned security groups

upvoted 2 times

🗨️ 👤 **Oskarma** 5 months, 2 weeks ago

Selected Answer: E

If you go to IAM in a Resource Group, you can choose a dynamic user assigned group.  
The limitation is only with Entra Roles. Tested in my tenant.

upvoted 3 times

🗨️ 👤 **test123123** 5 months, 3 weeks ago

Selected Answer: D

D. User1, VM1, App1

upvoted 1 times

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

Selected Answer: D

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

upvoted 1 times

🗨️ 👤 **Marius12345** 7 months, 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 2 times

🗨️ 👤 **AlexBrazil** 7 months, 4 weeks 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** 11 months, 1 week ago

User, group and application (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** 1 year, 1 month 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** 1 year, 2 months 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, 7 months 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 5 times

  **Nyamnyam** 1 year, 7 months 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 5 times

  **ACSC** 1 year, 9 months ago

**Selected Answer: E**

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

upvoted 6 times



## HOTSPOT

-

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

You need to configure External collaboration settings for the tenant to meet the following requirements:

- Guest users must be prevented from querying staff email addresses.
- Guest users must be able to access the tenant only if they are invited by User1.

Which three settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Guest user access restrictions:

- Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite restrictions:

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member
- Only users assigned to specific admin roles can invite guest users
- No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service  
sign up via user flows:

- No
- Yes

## Answer Area

Guest user access restrictions:

Guest users have the same access as members (most inclusive)  
Guest users have limited access to properties and memberships of directory objects  
**Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)**

Suggested Answer:

Guest invite restrictions:

Anyone in the organization can invite guest users including guests and non-admins (most inclusive)  
Member users and users assigned to specific admin roles can invite guest users including guests with member  
**Only users assigned to specific admin roles can invite guest users**  
No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service  
sign up via user flows:

**No**  
Yes

 **Roelvd** 7 months, 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

 **Giuseppe\_Geraci** 1 month, 2 weeks ago

the question is correct. You are asking how to restrict the invitation to user 'user1' only.

Where is it written that there are multiple global admins in this case? Where is it written that there is a user admin? Why do you have to invent situations that are not required in the question?

upvoted 1 times

 **Nyamnyam** 7 months, 3 weeks ago

Correct

upvoted 3 times

 **sehlohomoletsane** 9 months, 3 weeks ago

tested in lab

the answer is correct

upvoted 4 times

 **ServerBrain** 10 months, 1 week ago

100% correct

upvoted 3 times

 **EmnCours** 10 months, 2 weeks ago

Correct

upvoted 2 times

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all users.

You 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, 10 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** 1 year, 5 months 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 2 times

 **AcTiVeGrEnAdE** Most Recent 2 months ago


**Selected Answer: D**

Out dated question but the the answer would have been D if licensing still existed in Entra Id.  
upvoted 3 times

 **Oskarma** 5 months, 2 weeks ago

**Selected Answer: D**

No one, since recently Microsoft has retired the possibility of managing licenses from the Entra ID (formerly Azure AD) portal.  
If you see this question in exam, probably it will say "the Licenses blade in the Microsoft 365 admin center".  
upvoted 3 times

 **test123123** 5 months, 3 weeks ago


**Selected Answer: D**

D is the way.

Powershell

Set-AzureADUserLicense or Set-MgUserLicense or Set-MsolUserLicense.

upvoted 3 times

 **josemariamr** 6 months, 3 weeks 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 3 times

 **Davito** 7 months, 4 weeks 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** 11 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** 1 year, 1 month 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** 1 year, 2 months 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, 6 months 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, 10 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, 10 months ago

Agree. it should be powershell script

upvoted 1 times

  **stai** 1 year, 10 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** 11 months, 1 week ago

But your docs refers to Microsoft Graph ?

upvoted 1 times

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

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

You have a Microsoft 365 E5 subscription.

You create a user named User1.

You need to ensure that User1 can update the status of Identity Secure Score improvement actions.

Solution: You assign the Security Operator role to User1.

Does this meet the goal?


A. Yes

B. No

**Suggested Answer: B**

Community vote distribution

B (100%)

 **nils241** Highly Voted 11 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 15 times

 **test123123** Most Recent 5 months, 3 weeks ago

**Selected Answer: B**

Global administrator

Security administrator

Exchange administrator

SharePoint administrator

upvoted 3 times

 **sehlohomoletsane** 9 months, 3 weeks ago

**Selected Answer: B**

The answer is no

upvoted 2 times

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

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

You have a Microsoft 365 E5 subscription.

You create 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**  1 year, 11 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 8 times

 **SynnerG**  9 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, 10 months ago

**Selected Answer: A**

A. Yes

upvoted 1 times

 **1c67a2c** 1 year, 11 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

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%)

 **hellawait111** Highly Voted 1 year, 11 months ago

**Selected Answer: C**

Role explained here:

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

upvoted 18 times


 **Logitech** 1 year, 9 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 do more than this 3 things.

With Helpdesk Admin you can do more. Really stupid MS Question again....

D should be the answer.

upvoted 9 times

 **Alcpt** 1 year, 1 month 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** 6 months, 2 weeks 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 6 times



🗨️ 👤 **Giuseppe\_Geraci** 1 month, 2 weeks ago

The question says: ONLY. Helpdesk can do more.

upvoted 1 times

🗨️ 👤 **Nyamnyam** Highly Voted 👍 1 year, 7 months 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 14 times

🗨️ 👤 **AcTiVeGrEnAdE** Most Recent 🕒 2 months ago

Selected Answer: D

This question tests reading comprehension. While the Helpdesk Administrator role meets the following requirements:

Create and manage Azure support tickets

microsoft.azure.supportTickets/allEntities/allTasks

Read and configure Service Health in the Microsoft 365 admin center

microsoft.office365.serviceHealth/allEntities/allTasks

Create and manage Microsoft 365 service requests

microsoft.office365.supportTickets/allEntities/allTasks

the questions is asking for least privilege to only allow what is listed above and that can only be done with a custom role.....so D is the answer.

upvoted 1 times

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

Selected Answer: D

Answer) D

Helpdesk Administrator CANNOT configure service health...so this is why answer is D and not "Helpdesk Administrator"

upvoted 1 times

🗨️ 👤 **vdnh00** 4 months, 3 weeks ago

Selected Answer: C

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

upvoted 2 times

🗨️ 👤 **penatuna** 9 months ago

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

upvoted 1 times

🗨️ 👤 **omnomsnom** 1 year ago

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

upvoted 1 times

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

Selected Answer: C

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

upvoted 1 times

🗨️ 👤 **Justin0020** 1 year, 2 months 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** 1 year, 3 months 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 4 times

🗨️ 👤 **Er\_01** 1 year, 4 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, 5 months 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 5 times

🗨️ 👤 **marco\_aimi** 1 year, 6 months ago

"minimize administrative effort" using custom role? hum..  
upvoted 5 times

🗨️ 👤 **RoelvD** 1 year, 6 months ago

**Selected Answer: D**

"can perform only".. Helpdesk admin can do more then that. So D.  
upvoted 5 times

🗨️ 👤 **onelove01** 1 year, 6 months 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 8 times

🗨️ 👤 **Alscoran** 1 year, 7 months 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, 7 months ago

**Selected Answer: D**

Least privileged option is D. C can be, but has too much permissions  
upvoted 6 times

HOTSPOT

-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

You need to ensure that user authentication always occurs by validating passwords against the AD DS domain.

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

NOTE: Each correct selection is worth one point.

### Answer Area

Configure:  ▼

- Azure AD Password protection
- Cross-tenant synchronization
- Pass-through authentication
- Password hash synchronization

Use:  ▼

- Azure AD Connect
- Microsoft Identity Manager (MIM)
- The Microsoft Entra admin center
- The Microsoft Purview compliance portal

### Answer Area


Suggested Answer:

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 1 year, 4 months ago

Correct. PTA using AD Connect

upvoted 11 times

 **penatuna** Highly Voted 1 year, 3 months 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 two 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 5 times

  **Wicke**  1 year, 3 months 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

  **Futfuyfyfj** 8 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** 1 year, 4 months 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

  **Futfuyfyfj** 8 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** 1 year, 4 months ago

Correct Answer

upvoted 2 times

  **sehlohomoletsane** 1 year, 4 months ago

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

upvoted 1 times

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

### Guest user access

Guest user access restrictions ⓘ

[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@fabrikam.com | A user in fabrikam.com                                  |

Which users will be emailed a passcode?

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

**Suggested Answer: A**

Community vote distribution

B (51%)

A (49%)

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 26 times

 **Max\_He** Highly Voted 1 year, 2 months 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 12 times

 **krisbla** 7 months, 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 2 times

 **Nail** 8 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** 8 months, 2 weeks ago

My bad, it's right there in your text and I found the documentation for it.

upvoted 1 times

 **Giuseppe\_Geraci** Most Recent 1 month, 2 weeks ago

**Selected Answer: A**

User2 only, It will receive a one-time passcode email because:

They are not part of the tenant.

They haven't accessed any resources before.

Their email is not part of Azure AD or federated.

OTP is the fallback authentication mechanism for such guests.

upvoted 1 times

 **Kevin\_17** 1 month, 3 weeks ago

**Selected Answer: B**

has to be B

upvoted 1 times

 **LeoBarbas** 3 months, 1 week ago



**Selected Answer: B**

- User1 (User1@contoso.com) will receive a passcode if their authentication method is not stored.

- User2 (User2@outlook.com) will not receive a passcode because they are not yet invited.

- User3 (User3@fabrikam.com) will not receive a passcode as they are an internal user.

upvoted 1 times

  **noa808a** 3 months, 2 weeks ago

**Selected Answer: A**

The question is testing your knowledge of WHEN passcodes are sent. One-Time Passcodes for invitations are not sent to existing users. Therefore, A is correct.

upvoted 2 times

  **ElWhitepages** 3 months, 2 weeks ago

**Selected Answer: A**

In this scenario, only User2 ends up receiving a one-time passcode. Here's why:

User1 is already a guest in the tenant (B2B account). Since they have an existing guest identity in Fabrikam's Azure AD, they can sign in with their existing credentials rather than needing a one-time passcode.

User2 has never accessed Fabrikam, so when first invited, they are treated as a new external user. Because the tenant's settings allow guests from "any domain" and one-time passcodes are enabled, User2 will be emailed a passcode for sign-in.

User3 is an internal user in Fabrikam (same domain), so they already have a native Fabrikam account. They will authenticate as a regular member, not via a guest passcode flow.

Thus, with the tenant configured for one-time passcodes (and no existing guest account for User2), User2 is the only one who will receive an emailed passcode.

upvoted 1 times

  **d1e85d9** 3 months, 3 weeks ago

**Selected Answer: B**

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.

upvoted 1 times

  **mediamarkt** 3 months, 4 weeks ago

**Selected Answer: B**

has to be B



upvoted 1 times

  **PD1** 5 months, 1 week ago

**Selected Answer: A**

User2 only

upvoted 1 times

  **josemariamr** 6 months, 3 weeks ago

**Selected Answer: B**

Outlook is Microsoft account and is authenticated by Microsoft itself without needing passcodes.

upvoted 2 times

  **Davito** 7 months, 4 weeks 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** 7 months, 4 weeks 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** 8 months ago

**Selected Answer: B**

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

upvoted 2 times

🗨️ 👤 **N0cturnal** 8 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 3 times

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

Should be A.

upvoted 2 times

🗨️ 👤 **maomaopass** 1 year, 2 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%20for%20this%20feature%20provides>

passcode#:~:text=one%2Dtime%20passcodes-,The%20email%20one%2Dtime%20passcode%20feature%20is%20now%20turned%20on%20by%20default%20for%20this%20feature%20provides

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

upvoted 1 times

🗨️ 👤 **Alcpt** 1 year, 2 months 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 4 times



You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

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

**Suggested Answer: A**

Community vote distribution

B (100%)

  **throwaway10188** 11 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** 1 year, 2 months 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** 1 year, 2 months ago

**Selected Answer: B**

B as per the other questions

upvoted 3 times

  **MS\_RF** 1 year, 2 months ago

**Selected Answer: B**

B of course

upvoted 2 times

  **JCKD4Ni3L** 1 year, 2 months ago

**Selected Answer: B**

B is the correct answer...

upvoted 1 times

  **shuhaidawahab** 1 year, 2 months ago

REPEATED QUESTIONS

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

Note:

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

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

2. the Set-MsolUserLicense cmdlet

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

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

upvoted 1 times

  **Ed2learn** 1 year, 2 months 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** 1 year, 2 months 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** 1 year, 2 months 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

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%)

  **sn0rlaxxx** Highly Voted  5 months ago

**Selected Answer: A**

Microsoft Entra users can be synchronized between tenants. (Groups, devices, and contacts aren't currently supported.)

[https://learn.microsoft.com/en-us/entra/identity/multi-tenant-organizations/cross-tenant-synchronization-overview?form=MG0AV3#cross-tenant-synchronization-setting~:text=Microsoft%20Entra%20users%20can%20be%20synchronized%20between%20tenants.%20\(Groups%2C%20devices%2C%20and%20contacts%20](https://learn.microsoft.com/en-us/entra/identity/multi-tenant-organizations/cross-tenant-synchronization-overview?form=MG0AV3#cross-tenant-synchronization-setting~:text=Microsoft%20Entra%20users%20can%20be%20synchronized%20between%20tenants.%20(Groups%2C%20devices%2C%20and%20contacts%20)  
upvoted 8 times

  **AcTiVeGrEnAdE** **Most Recent**  2 months ago

**Selected Answer: A**

Answer is correct. While you can target a security group of users...only the users will sync over. Group objects will not sync.

upvoted 1 times

  **noa808a** 3 months, 2 weeks ago

**Selected Answer: A**

Answer is correct.  
upvoted 1 times

  **rvln7** 4 months, 1 week ago

**Selected Answer: A**

only users can be synchronized between tenants!  
upvoted 1 times

  **PD1** 5 months, 1 week ago

**Selected Answer: D**

All can sync.

upvoted 1 times

  **d1e85d9** 3 months, 3 weeks ago

Dumb one:

clearly explain here Answer will be "A"

<https://learn.microsoft.com/en-us/entra/identity/multi-tenant-organizations/cross-tenant-synchronization-overview?form=MG0AV3#cross-tenant-synchro>  
setting::~text=Microsoft%20Entra%20users%20can%20be%20synchronized%20between%20tenants.%20(Groups%2C%20devices%2C%20and%20contacts'  
upvoted 1 times

  **Frank9020** 5 months, 2 weeks ago

**Selected Answer: B**

Only users and security groups are synchronized. Microsoft 365 groups are not included in cross-tenant synchronization.  
upvoted 1 times

  **anonymousarpanch** 5 months, 2 weeks ago


**Selected Answer: A**

Ignore my previous response. After further studying the user and groups assignments, apparently it is now known that the scoping for groups is only to select the users and the group itself is not synchronised to target tenant. This has been clarified by Microsoft in Multitenant org FAQ. Sometimes, I wonder why don't they give everything in one place?. Learning one thing in azure takes so much time. And then after 3 months they change the entire setting.  
upvoted 1 times

  **anonymousarpanch** 5 months, 2 weeks ago

**Selected Answer: B**

May sound weird. But now, we Can sync user and groups. M365 groups are not supported. This is as per latest Microsoft documentation. Lookout for 'what is cross-tenant synchronization'. There is a hyperlink 'scoping users or groups to be provisioned with scoping filters'. Go through it..which should clarify  
upvoted 1 times

  **test123123** 5 months, 3 weeks ago

**Selected Answer: D**



<https://learn.microsoft.com/en-us/entra/identity/multi-tenant-organizations/cross-tenant-synchronization-configure#step-7-define-who-is-in-scope-for-provisioning>

You can sync both users and groups.  
upvoted 2 times

  **Sunth65** 6 months 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** 6 months, 1 week ago

**Selected Answer: A**

correct chatgpt  
upvoted 1 times

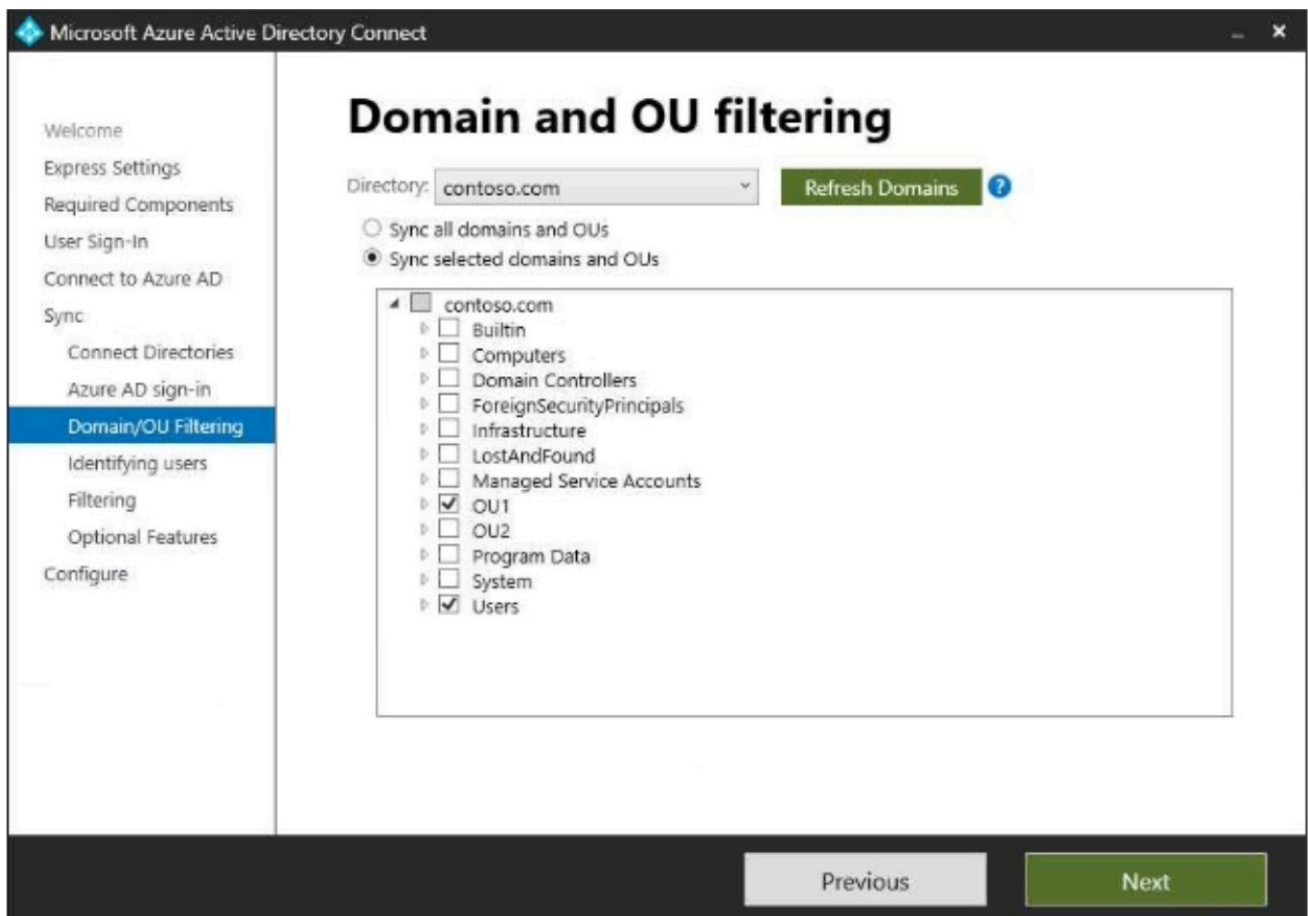
## HOTSPOT

-

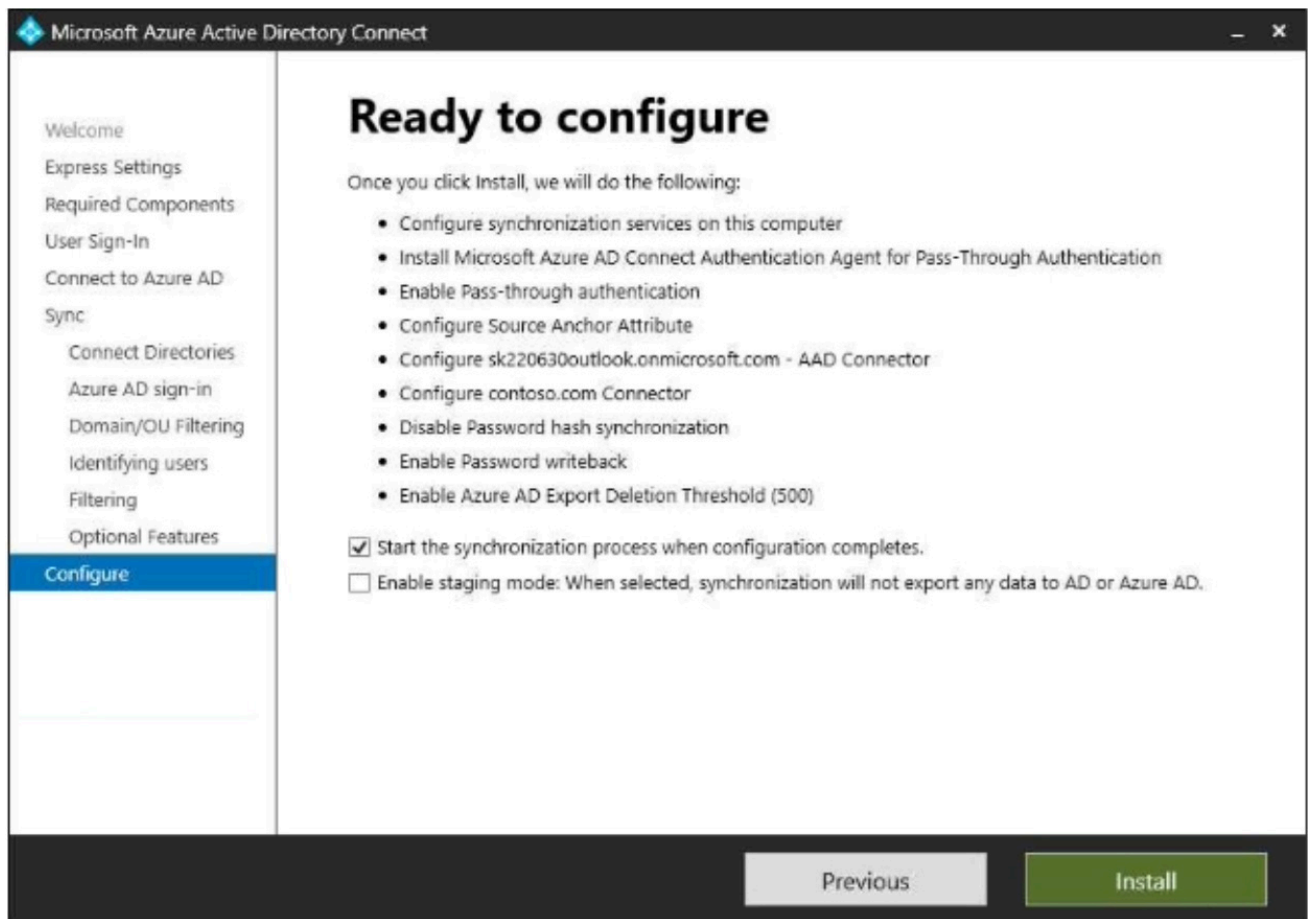
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD and contains the users shown in the following table.

| Name  | Organizational unit (OU) |
|-------|--------------------------|
| User1 | OU1                      |
| User2 | OU2                      |

In Azure AD Connect, Domain/OU Filtering is configured as shown in the following exhibit.



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



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

NOTE: Each correct selection is worth one point.

### Answer Area

| Statements                                                                                                 | Yes                   | No                    |
|------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| User1 can use self-service password reset (SSPR) to reset his password.                                    | <input type="radio"/> | <input type="radio"/> |
| If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller. | <input type="radio"/> | <input type="radio"/> |
| User2 can be added to a Microsoft SharePoint Online site as a member.                                      | <input type="radio"/> | <input type="radio"/> |

Suggested Answer:

Answer Area

| Statements                                                                                                 | Yes                              | No                    |
|------------------------------------------------------------------------------------------------------------|----------------------------------|-----------------------|
| User1 can use self-service password reset (SSPR) to reset his password.                                    | <input checked="" type="radio"/> | <input type="radio"/> |
| If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller. | <input checked="" type="radio"/> | <input type="radio"/> |
| User2 can be added to a Microsoft SharePoint Online site as a member.                                      | <input checked="" type="radio"/> | <input type="radio"/> |

**niesz1** Highly Voted 1 year, 8 months ago

YES

YES

NO- User 2 is not synced to 365

upvoted 37 times

**Das\_Duck** 8 months, 2 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 4 times

  **AcTiVeGrEnAdE** 2 months ago

By default, SSPR is disabled for all users AND it must be configured in Entra Id and the Entra Connect Sync engine with password writeback for it to work properly.

upvoted 1 times

  **Another\_one**  1 year, 8 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 16 times

  **OrangeSG** 1 year, 7 months ago


Password write-backup are enabled in the last screenshoot.

upvoted 6 times

  **omnomsnom** 1 year 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

  **test123123** 5 months, 3 weeks ago

By default Self service password reset enabled is set to "None" for normal users in Entra ID - Password reset Blade. It is always enabled for admins. Ive checked on 3 different new tenants.

So the answer should be:

NO (Assume default value NONE)

YES (Because auth is PTA)

NO (User 2 not in the standard Users OU so is not synched from onprem AD to cloud)

upvoted 1 times

  **Giuseppe\_Geraci**  1 month, 2 weeks ago

No - Yes - No. SSPR is enabled by default but must be configured before use it.

upvoted 1 times

  **AcTiVeGrEnAdE** 2 months ago



NO

YES

NO

based on screenshots, SSPR is not configured anywhere. SSPR must be configured in Entra ID and the sync engine. Also, there is not "update password in cloud only" for directory synced users....

upvoted 2 times

  **noa808a** 3 months, 2 weeks ago

For those lost in the comments like I am:

YES YES YES: Currently at 1 vote

YES YES NO: Currently at 5 votes

NO YES NO: Currently at 4 votes

upvoted 1 times

  **YesPlease** 4 months, 1 week ago

YES - They can use SSPR, but it will only update the cloud password and not the on-premises password. This is because HASH is turned OFF

YES - Passthrough authentication is turned ON

NO - User2 is not synced

upvoted 1 times

  **Frank9020** 5 months ago

1 - User1: No. Reason: Azure AD Connect is configured to disable password hash synchronization, and User1 is from OU1, which is synchronized.

However, for self-service password reset (SSPR) to work, either password hash synchronization or pass-through authentication with SSPR enabled is

required. Since password hash synchronization is disabled, User1 cannot use SSPR.

2 - User1: Yes. Reason: Azure AD Connect is configured with Pass-through authentication (PTA) and password hash synchronization is disabled. With PTA enabled, authentication requests for User1 will be forwarded to the on-premises Active Directory Domain Controller for verification.

3 - User2: No. Reason: In the Domain/OU Filtering settings, OU2 is not selected for synchronization, meaning User2 is not being synchronized to Azure AD. Since User2 does not exist in Azure AD, he cannot be added as a member to a SharePoint Online site.

upvoted 1 times

  **Sunth65** 5 months ago

NB! But pass-through authentication and Password writeback are enabled in this case !

upvoted 1 times

  **Frank9020** 4 months, 4 weeks ago

Yes, you are right about that, but SSPR must be explicitly enabled in Azure AD for users to reset passwords, and if you read the question on top, this is a sync config in Azure AD.

Password Writeback only allows changes to be written back to on-prem AD, but it does not enable the self-service reset functionality by itself.

Without SSPR enabled, users would have no way to initiate a password reset via Azure AD. SSPR (Self-Service Password Reset) is a separate feature that must be enabled in Azure AD for users to reset their passwords if they forget them.

upvoted 1 times



  **Siraf** 1 year, 6 months 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

  **Fijii** 4 months ago

What you see "Users" is the default users OU, it does not mean "all the users" I think it's meant to trick people. User2 is in the OU2, not in the Users OU. Since OU2 is not synced, User2 will not be synced.

upvoted 1 times

  **penatuna** 1 year, 5 months 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, 7 months 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, 7 months ago

NO : password hash synchronization is disabled

YES : PTA is enabled

NO : No Sync to AAD

upvoted 2 times

  **mohamedbenamor** 11 months, 1 week ago

Password Write back requires PTA

upvoted 1 times

  **Nivos23** 1 year, 7 months ago

In my opinion it is

yes

yes

no

upvoted 4 times



You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the 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 1 year, 1 month 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 9 times

 **ralphw** Highly Voted 1 year, 1 month ago

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

upvoted 8 times

 **Waris\_khan8623** Most Recent 9 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** 9 months, 2 weeks ago

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

upvoted 1 times

 **Ed2learn** 1 year, 2 months ago

the other right answer.

upvoted 2 times

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

| Name   | Role                      |
|--------|---------------------------|
| Admin1 | User Administrator        |
| Admin2 | Password Administrator    |
| Admin3 | Application Administrator |

You need to compare the role permissions of each user. The solution must minimize administrative effort.

What should you use?

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

**Suggested Answer:** C

Community vote distribution

B (78%)

C (22%)

 **Julesy** Highly Voted 1 year, 9 months ago

**Selected Answer: B**

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

upvoted 14 times

 **Alscoran** 1 year, 7 months 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 5 times

 **Giuseppe\_Geraci** 1 month, 2 weeks ago


app admin is listed

upvoted 1 times

 **strongline** 1 year ago


app admin is listed

upvoted 1 times

 **Er\_01** 1 year, 5 months ago

Your link compares the role not the user.

upvoted 1 times

 **vladi72** Highly Voted 12 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 6 times

 **AlexBrazil** 7 months, 4 weeks ago

It does have. I've checked.

upvoted 2 times

 **AcTiVeGrEnAdE** Most Recent 2 months ago

**Selected Answer: B**

I am really surprised that the Entra Id Admin Center would not have this capability but the answer is surprisingly the M365 Admin Portal.

upvoted 2 times

🗨️ 👤 **PD1** 5 months, 1 week ago

**Selected Answer: C**

To compare the role permissions of each user in your Azure AD tenant with minimal administrative effort, you should use the Microsoft Entra admin center (Option C).

The Microsoft Entra admin center is specifically designed to manage and monitor your Microsoft Entra ID (formerly known as Azure Active Directory). It allows you to view and manage user roles and permissions efficiently.

upvoted 2 times

🗨️ 👤 **Oskarma** 5 months, 2 weeks ago

**Selected Answer: B**

Just tested in my tenant. You can choose the THREE roles to compare them. :-)

upvoted 2 times

🗨️ 👤 **Grg433** 5 months, 3 weeks ago

**Selected Answer: C**

Option B: the Microsoft 365 admin center is primarily used for managing Microsoft 365 services, such as users, groups, licenses, and basic security settings. However, it does not provide detailed insights into Azure AD role permissions or allow for a direct comparison of role permissions assigned to users.

To specifically compare and manage Azure AD roles and permissions, Microsoft Entra admin center (Option C) is the correct tool, as it focuses on identity and access management within Azure AD.

Therefore, while Option B allows for some user and role management, it does not meet the requirement to compare detailed role permissions in Azure AD. Option C is more suitable for this task.

upvoted 2 times

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

🗨️ 👤 **jtlucas99** 1 year, 1 month 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** 1 year, 1 month ago

Microsoft 365 admin center

upvoted 1 times

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

**Selected Answer: B**

B is correct answer!  
upvoted 1 times

🗳️ 👤 **Er\_01** 1 year, 4 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** 1 year, 5 months 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** 1 year, 4 months ago

I also tested it, it is correct  
upvoted 1 times

🗳️ 👤 **Er\_01** 1 year, 5 months 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** 1 year, 5 months 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, 5 months 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 Administrator:

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, 7 months ago

**Selected Answer: C**

Application Administrator not visible on M365 site  
upvoted 1 times

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

<https://admin.microsoft.com/#/rbac/directory>  
upvoted 1 times

🗳️ 👤 **Blagojche** 1 year, 7 months ago

Application Administrator is present in M365 Admin Center, check!  
upvoted 2 times

🗳️ 👤 **Alscoran** 1 year, 7 months 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

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, 7 months 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** 6 months, 3 weeks ago

The Update-MgPolicyPermissionGrantPolicyExclude cmdlet is related to permission grant policies and doesn't apply to self-service sign-up restrictions.

upvoted 7 times

 **Labelfree** Highly Voted 6 months, 3 weeks ago

**Selected Answer: A**

Correct answer is A. B isn't even a valid command.

upvoted 7 times

 **d1e85d9** Most Recent 2 months, 3 weeks ago

**Selected Answer: A**

Answer: A

upvoted 1 times

 **rvln7** 4 months, 1 week ago

**Selected Answer: A**


A. The Update-MgOrganization cmdlet is used to configure organization-wide settings in Microsoft Entra ID (Azure AD), including disabling self-service sign-ups for users.

B. Update-MgPolicyPermissionGrantPolicyExclude – This cmdlet is used for managing permission grant policies, not self-service sign-up settings.

C. Update-MgDomain – This is used to update domain properties but does not control user self-service sign-up.

D. Update-MgDomainFederationConfiguration – This is used for managing domain federation settings, which is unrelated to blocking self-service sign-ups.

upvoted 2 times

 **YesPlease** 4 months, 1 week ago

**Selected Answer: A**

Answer) A Update-MyOrganization

To turn off Self-Service Password Reset (SSPR) using the "Update-MgOrganization" cmdlet in PowerShell, you would need to set the "allowedToUseSSPR" parameter to "false" within the policy object  
upvoted 2 times

🗨️ 👤 **Frank9020** 5 months, 2 weeks ago

**Selected Answer: A**

A: The PowerShell cmdlet Update-MgOrganization is used to configure settings for the organization, including self-service sign-up options.

B. Update-MgPolicyPermissionGrantPolicyExclude: This cmdlet is used to modify permission grant policies for apps, not for disabling self-service sign-up.  
upvoted 4 times

🗨️ 👤 **PD1** 5 months, 3 weeks ago

**Selected Answer: A**

You are correct! The Update-MgOrganization cmdlet with the AllowEmailVerifiedUsers parameter can also be used to prevent users from creating accounts using self-service sign-up.  
upvoted 2 times

🗨️ 👤 **Mole857** 7 months ago

**Selected Answer: A**

Isn't the correct answer A?

Update-MgOrganization AllowEmailVerifiedUsers \$false would block self-service sign-up to the tenancy?  
upvoted 5 times

🗨️ 👤 **Tony416** 10 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** 6 months, 3 weeks ago

According to these links Update-MgPolicyAuthorizationPolicy which is not an option here. A is correct.

upvoted 2 times

🗨️ 👤 **d3ebc45** 1 year 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 3 times

🗨️ 👤 **Panama469** 11 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** 1 year, 1 month 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 don't 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** 1 year, 2 months ago

la opción A, es la correcta.

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

upvoted 2 times

  **belyo** 1 year, 3 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%2D>

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, 6 months 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, 6 months ago

**Selected Answer: B**

I stand for B

upvoted 1 times

  **Ed2learn** 1 year, 8 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

HOTSPOT

-

You have an Azure AD tenant.

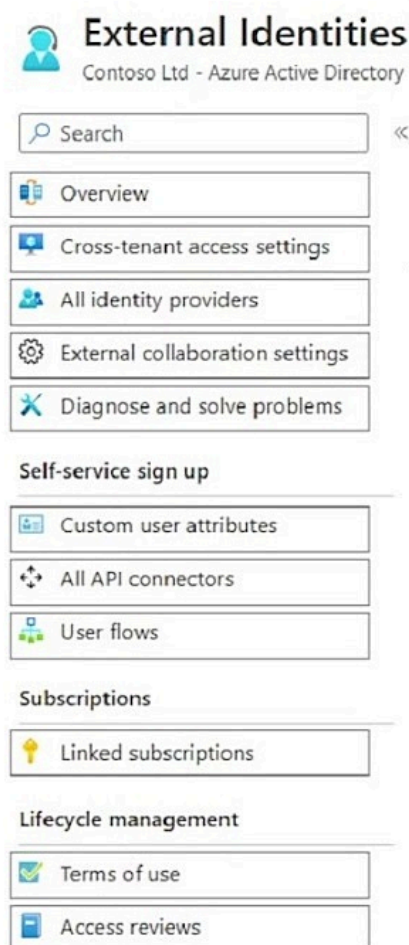
You need to configure the following External Identities features:

- 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



The screenshot shows the 'External Identities' management interface for 'Contoso Ltd - Azure Active Directory'. It includes a search bar, a left-hand navigation menu with options like Overview, Cross-tenant access settings, All identity providers, External collaboration settings, and Diagnose and solve problems. Below this, there are sections for 'Self-service sign up' (Custom user attributes, All API connectors, User flows), 'Subscriptions' (Linked subscriptions), and 'Lifecycle management' (Terms of use, Access reviews).

**External Identities**  
Contoso Ltd - Azure Active Directory

Search

Overview

Cross-tenant access settings

All identity providers

External collaboration settings

Diagnose and solve problems

**Self-service sign up**

Custom user attributes

All API connectors

User flows

**Subscriptions**

Linked subscriptions

**Lifecycle management**

Terms of use

Access reviews



## Answer Area



### External Identities

Contoso Ltd - Azure Active Directory

 <<

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

Suggested Answer:

**Nivos23** Highly Voted 1 year, 7 months ago

I think the answer is correct

External Collaboration settings

And

Linked Subscriptions

upvoted 11 times

**test123123** 5 months, 3 weeks ago

Agreed. Cross-tenant access is more about automation of continuously synching (Pvision and deprovision) multiple users and their metadata from TenantA to TenantB.

upvoted 2 times

**AcTiVeGrEnAdE** Most Recent 2 months ago

My thoughts:

Cross tenant-access settings

Linked Subscriptions

upvoted 2 times

**noa808a** 3 months, 2 weeks ago

Correct.

upvoted 1 times

**YesPlease** 4 months, 1 week ago

Cross-Tenant Access Settings

and

Linked Subscriptions

<https://learn.microsoft.com/en-us/entra/external-id/cross-tenant-access-settings-b2b-collaboration>

<https://learn.microsoft.com/en-us/entra/external-id/external-identities-pricing>

upvoted 1 times

🗨️ 👤 **Nail** 7 months, 3 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 2 times

🗨️ 👤 **AlexBrazil** 7 months, 4 weeks 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 2 times

🗨️ 👤 **Justin0020** 1 year, 2 months ago

My answer is:

Cross tenant-access settings

Linked Subscriptions

upvoted 3 times

🗨️ 👤 **penatuna** 1 year, 7 months 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, 7 months 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, 7 months 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



You have an Azure AD tenant that contains the external user shown in the following exhibit.

The screenshot displays the 'Overview' tab for an external user in the Microsoft Entra admin center. The user's profile includes a purple circular icon with 'EU' and the text 'External User'. Below this, the email address is listed as 'external195\_gmail.com#EXT#@sk230415outlook.onmicrosoft.com' with a 'Guest' role. A table of properties shows details like the user principal name, object ID, creation date (Apr 30, 2023), and user type (Guest). To the right, summary statistics show 0 group memberships, 0 applications, 0 assigned roles, and 0 assigned licenses. At the bottom, a 'My Feed' section contains three cards: 'Account status' (Enabled), 'Sign-ins' (Last sign-in: -- --), and 'B2B collaboration' (Invitation state: Accepted). Each card has an 'Edit' or 'See all' link.

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 7 months, 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 14 times

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

Cool,

I didnt know this one, I would have recreated the guest user  
upvoted 6 times

  **kijken** 7 months, 2 weeks ago

answer is D btw

upvoted 4 times

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, 7 months 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 11 times

 **test123123** Most Recent 5 months, 3 weeks ago

**Selected Answer: A**

External Collaboration settings you find:

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)

upvoted 2 times

 **Labelfree** 6 months, 3 weeks ago

**Selected Answer: A**

Untested atm but sounds right.

upvoted 1 times

 **Jackdisuin** 1 year, 4 months ago

Correct. External collaboration settings > collaboration restrictions

upvoted 3 times

You have an Azure AD tenant that contains a user named User1 and a Microsoft 365 group named Group1. User1 is the owner of Group1.

You need to ensure that User1 is notified every three months to validate the guest membership of Group1.


What should you do?

- A. Configure the External collaboration settings.
- B. Create an access review.
- C. Configure an access package.
- D. Create a group expiration policy.

**Suggested Answer: D**

Community vote distribution

B (100%)

 **haazybanj** Highly Voted 1 year, 7 months 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 12 times

 **hml\_2024** Most Recent 10 months 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

 **loukyexamtopic** 11 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** 11 months 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, 7 months ago

**Selected Answer: B**

Access review

upvoted 1 times


 **penatuna** 1 year, 7 months 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, 7 months 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, 7 months ago

**Selected Answer: B**

Validatating a membership is access review, in my opinion.

upvoted 3 times



## 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.)

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](#) →

[Add filters](#)

2 users found

|                          | Name  | User principal name               | User type | Directory synced |
|--------------------------|-------|-----------------------------------|-----------|------------------|
| <input type="checkbox"/> | User1 | User1@m365x629615.onmicrosoft.com | Member    | No               |
| <input type="checkbox"/> | 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?](#)

[Add filters](#)

|                          | Name   | Group Type | Membership Type |
|--------------------------|--------|------------|-----------------|
| <input type="checkbox"/> | Group1 | Security   | Assigned        |
| <input type="checkbox"/> | 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 >



## User Administrator | Assignments

Privileged Identity Management | Azure AD roles

» [+ Add assignments](#) [Settings](#) [Refresh](#) [Export](#) [Got feedback?](#)

[Eligible assignments](#) [Active assignments](#) [Expired assignments](#)

| 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.)



## Group2 | Members

Group



+ Add members

Remove

Refresh

Bulk operations ▾

Columns

Preview features

Got feedback?

✓ This page includes previews available for your evaluation. [View previews →](#)

## Direct members

|                          | Name                                                                                    | User type |
|--------------------------|-----------------------------------------------------------------------------------------|-----------|
| <input type="checkbox"/> |  User3 | Member    |
| <input type="checkbox"/> |  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. | <input type="radio"/> | <input type="radio"/> |
| Admin1 can add User1 to Group3.                    | <input type="radio"/> | <input type="radio"/> |
| Admin3 can reset the password of User1.            | <input type="radio"/> | <input type="radio"/> |

## Answer Area


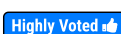
Suggested Answer:

| Statements                                         | Yes                              | No                               |
|----------------------------------------------------|----------------------------------|----------------------------------|
| Admin1 can reset the passwords of User3 and User4. | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin1 can add User1 to Group3.                    | <input type="radio"/>            | <input checked="" type="radio"/> |
| Admin3 can reset the password of User1.            | <input checked="" type="radio"/> | <input type="radio"/>            |

 **SFAY**  1 year, 5 months ago

No, No, Yes

upvoted 36 times

 **Bosswarf**  1 year, 4 months 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 23 times

 **Ody** 1 year, 4 months ago

Link.



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

upvoted 2 times

  **STPC** Most Recent 6 days, 1 hour ago

No No Yes

upvoted 1 times



  **d1e85d9** 2 months, 3 weeks ago

NO

NO

YES

upvoted 1 times

  **Frank9020** 5 months, 2 weeks ago

No, No, Yes

Administrative units in Azure AD do not extend permissions to indirect members of groups. For the User Administrator to reset User3's password, User3 must be directly added to AU1.

upvoted 2 times

  **anonymousarpanch** 5 months, 2 weeks ago

No, No, Yes..Administrative groups cannot be nested. Refer the table for permissions. It says that a user administrator scoped to an admin unit that contains a group cannot 'reset the passwords of individual members of the group'

upvoted 1 times

  **[Removed]** 1 year, 4 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** 1 year, 3 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** 1 year, 5 months 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 10 times

  **loukyexamtopic** 11 months, 1 week ago

incorrect, they are actually part of department1 admin unit, check pictures again

upvoted 1 times

## HOTSPOT

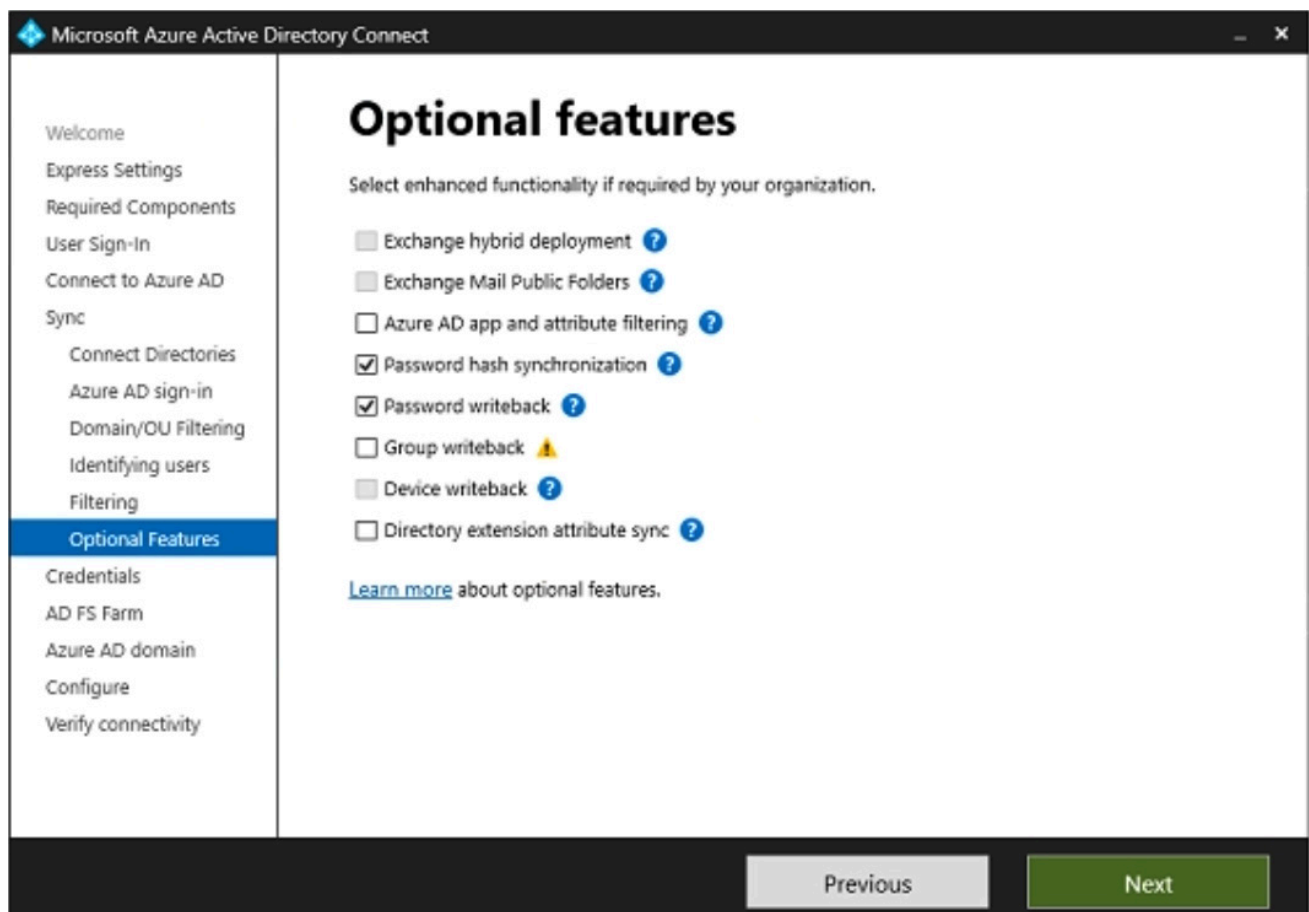
-

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.



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.        | <input type="radio"/> | <input type="radio"/> |
| User2 can sign in to Server1.       | <input type="radio"/> | <input type="radio"/> |
| User3 can sign in to Microsoft 365. | <input type="radio"/> | <input type="radio"/> |

#### Answer Area

| Statements                          | Yes                              | No                               |
|-------------------------------------|----------------------------------|----------------------------------|
| You can add User1 to Group1.        | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 can sign in to Server1.       | <input type="radio"/>            | <input checked="" type="radio"/> |
| User3 can sign in to Microsoft 365. | <input checked="" type="radio"/> | <input type="radio"/>            |

Suggested Answer:

 **MatExam** Highly Voted 1 year, 5 months 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 23 times

 **test123123** 5 months, 3 weeks ago

Agreed.

upvoted 1 times

 **naveenbio** 6 months, 4 weeks ago

It is correct (YES, YES & NO)

upvoted 1 times

 **krisbla** 7 months, 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

 **ultravincen** 1 year, 3 months 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 1 year, 1 month 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 7 times

 **AcTiVeGrEnAdE** Most Recent 2 months ago

Yes

Yes

No

The provided answers are incorrect

upvoted 1 times

🗨️ 👤 **d1e85d9** 3 months, 3 weeks ago

1. Yes: Federation is ON so, 6 character password doesn't impact to sync to Azure

2. Yes: User2 is still enabled in on-prem AD. There is no writeback for user.

So user in Azure AD will NOT sync to On-Prem AD

3. No: Same as User2, enable user3 will not write back to on-prem AD.

upvoted 1 times

🗨️ 👤 **d1e85d9** 2 months, 3 weeks ago

Actually the given answers are correct.

1. NO - 6 character cannot sync even Fed is enable.

2. NO - user2 has been disabled in the last paragraph of question. Writeback in enable.... so user2 has been disabled.

3. YES - user3 has been enabled in the last paragraph of the question so can.

upvoted 2 times

🗨️ 👤 **psp65** 3 months, 3 weeks ago

NYN

if you disable or enable a synched user from online, the user state will be reset by entra connect according the user's state onprem. Furthermore a user won't be synched if his password is less than 8 char

upvoted 1 times

🗨️ 👤 **bardock100** 4 months, 1 week ago

1. No - Because user1 is not synchronised to Entra because has 6-character password. You need 8-character password to make sync user from AD to Entra.

2. Yes - User2 exist in AD and can login to Server1 which is in local AD. Disabling an account in Entra does not disable it in AD, it only works one way from AD to Entra. Only passwords work both ways if password writeback is enabled.

3. Yes - User3 is in Entra and is now Enabled after following steps: Enable User3

upvoted 3 times

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

No: because you are doing a federated connection to o365, the user needs a minimum password of 8 characters to be allowed on o365

No: federation means a sync between both systems, so disabling on o365 side will disable them on local system too

Yes: the user meets minimum password requirements for o365 and was enabled.

upvoted 2 times

🗨️ 👤 **Frank9020** 5 months ago

Correct answer is:

You can add User1 to Group1. ✓ Yes

User2 can sign in to Server1. ✓ Yes (because Server1 is on-prem)

User3 can sign in to Microsoft 365. ✓ Yes, User3 can sign in to Microsoft 365 because it is cloud based, and since PHS is enabled, User3 can authenticate directly against Microsoft Entra ID without needing on-premises AD authentication.

upvoted 2 times

🗨️ 👤 **rtsh06** 7 months, 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 able to sign in to Microsoft 365.

upvoted 2 times

🗨️ 👤 **HartMS** 1 year, 2 months 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 2 times

  **armid** 4 months, 3 weeks ago

this! Federating means all authentication happens on premise. The password hash sync only ensures users can sign in to M36 in case your on prem FS servers fail.

So can you add user1 to group1 in the cloud space? YES, it just wont be available on premise

Can User 2 sign in to server 1? YES. Remember all auth is on premise. We disabled this user in the cloud which has no effect for on prem environment

Can user 3 login to M365? YES, we enabled it on prem and all authentication is on prem with federated services.

upvoted 1 times

  **armid** 4 months, 1 week ago


apologies obviously i got confused about where we enabled the user3 in the Q.. we enable it in Entra! so NO for #3.

YES - i think user 1 syncs even though the PW doesnt meet complexity for Entra, however we sync only the hash; so i dont think Entra "knows" what the clear text password is

YES - disabled in cloud will not diable it on prem, actually it will get enabled in cloud again during next sync, anyway no reason why he couldnt sign into on prem server

NO - same as above but the other way around. The account will get re-disabled on next sync

upvoted 1 times

  **emartiy** 1 year, 3 months 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 sufficient to entra id SSPR etc.


YES - NO - YES would be my selections for this question.

upvoted 4 times

  **einkaufacs** 1 year, 4 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** 1 year, 4 months 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 synced user.

upvoted 2 times

  **Ody** 1 year, 4 months 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]** 1 year, 5 months ago

Why would the first one be no?

upvoted 1 times

  **Ody** 1 year, 4 months ago

I was thinking it was due to the 8 character minimum in Entra ID

upvoted 2 times

  **Ody** 1 year, 4 months 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** 7 months, 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

🗨️ 👤 **armid** 4 months, 1 week ago

but you only sync the hash? so technically Entra doesnt know what the password is.

upvoted 1 times

🗨️ 👤 **Tim1119** 1 year, 5 months 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



## 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

« Save Discard Got feedback?

**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

**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

**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.                                                              | <input type="radio"/> | <input type="radio"/> |
| Admin1 can set Devices to be Microsoft Entra joined or Microsoft Entra registered require Multi-Factor Authentication to <b>Yes</b> . | <input type="radio"/> | <input type="radio"/> |
| Admin2 is a local administrator on Device3.                                                                                           | <input type="radio"/> | <input type="radio"/> |

### Answer Area

Suggested Answer:

| Statements                                                                                                                            | Yes                   | No                               |
|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------|----------------------------------|
| User1 can join four additional Windows 10 devices to Microsoft Entra ID.                                                              | <input type="radio"/> | <input checked="" type="radio"/> |
| Admin1 can set Devices to be Microsoft Entra joined or Microsoft Entra registered require Multi-Factor Authentication to <b>Yes</b> . | <input type="radio"/> | <input checked="" type="radio"/> |
| Admin2 is a local administrator on Device3.                                                                                           | <input type="radio"/> | <input checked="" type="radio"/> |

 **Anusha\_2000** Highly Voted 1 year, 5 months ago

No

Yes

No

upvoted 28 times

 **penatuna** Highly Voted 1 year, 4 months 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 15 times

 **penatuna** 1 year, 4 months 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 16 times

 **penatuna** 1 year, 4 months 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 9 times



  **AcTiVeGrEnAdE** Most Recent 2 months ago

NO

NO

NO

upvoted 2 times


  **d1e85d9** 3 months, 3 weeks ago

1. No - max 5 device.

2. No - Cloud Device Administrator role cannot change MFA settings for Azure Entra devices.

3. No - this is only registered.

upvoted 2 times

  **YesPlease** 4 months, 1 week ago

1) No: MS Entra limits reflect both Registered and JOINED

<https://learn.microsoft.com/en-us/mem/intune/enrollment/device-limit-intune-azure#microsoft-entra-device-limit>



2) No: Cloud Device Administrator can only ENABLE, DISABLE, and DELETE devices and are not able to change any other properties.

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

3) No: Although ADMIN2 has the right role as "Microsoft Entra Joined Device Local Administrator", the device is only REGISTERED and not JOINED so permissions are not valid locally.

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

upvoted 2 times

  **rtsh06** 7 months, 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** 7 months, 2 weeks ago

No

No



No

upvoted 1 times

  **BRZSZCL** 8 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, because there was only 1 Entra Joined device, but in discussion panel I have realised it is different.

upvoted 1 times

  **hml\_2024** 10 months ago

Check Question 21

Yes

No

No

upvoted 3 times

  **thetootall** 11 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** 11 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** 1 year, 1 month 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** 1 year, 3 months 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 Admins 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

  **Futfuyfyfj** 1 year, 2 months ago


The device maximum has nothing to do with the join type, it's an overall limit regardless join or register so the first one is a NO.

upvoted 5 times

  **Alcpt** 1 year, 1 month ago

correct. the answer is NO NO NO

upvoted 1 times


  **ELQUMS** 1 year, 5 months ago

No

Yes

No

upvoted 4 times

  **dbz\_34** 1 year, 5 months ago

no

yes

no

upvoted 4 times

You have an Azure subscription named Sub1 that contains a user named User1.

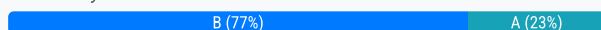
You need to ensure that User1 can purchase a Microsoft Entra Permissions Management license for Sub1. The solution must follow the principle of least privilege.

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



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

**Selected Answer: B**

Correct

upvoted 11 times

**Alcpt** 1 year, 2 months 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** 1 year 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 5 times

**Alcpt** 1 year, 1 month ago

im guessing here. yes its B.

pity there is no delete button

upvoted 2 times

**csi\_2025** Most Recent 4 months ago

**Selected Answer: B**

What is sub1? A user? A submarine? A substitute?

upvoted 2 times

**YesPlease** 4 months, 1 week ago

**Selected Answer: B**

Answer B) Billing Administrator

Billing Administrator can: Makes purchases, manages subscriptions, manages support tickets, and monitors service health.

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

upvoted 1 times

**PD1** 5 months, 1 week ago

**Selected Answer: B**

B. Billing Administrator

upvoted 1 times

🗨️ **mohamedbenamor** 7 months, 1 week ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/entra/permissions-management/product-roles-permissions#enabling-permissions-management>  
upvoted 3 times

🗨️ **seleneliane** 9 months, 2 weeks ago

It's A that i will choose!  
upvoted 1 times

🗨️ **jim85** 1 year ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/entra/permissions-management/product-roles-permissions> - Billing Admin  
upvoted 2 times

🗨️ **BM03** 1 year, 2 months 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** 1 year, 2 months ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/entra/permissions-management/onboard-enable-tenant>  
upvoted 1 times

🗨️ **Alcpt** 1 year, 2 months 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** 1 year, 3 months ago

**Selected Answer: B**

Correct  
upvoted 1 times

🗨️ **Menard001** 1 year, 3 months 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** 1 year, 4 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** 1 year, 3 months 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

🗨️ 👤 **Milla** 1 year, 3 months ago

Correct answer

upvoted 1 times

🗨️ 👤 **penatuna** 1 year, 4 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** 9 months, 2 weeks ago

This is in yesterday exam. I choose "C".

upvoted 1 times

🗨️ 👤 **penatuna** 1 year, 1 month 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** 1 year, 5 months ago

Billing administrator

upvoted 3 times

🗨️ 👤 **throwaway10188** 1 year, 5 months 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

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:

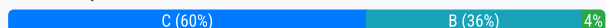
- View all resources.
- Restart virtual machines.
- Create virtual machines in RG1 only.
- Create storage accounts in RG1 only.

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



**penatuna** 1 year, 3 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 9 times

**[Removed]** 1 year, 1 month 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 6 times

**Chibibo** 4 days, 22 hours ago

**Selected Answer: B**



Create two custom roles:

- Role 1 can view any resource type and restart virtual machines;
- Role 2 can create virtual machines and storage accounts.

Assign Role 1 to User1 at the subscription.

Assign Role 2 to User1 at RG1.

Keep in mind that they ask for the MINIMUM number of assignments, and they don't say that you can only use standard role definitions.

upvoted 1 times

  **Giuseppe\_Geraci** 1 month, 2 weeks ago

**Selected Answer: C**

Reader View all resources

Virtual Machine Contributor Restart VMs across all resource groups

Contributor Create VMs and storage accounts in RG1

upvoted 2 times

  **AcTiVeGrEnAdE** 2 months ago

**Selected Answer: B**

what a dumb question that I hope I don't see on the exam. The question does not state if they had to be built in or custom roles but the one common thing I think we can all agree on is least privileged.

One custom role at the subscription level to read all resources and restart virtual machines

A second custom role for RG1 for storage and compute

upvoted 1 times

  **nik\_si** 3 months ago

**Selected Answer: C**

Reader Role at the subscription level:

Allows User1 to view all resources.



Virtual Machine Contributor Role at the subscription level:

Allows User1 to restart virtual machines in any resource group.

Custom Role at the RG1 level:

Includes permissions to create virtual machines and storage accounts in RG1.

upvoted 1 times

  **ElWhitepages** 3 months, 2 weeks ago

**Selected Answer: C**

Reader at the subscription level

Lets User1 see all resources (every RG, every resource type).

Virtual Machine Operator at the subscription level

Lets User1 start, stop, and restart VMs anywhere in the subscription—but not create or delete them.

Contributor on RG1

Lets User1 create (and manage) any resource in RG1 (including VMs, storage accounts, etc.)

Does not give them creation rights in RG2 or other resource groups.

upvoted 1 times

  **bardock100** 4 months, 1 week ago

**Selected Answer: C**

To meet the requirements for User1, you will need to assign three RBAC roles:

Reader role at the subscription level to allow User1 to view all resources.

Virtual Machine Contributor role at the subscription level to allow User1 to restart virtual machines.

Contributor role at the RG1 level to allow User1 to create virtual machines and storage accounts in RG1 only.

Therefore, the minimum number of RBAC role assignments required is C. 3

upvoted 2 times

  **YesPlease** 4 months, 1 week ago

**Selected Answer: B**

Answer B) 2

You can create just one custom role to create VM, restart them and the create storage account....and apply it to only RG1. Assign READER role at top level to view all resources outside of RG1.

upvoted 1 times

🗨️ **csi\_2025** 4 months ago

And than you forget that the second requirement is to restart virtual machines regardless in which RG they are.

upvoted 1 times

🗨️ **\_marc** 4 months, 2 weeks ago

**Selected Answer: B**

Can be done with 2 custom role assignments. The question doesn't explicitly state that only in-built roles can be used.

upvoted 1 times

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

**Selected Answer: C**

This is a retarded question. It can be either 3 or 4

upvoted 2 times

🗨️ **khangkowng1** 6 months, 2 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 4 times

🗨️ **emartiy** 1 year, 3 months ago

**Selected Answer: B**

2 RBAC roles are sufficient to perform what in case.

upvoted 4 times

🗨️ **Alcpt** 1 year, 2 months ago

Nope.

#1 Global reader to read the entire sub,

#2 vm contributor

#3 vm contributor

#4 storage account contributor

upvoted 4 times

🗨️ **emartiy** 1 year, 3 months 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 resource

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 based Storage 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

🗨️ **mb0812** 1 year, 3 months 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 5 times

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

🗨️ 👤 **mb0812** 1 year, 3 months 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** 1 year, 4 months 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 4 times

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

It's 2 (B), by adding custom role/s.

upvoted 4 times

🗨️ 👤 **enklau** 8 months, 2 weeks ago

yes i think the same

upvoted 1 times

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 fabrikam.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**  9 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 7 times

 **penatuna** 9 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**  11 months 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 6 times

 **d1e85d9**  3 months, 2 weeks ago

**Selected Answer: D**

The correct answer is:

D. Collaboration restrictions

Explanation:

Since you are unable to invite guest users from adatum.com but can invite users from fabrikam.com, this indicates that there is a restriction on external collaboration for certain domains.

In Microsoft Entra ID (formerly Azure AD), Collaboration restrictions allow organizations to control which external domains can be invited as guest users. If adatum.com is blocked, you will see an error when attempting to invite users from that domain.

To resolve this issue:

Go to Microsoft Entra admin center.

Navigate to External Identities > External collaboration settings.

Under Collaboration restrictions, check if adatum.com is blocked and remove it from the restricted list.

Thus, the correct setting to configure is Collaboration restrictions.

upvoted 1 times

  **bardock100** 4 months, 1 week ago

**Selected Answer: C**

C)

External Identities | External collaboration settings | Collaboration restrictions

upvoted 1 times

  **SFAY** 11 months ago

**Selected Answer: D**

Correct

upvoted 4 times

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.

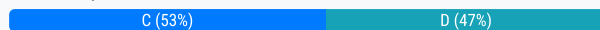
| Name     | Type                  | Location |
|----------|-----------------------|----------|
| VM1      | Virtual machine       | West US  |
| storage1 | Storage account       | East US  |
| WebApp1  | Azure App Service app | East US  |

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



**wheelcj** Highly Voted 1 year, 3 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 13 times

**AleFerrillo** 1 year, 1 month 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 6 times

**hml\_2024** 9 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 5 times

**Alcpt** 1 year, 1 month ago

D is correct, you can assign UAMI on all the resources under Identity.

upvoted 3 times

**NICKTON81** Highly Voted 1 year, 2 months 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** 11 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 10 times

**AcTiVeGrEnAdE** Most Recent 2 months ago

**Selected Answer: A**

A is the answer

-Storage accounts do not use managed identities directly. Managed identities will be used by -applications or services to access storage securely.

- Despite any managed identity residing in Entra Id and being globally available, user assigned managed identity can only be used in the region it was created in and can be shared amongst multiple resources. So VM1 cannot be used by the user created managed identity in East US.

-Azure app service in East can leverage the user-assigned managed identity.

upvoted 1 times

  **bardock100** 4 months ago

**Selected Answer: B**

Copilot:

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

Given that Managed1 is in the East US region, only resources in the same region can use it. Therefore, the correct answer is:

B. storage1 and WebApp1 only

If you have any more questions or need further clarification, feel free to ask!


upvoted 1 times

  **\_marc** 4 months, 2 weeks ago

**Selected Answer: C**

A storage account is not an actor, that is, it doesn't initiate any connection to another cloud service. Rather it is passive and allows access from other services. The storage account would have a RBAC role allowing other managed identities to access it, but there is no need for a storage account to have its own managed identity.


upvoted 2 times

  **Oskarma** 5 months, 1 week ago

**Selected Answer: D**

You can assign a user-assigned managed identity in a storage account and in different regions (tested in my tenant). So, D.

upvoted 1 times

  **test123123** 5 months, 3 weeks ago

**Selected Answer: D**

<https://learn.microsoft.com/en-us/azure/search/search-howto-managed-identities-storage#user-assigned-managed-identity>

upvoted 1 times

  **\_marc** 4 months, 2 weeks ago

Read it again: "You must have a user-assigned managed identity already configured and associated with your search service, and the identity must have a role-assignment on Azure Storage." Storage needs to add the managed identity into an RBAC role, it doesn't need the identity itself.

upvoted 1 times

  **c3e0fc1** 6 months, 3 weeks 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** 10 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** 10 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** 11 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** 1 year 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** 1 year, 1 month 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** 1 year, 2 months 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 4 times

  **NotanAdmin** 1 year, 1 month 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** 1 year, 2 months 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** 1 year, 2 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](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** 1 year, 3 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** 1 year, 3 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

## 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<br>smtp: sales@contoso.com                               |
| User2 | user2@contoso.com         | smtp: user2@contoso.com<br>smtp: user.2@contoso.com<br>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.

### 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** 8 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

  **palanka** 4 months, 4 weeks ago

But if user 3 has not synchronised, why will user 2 have an error?

upvoted 1 times

  **YesPlease**  4 months, 1 week ago

1) Successfully synced

Object already existed and the addition of another smtp email does not conflict with anything else.

2) AttributeValueMustBeUnique error occurs

If Microsoft Entra Connect attempts to add a new object or update an existing object with a value for the preceding attributes that's already assigned to another object in Microsoft Entra ID, the operation results in the AttributeValueMustBeUnique sync error.

3) invalidSoftMatch error occurs

An object was added in on-premises Active Directory with the same value for the proxyAddresses attribute as that of an existing object in Microsoft Entra ID. The object added on-premises isn't getting provisioned in Microsoft Entra ID.

upvoted 3 times

  **armid** 4 months, 3 weeks ago



how can it be? Dont the changes sync in order in which they happened? So if user3 fails to sync due to softmatch and THEN we modify user1 (removing his sales proxy) and THEN we modify user 2 adding the sales proxy, then user 1 and user 2 should sync successfully, because bob isn't getting synced?

upvoted 1 times

  **armid** 4 months, 3 weeks ago

i mean user3 isn't getting synced, gosh got lost in Microsoft Learn examples lol

upvoted 1 times

  **Nielll** 1 year, 3 months ago

this seems to be correct. the 1st table assumes that aliases are already being synced.

upvoted 1 times

  **Nielll** 1 year, 3 months ago



changed my mind

successfully synced

unique error

unique error

upvoted 2 times

  **Nielll** 1 year, 3 months ago

i changed my mind i again. i recreated this and verified that the given answers are correct

upvoted 6 times



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.

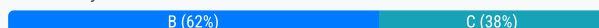
| Name  | Email                  | Description                                                   |
|-------|------------------------|---------------------------------------------------------------|
| User1 | User1@contoso.com      | An existing guest user in fabrikam.com                        |
| User2 | 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



🗳️ **SilverFox** Highly Voted 1 year, 2 months ago

**Selected Answer: B**



Repeat question.  
upvoted 7 times

🗳️ **criminal1979** Highly Voted 1 year, 2 months ago

**Selected Answer: C**

I say the answer is C in this case.

upvoted 7 times

  **Alcpt** 1 year, 2 months ago

U guys need to study the material. Stop guessing

upvoted 4 times

  **criminal1979** 11 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 2 times

  **Nail** 8 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 3 times

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

Selected Answer: B

Answer the question guys, don't start confusing yourselves with whether this is one time or every time code or if they receive it just once or every time, because THEY ARE NOT ASKING THAT. They are asking who will be sent a code at the time Bob invites them. NOT at the time the users try to access the resources. Email with OTP and invitation will be sent to B only.

But to cover all basis, if a week later User1 decides to go to that shared resource AND Contoso.com is not a Microsoft account, then they will be sent OTP to reauthenticate. But again, this is not what this question is asking!

upvoted 6 times

  **stefwandars** 3 months, 2 weeks ago

I hear what you are saying, but you are wrong. The situation is as follows: shares a Microsoft SharePoint Online document library. When a file is being shared, it will only send an email that the item has been shared, no mail with a passcode will be sent.

Only when the users open the link of the shared resource, they will be asked to sign-in and when no other authentication method is provided, they will get a OTP: thus answer: C

upvoted 1 times

  **armid** 4 months, 3 weeks ago

RATIONALE (I capitalized "or uses a link" for those who believe OTP is one time thing, which it isn't):

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.

At the time of invitation, there's no indication that the user you're inviting will use one-time passcode authentication. But when the guest user signs in, one-time passcode authentication will be the fallback method if no other authentication methods can be used.

upvoted 1 times

  **armid** 4 months, 2 weeks ago

actually thinking about it, answer is still B, but the reason is that the setting for OTP was disabled and now is enabled. So only the previously non-existing users will be affected.

upvoted 1 times

  **Frank9020** 5 months ago

Selected Answer: C

Correct answer is C. As long as we have not info about how User1 authenticates, C is the logical option in this case.

upvoted 1 times

  **Matt19** 6 months, 2 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** 7 months 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 2 times

🗨️ 👤 **HaubeRR89** 7 months 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** 9 months 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** 1 year ago

**Selected Answer: B**

The correct answer is B

upvoted 2 times

🗨️ 👤 **RucasII** 1 year, 1 month 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 2 times

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

**Selected Answer: B**

I think it's "B", since user 1 is already an existing member by other meaning already received the one-time passcode

upvoted 4 times

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

**Selected Answer: C**

passcode apply only to None Microsoft Entra or Microsoft account like (outlook or MSN)

upvoted 1 times

🗨️ 👤 **Alcpt** 1 year, 2 months ago

B. you will not send ONE TIME PASSCODES a second time! Ever! Unless the guest leaves.

upvoted 4 times

🗨️ 👤 **omnomsnom** 11 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

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 9 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 14 times

 **Alcpt** 8 months ago

Correct SAMI before UAMI

upvoted 3 times



You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the 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%)

 **ddz** Highly Voted 9 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 5 times

 **Trader6** Most Recent 8 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 3 times

 **klayytech** 8 months, 2 weeks ago

**Selected Answer: C**

C. the Set-MgUserLicense cmdlet

upvoted 3 times

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the 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%)

🗳️ 👤 **Sencha90** 1 month, 2 weeks ago

**Selected Answer: A**

How many times are they going to ask this.

upvoted 1 times

🗳️ 👤 **indope94** 1 month, 3 weeks ago

**Selected Answer: D**

D = juiste keuze bij "least administrative effort" + bulkbewerkingen.

upvoted 1 times

🗳️ 👤 **bardock100** 4 months, 1 week ago

**Selected Answer: A**

A is no longer good, All answers are wrong open Entra and check :)

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

upvoted 1 times

🗳️ 👤 **Trader6** 8 months, 2 weeks ago

**Selected Answer: A**

Only possible answer

upvoted 2 times

🗳️ 👤 **dzdz** 9 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 3 times

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.



From the Groups blade in the 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 Identity Governance blade in the Microsoft Entra admin center
- B. the Update-MgGroup cmdlet
- C. the Set-MgUserLicense cmdlet
- D. the Administrative units blade in the Microsoft Entra admin center

**Correct Answer:** C

  **Oskarma** 5 months, 1 week ago

**Selected Answer:** C

A lot of times repeated question.

upvoted 3 times

## SIMULATION

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 Password: =1122334455667788

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 99999999

-

You need to ensure the owner of each Microsoft 365 group is notified to renew their group every 180 days. Groups that are NOT renewed must be deleted. For groups without an owner, the notifications must be sent to Allan Deyoung.

To complete this task, sign in to the appropriate admin center.

**Correct Answer:**

**Microsoft 365 group expiration policy**

With the increase in usage of Microsoft 365 groups and Microsoft Teams, administrators and users need a way to clean up unused groups and teams. A Microsoft 365 groups expiration policy can help remove inactive groups from the system and make things cleaner.

**How to set the expiration policy**

As noted above, expiry is turned off by default. An administrator will have to enable the expiration policy and set the properties for it to take effect.

**Step 1:** To enable it, go to Microsoft Entra ID > Groups > Expiration. Here you can set the default group lifetime.

**Step 2:** Set Group lifetime (in days) to 180

Save Discard

Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to group expiration. Group owners must have Exchange licenses to receive notification emails. If a group is not renewed, it is deleted along with its associated content from sources such as Outlook, SharePoint, Teams, and PowerBI.

\* Group lifetime (in days) 180

\* Email contact for groups with no owners admin@contoso.com

Enable expiration for these Office 365 groups All Selected None

Select Office 365 groups >

BD Business Development ...

**Step 3:** Set Email contact for groups with no owners: Allan Deyoung

**Step 4:** Set Enable expiration for these Office 365 groups: All

**Step 5:** Click Save

**Reference:**

<https://learn.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-groups-expiration-policy>

**Oskarma** 5 months, 1 week ago

Entra ID | Groups | Expiration

- Group lifetime (in days): 180
  - Email contact for groups with no owners: correo@correo.com
  - Enable expiration for these Microsoft 365 groups: All
- upvoted 5 times

**Fijii** 4 months ago

The solution shown is clearly the correct one. But I found a similar way in Entra > Identity > Access reviews. You can create an access review for Team + Groups and configure pretty much the same things, I'm just not sure about membership, in the Identity Governance it seems to be focused on guest or you have to select manually each group.

Like I said, the correct solution it the one shown in Entra > Groups > Expiration, still wanted to propose an alternate way (would this give points in the actual exam ?)

upvoted 2 times

## SIMULATION

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 Password: =1122334455667788

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 99999999

-

You need to prevent all users from using passwords that are variations of the word Falcon.

To complete this task, sign in to the appropriate admin center.

**Correct Answer:**

Eliminate bad passwords using Microsoft Entra Password Protection

Step 1: Select Authentication methods

Step 2: Select Password Protection

Step 3: In Custom banned passwords, Set Enforce custom list: Yes

**Authentication methods | Password protection** ✨ ...

Contoso - Microsoft Entra ID Security

Search « Save Discard Got feedback?

**Manage**

- Policies
- Password protection**
- Registration campaign
- Authentication strengths
- Settings

**Monitoring**

- Activity
- User registration details
- Registration and reset events
- Bulk operation results

Custom smart logout

Lockout threshold ⓘ 10 ✓

Lockout duration in seconds ⓘ 60 ✓

**Custom banned passwords**

Enforce custom list ⓘ **Yes** No

Custom banned password list ⓘ

- contoso
- fabrikam
- tailwind
- michigan
- wolverine
- harbaugh
- howard

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ **No** Yes

Mode ⓘ **Enforced** Audit

Step 4: In Custom banned password list, add the word Falcon

Reference:

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad>

🗨️ 👤 **Oskarma** 5 months, 1 week ago

Entra ID | Authentication methods | Password protection

- Custom banned passwords
- Enforce custom list: Yes
- Custom banned password list: Falcon

upvoted 3 times

## SIMULATION

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 Password: =1122334455667788

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 99999999

-

You need to assign a Windows 10/11 Enterprise E3 license to the sg-Retail group.

To complete this task, sign in to the appropriate admin center.



**Correct Answer:**

**Step 3:** Select the name of the license plan [Select Windows 10/11 Enterprise E3 license] you want to assign to the group.

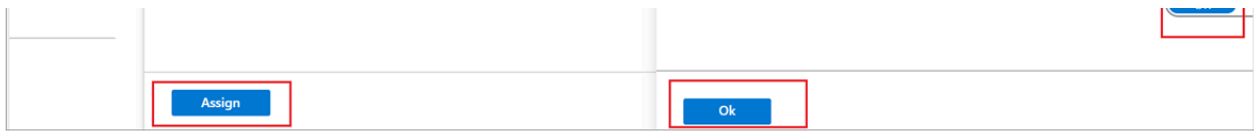
All products

 [New support request](#)

Step 6: Select Assignment options, make sure you have the appropriate license options turned on, and then select OK.

PowerApps for Dynamics 365

Off



The Assign license page updates to show that a user is selected and that the assignments are configured.

Step 7: Select Assign.

The group is added to the list of licensed groups and all of the members have access to the included Microsoft Entra services.

Reference:

<https://learn.microsoft.com/en-us/entra/fundamentals/license-users-groups>

 **Oskarma**  5 months, 1 week ago

Microsoft 365 | Billing | Licenses | Windows 10/11 Enterprise E3

- Groups tab
  - Assign licenses
  - Choose sg-Retail
  - Assign
- upvoted 5 times

 **bardock100**  3 months, 3 weeks ago

Today only in Microsoft 365 admin center you can assign licenses

upvoted 3 times

 **csi\_2025** 4 months ago

As Oskarma says. The old solution is not possible anymore, Microsoft blocked that you can add Licenses in Entra ID.

upvoted 4 times

## SIMULATION

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 Password: =1122334455667788

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 99999999

-

You need to create a group named Audit. The solution must ensure that the members of Audit can activate the Security Reader role.

To complete this task, sign in to the appropriate admin center.

Correct Answer:

Create a role-assignable group in Microsoft Entra ID

Step 1: Sign in to the Microsoft Entra admin center as at least a Privileged Role Administrator.

Step 2: Browse to Identity > Groups > All groups.

Step 3: Select New group.

Step 4: On the New Group page, provide group type, name [Enter Audit] and description.

Step 5: Set Microsoft Entra roles can be assigned to the group to Yes.

Home > Groups | All groups >

## New Group

Got feedback?

Group type \* ⓘ  
Security

Group name \* ⓘ  
Contoso\_Helpdesk\_Administrators

Group description ⓘ  
Helpdesk Administrator role assigned to group

Microsoft Entra roles can be assigned to the group ⓘ  
☒ Yes ☐ No

Membership type ⓘ  
Assigned

Owners  
No owners selected

Members  
No members selected

Roles  
No roles selected

Create


Step 6: Select the members and owners for the group. [Skip]

Step 7: Add role: Click No Roles select and select the Security Reader role.

Step 8: Select Create.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-create-eligible>

 Oskarma 5 months, 1 week ago

Entra ID (it's possible from Microsoft 365 admin center too) | Groups | All groups

- New group
  - Group name: Audit
  - Microsoft Entra roles can be assigned to the group: Yes
  - Create
- upvoted 3 times

  **armid** 4 months, 2 weeks ago

i'd say in addition to it you should aslo assign the eligibility to security reader role to the group in Identity Governance | PIM  
upvoted 6 times

  **Phil\_79** 2 weeks, 6 days ago

yep, the question is quite ambiguous... hope in the exam has been made more clear  
upvoted 2 times

## HOTSPOT

-

You have a Microsoft Entra tenant named contoso.com that contains an administrative unit named AU1 and two users named User1 and User2. User1 is a member of AU1.

You need to perform the following role assignments:

- User1: Security Administrator
- User2: User Administrator

For which scopes can each user be assigned the role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User1:

- AU1 only
- contoso.com only
- AU1 and contoso.com

User2:

- AU1 only
- contoso.com only
- AU1 and contoso.com

**Answer Area**

Correct Answer:

User1:

- AU1 only
- contoso.com only
- AU1 and contoso.com

User2:

- AU1 only
- contoso.com only
- AU1 and contoso.com

 **sn0rlaxxx** Highly Voted 5 months ago

User 1: Contoso Only

User 2: AU1 and Contoso.com

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/manage-roles-portal?form=MG0AV3&tabs=admin-center#:~:text=Roles%20that%20can%20be%20assigned%20with%20administrative%20unit%20scope>

upvoted 6 times

 **armid** 4 months, 2 weeks ago

thats right

1. Security Admin cannot be scoped to AUs
2. you dont need to be memeber of AU to be given administrative rights to it;

upvoted 5 times

 **siggijjions** Most Recent 3 weeks, 6 days ago

User 1:Contoso Only

User 2: I can't see where it is mentioned that he needs to be a user administrator for only the AU1, so giving him tenant wide user administrator

should include all users, as well as those inside the AU1?


Maybe i am not understanding this correctly

upvoted 1 times

  **siggijjions** 3 weeks, 6 days ago

Nevermind - read the question again and now see that it is asking where it CAN be assigned, not where it should be assigned

upvoted 1 times

  **noa808a** 3 months, 2 weeks ago

The correct answer:

User1: Only in the Tenant (Contoso.com)

User2: AU1 & Tenant.

upvoted 1 times



  **csi\_2025** 4 months ago

Just checked it myself.

User1: Only in the tenant; Security Admin is not a role available for administrative units

User2: Only in the tenant; Simply because he is not in the AU -> Can't get assigned the role in it (but is available in administrative units)

upvoted 1 times

  **noa808a** 3 months, 2 weeks ago

Incorrect. You do not need membership of the AU to be assigned a role.

From Microsoft documentation: "Administrators don't have to be members of the administrative unit they manage."

upvoted 2 times

  **YesPlease** 4 months, 1 week ago

User1: Can be Security Admin of the tenant, but not the AU since it does not have the Security Administrator role available for use with AU



<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/manage-roles-portal?form=MG0AV3&tabs=admin-center#roles-that-can-be-assig>

User2: Can be User Admin of the tenant, but not the AU since they are not a member of the AU.

[https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-restricted-](https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-restricted-management#:~:text=Even%20Global%20Administrators%20won%27t%20be%20allowed%20to%20modify%20the%20objects%20unless%20they%20assign%2)

[management#:~:text=Even%20Global%20Administrators%20won%27t%20be%20allowed%20to%20modify%20the%20objects%20unless%20they%20assign%2](https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-restricted-management#:~:text=Even%20Global%20Administrators%20won%27t%20be%20allowed%20to%20modify%20the%20objects%20unless%20they%20assign%2)

upvoted 1 times

  **noa808a** 3 months, 2 weeks ago

Incorrect. You do not need membership of the AU to be assigned a role.

From Microsoft documentation: "Administrators don't have to be members of the administrative unit they manage."



upvoted 1 times

  **Frank9020** 5 months ago

User1: Security Administrator- Can be assigned at AU1 level - Can be assigned at contoso.com (tenant-wide) = AU1 and contoso.com

User2: User Administrator- Can only be assigned at contoso.com (tenant-wide) (User is not a member of AU1) = contoso.com only

upvoted 3 times

  **noa808a** 3 months, 2 weeks ago

Incorrect. You do not need membership of the AU to be assigned a role.

From Microsoft documentation: "Administrators don't have to be members of the administrative unit they manage."

upvoted 1 times

  **Frank9020** 5 months ago

Since User2 is not a member of AU1, User2 cannot have an AU-scoped role.

upvoted 1 times

  **AcTiVeGrEnAdE** 2 months ago

Incorrect, You can assign roles scoped to AU's and the users do not need to be a user in the AU. When you create the role assignment you select an AU instead of the directory.

upvoted 1 times



You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the 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-MgUserLicense cmdlet
- B. the Identity Governance blade in the Microsoft Entra admin center
- C. the Groups blade in the Microsoft Entra admin center
- D. the Update-MgGroup cmdlet



**Correct Answer: A**

  **Maniact165** 1 month, 2 weeks ago

**Selected Answer: C**

isn't this C?

upvoted 1 times

  **Oskarma** 5 months, 1 week ago

**Selected Answer: A**

How many times is this question here? 😊

upvoted 3 times

  **Shingie** 4 months, 2 weeks ago

I am asking the same question too, this question has appeared 10 times so far I think

upvoted 2 times

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%)

 **test123123** 5 months, 3 weeks ago

**Selected Answer: B**

The best recommendation for your scenario is B. user-assigned managed identities and Azure Key Vault. Here's why:

**Securely Store Secrets:** Azure Key Vault is designed to securely store and manage secrets, keys, and certificates.

**Credentials Not in Code:** By using managed identities, you avoid hardcoding credentials in your application code. Managed identities allow your virtual machines to authenticate to Azure Key Vault without storing credentials in the code.

**Microsoft Entra Authentication:** Managed identities use Microsoft Entra ID (formerly Azure AD) for authentication, ensuring secure access to Azure resources.

**Minimize Administrative Effort:** User-assigned managed identities provide flexibility and can be reused across multiple resources, reducing administrative overhead<sup>12</sup>.

This combination ensures secure, efficient, and manageable authentication for your virtual machines and their interactions with the third-party API.  
upvoted 3 times

 **5f2afa7** 6 months 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 4 times

## HOTSPOT

-

You have an Azure subscription named Sub1 that contains the resources shown in the following table.

| Name        | Type                     | In resource group |
|-------------|--------------------------|-------------------|
| Vault1      | Azure Key Vault          | RG1               |
| Automation1 | Azure Automation account | RG1               |
| Automation2 | Azure Automation account | RG2               |
| VM1         | Virtual machine          | RG2               |

Sub1 contains the managed identities shown in the following table.

| Name      | Type            | Assigned to |
|-----------|-----------------|-------------|
| Identity1 | User-assigned   | Automation1 |
| Identity2 | System-assigned | Automation2 |
| Identity3 | System-assigned | VM1         |

Sub1 has the role-based access control (RBAC) role assignments shown in the following table.

| Identity  | Role                   | Scope |
|-----------|------------------------|-------|
| Identity1 | Key Vault Secrets User | RG2   |
| Identity2 | Key Vault Secrets User | Sub1  |
| Identity3 | Key Vault Secrets User | RG1   |

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

Automation1 can access the contents of the secrets stored in Vault1.

☐☐

Identity2 can be assigned to Automation2 to gain access to the contents of the secrets stored in Vault1.

☐☐

VM1 can access the contents of the secrets stored in Vault1.

☐☐

## Correct Answer:

## Answer Area

## Statements

Yes

No

Automation1 can access the contents of the secrets stored in Vault1.

☐☒

Identity2 can be assigned to Automation2 to gain access to the contents of the secrets stored in Vault1.

☒☐

VM1 can access the contents of the secrets stored in Vault1.

☒☐

 **Frank9020** 5 months ago

1: Automation1 has Identity1 assigned to it.

Identity1 has the Key Vault Secrets User role at the RG2 scope. Vault1 is in RG1, not RG2.

Since Identity1 has access to secrets in RG2, but Vault1 is in RG1, Automation1 cannot access the secrets in Vault1. Answer: ✗ No

2: Identity2 is a system-assigned managed identity for Automation2.

Identity2 has the Key Vault Secrets User role at the Subscription (Sub1) level.

Sub1 includes RG1, where Vault1 is located.

Since Identity2 has permission at the subscription level, which includes RG1, it already has access to Vault1. Answer: ✓ Yes

3: VM1 has Identity3 assigned to it.

Identity3 has the Key Vault Secrets User role at the RG1 scope. Vault1 is in RG1.

Since Identity3 has permissions for RG1, and Vault1 is in RG1, VM1 can access the secrets in Vault1. Answer: ✓ Yes

upvoted 4 times

 **Oskarma** 5 months, 1 week ago

1. No. The scope of Identity1 isn't RG1 (Vault1)
  2. Yes. Indeed it's assigned, and i'ts scope is all the Subscription Sub1
  3. Yes. Identity3 is assigned to VM1 and it's scope is RG1, where it's Vault1
- upvoted 3 times

You have an Azure subscription that contains an Azure Automation account named Automation1.



You need to grant Automation1 access to Azure resources. The solution must meet the following requirements:

- Ensure that any permissions granted to Automation1 are removed when the account is deleted.
- Minimize administrative effort.

What should you use?



- A. a client secret
- B. a system-assigned managed identity
- C. a certificate
- D. user-assigned managed identity

**Correct Answer:** B

  **noa808a** 3 months, 2 weeks ago

**Selected Answer: B**

Key word/phrase here is permissions are removed when completed. Only system-assigned managed identity is capable of this.  
upvoted 1 times

  **test123123** 5 months, 3 weeks ago

**Selected Answer: B**

System-Assigned Managed Identity

Lifecycle: Created and managed by Azure. The identity is tied to the lifecycle of the Azure resource (e.g., a virtual machine). When the resource is deleted, the identity is automatically deleted as well.

Scope: Each system-assigned managed identity is unique to a single Azure resource. It cannot be shared across multiple resources.

Use Case: Ideal for scenarios where you want the identity to be automatically managed and deleted with the resource1.

upvoted 3 times

You have a Microsoft Entra tenant named contoso.com that contains an 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. Add a custom domain name to contoso.com.
- B. Configure the External collaboration settings.
- C. Create a guest user account in contoso.com.
- D. Add a WS-Fed identity provider.

**Correct Answer:** C

  **Oskarma** 5 months, 1 week ago

**Selected Answer:** C

Yeap. Simple.

upvoted 2 times

## HOTSPOT

-

You have two Microsoft Entra tenants named contoso.com and fabrikam.com.

Contoso.com contains the users shown in the following table.

| Name  | Type   |
|-------|--------|
| User1 | Member |
| User2 | Member |
| User3 | Guest  |

Contoso.com contains the groups shown in the following table.

| Name   | Membership type | Members       |
|--------|-----------------|---------------|
| Group1 | Assigned        | User1         |
| Group2 | Assigned        | Group1, User2 |

You configure cross-tenant synchronization from contoso.com to fabrikam.com and enable cross-tenant synchronization for User3 and Group2.

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

NOTE: Each correct selection is worth one point.

## Answer Area

| Statements                       | Yes                   | No                    |
|----------------------------------|-----------------------|-----------------------|
| User1 will sync to fabrikam.com. | <input type="radio"/> | <input type="radio"/> |
| User2 will sync to fabrikam.com. | <input type="radio"/> | <input type="radio"/> |
| User3 will sync to fabrikam.com. | <input type="radio"/> | <input type="radio"/> |

## Answer Area

| Statements                       | Yes                              | No                               |
|----------------------------------|----------------------------------|----------------------------------|
| User1 will sync to fabrikam.com. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 will sync to fabrikam.com. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User3 will sync to fabrikam.com. | <input checked="" type="radio"/> | <input type="radio"/>            |

## Correct Answer:

**JohnCH** 3 weeks, 3 days ago

It should be NYN

User1 - Cross-Tenant syn not sync member inside the nested group

User2 - Is a direct member

User3 - Is Guest User

upvoted 3 times

**etodesco** 1 month, 3 weeks ago

NNY for me.

only users is supported.

Show here: <https://learn.microsoft.com/en-us/entra/identity/multi-tenant-organizations/cross-tenant-synchronization-overview>

upvoted 1 times

**etodesco** 1 month, 3 weeks ago

Sorry, but is not clear.

Here: <https://learn.microsoft.com/en-us/entra/identity/multi-tenant-organizations/cross-tenant-synchronization-configure>

says:

"If you select a group to assign to the configuration, only users that are direct members in the group will be in scope for provisioning. You can select a static group or a dynamic group. The assignment doesn't cascade to nested groups"

upvoted 1 times

  **YesPlease** 4 months, 1 week ago

NO - Cross-tenant sync does not sync members of groups nested within groups

Yes - User2 is a direct member of a group that is explicitly going to be synced



Yes - User3 is explicitly going to be synced

upvoted 2 times

  **ethhacker** 4 months, 1 week ago

YYY, group 1 is assigned in group 2

upvoted 1 times

  **Fijii** 4 months ago

No group nesting, only the group "object" is going to be sync

upvoted 1 times

  **AcTiVeGrEnAdE** 2 months ago

cross-tenant sync will not sync group objects; only direct users. As you stated, group nesting is also not supported.

upvoted 1 times



You have a Microsoft Exchange organization that uses an SMTP address space of contoso.com.

Several users use their contoso.com email address for self-service sign-up to Microsoft Entra.


You gain global administrator privileges to the Microsoft Entra tenant that contains the self-signed users.

You need to prevent the users from creating user accounts in the contoso.com Microsoft Entra tenant for self-service sign-up to Microsoft 365 services.

Which PowerShell cmdlet should you run?

- A. Update-MgPolicyAuthorizationPolicy
- B. Update-MgDomain
- C. Update-MgPolicyPermissionGrantPolicyExclude
- D. Update-MgDomainFederationConfiguration

**Correct Answer: A**

  **JFROG** 5 months, 2 weeks ago

**Selected Answer: A**

I agree with A. Check <https://learn.microsoft.com/en-us/microsoft-365/commerce/subscriptions/manage-self-service-signup-subscriptions?view=o365-worldwide#block-users-from-signing-up>  
upvoted 1 times

  **anonymousarpanch** 5 months, 2 weeks ago

**Selected Answer: A**

. Allows to set guest user access level for tenant  
Lookout for update-mgpolicyauthorizationpolicy  
upvoted 1 times

  **northgaterebel** 5 months, 2 weeks ago

**Selected Answer: A**

A is correct. Use the "Update-MgPolicyAuthorizationPolicy" cmdlet with the "AllowedToSignUpEmailBasedSubscriptions" parameter set to False.  
<https://learn.microsoft.com/en-us/entra/identity/users/directory-self-service-signup>  
upvoted 2 times

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%)

 **mert123** Highly Voted 6 months, 1 week ago

**Selected Answer: D**

i think its D


upvoted 5 times

 **AcTiVeGrEnAdE** Most Recent 2 months ago

**Selected Answer: D**

WOW, the wording in this question is sick. I was so tempted to go with B since User 1 appears to already have access given their group membership but the simply fact is that any of these users can request access....even if they belong to a group that has already given them access. User2 does not automatically have access to the app if they an approver for it...just means they been assigned to make decisions. User 3 can request access as well.

upvoted 3 times

 **d1e85d9** 2 months, 3 weeks ago

**Selected Answer: C**

User2 is Approver, means already has access to app,


Then why need request access for user2?

upvoted 1 times

 **AcTiVeGrEnAdE** 2 months ago

Not true, an approver is just a decision maker that is independent of already having access to a app.

upvoted 2 times

 **csi\_2025** 4 months ago

**Selected Answer: D**

I think its D because while User1 is in group1 that doesn't automatically mean he has access to the app.

upvoted 1 times

 **Btn26** 5 months, 4 weeks 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 4 times

  **Shingie** 4 months, 2 weeks ago

Since no restrictions are specified on who can request access, all three users (User1, User2, and User3) are eligible to request access to App1.

upvoted 1 times

  **Sunth65** 6 months ago

**Selected Answer: C**

Approve access to this application: User2 !

upvoted 3 times

## HOTSPOT

-

You have a Microsoft Entra tenant that contains the users shown in the following table.

| Name  | Microsoft Entra role               |
|-------|------------------------------------|
| User1 | Global Administrator               |
| User2 | Attribute Definition Administrator |
| User3 | Security Administrator             |

The tenant contains the identities shown in the following table.

| Name     | Type              |
|----------|-------------------|
| Group1   | Security group    |
| Service1 | Service principal |
| MI1      | Managed identity  |

Which users can create custom security attributes, and to which identities can the attributes be assigned? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Can create custom security attributes:

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

Custom security attributes can be assigned to:

- Group1 only
- Group1 and MI1 only
- Group1 and Service1 only
- Group1, MI1, and Service1 MI1 only
- MI1 and Service1 only
- Service1 only

## Answer Area


Can create custom security attributes:

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

Correct Answer:

Custom security attributes can be assigned to:

- Group1 only
- Group1 and MI1 only
- Group1 and Service1 only
- Group1, MI1, and Service1 MI1 only
- MI1 and Service1 only
- Service1 only

 **d1e85d9** 2 months, 3 weeks ago

Can create custom security attributes:

- Global administrator

- Attribute Definition administrator

Custom security attributes can be assigned to:

- Security group (group1)
  - Service principal (Service1)
- upvoted 1 times

🗨️ 👤 **AcTiVeGrEnAdE** 2 months ago

This is one thing Global Administrator cannot do. Actually learned this in my GCCH tenant when I had a request come in.

Custom security attributes can only be applied to users and service principals

upvoted 1 times

🗨️ 👤 **Rackup** 3 months, 4 weeks ago

User1 and User2 only for creating custom security attributes  
Group1, MI1, and Service1 for where attributes can be assigned

upvoted 1 times

🗨️ 👤 **AcTiVeGrEnAdE** 2 months ago

Global Admin cannot create custom security attributes

upvoted 1 times

🗨️ 👤 **krutesh** 4 months ago

Answer:

User1 and User2 can create custom security attributes.  
custom security attributes can be assigned to Service1 Only.

While Attribute Definition Administrator role is specifically designed for managing custom security attributes, Global Administrators have highest level of permissions and can perform this task as well.

Custom security attributes can be added to following Microsoft Entra objects:

Microsoft Entra users

Microsoft Entra enterprise applications (service principals)

upvoted 1 times

🗨️ 👤 **AcTiVeGrEnAdE** 2 months ago

Global Admin cannot create custom security attributes

upvoted 1 times

🗨️ 👤 **csi\_2025** 4 months ago

This is wrong. A GA does not have the permission to do so. While a GA has widespread permissions across the tenant he does not have permissions for all tasks including creating custom security attributes.

upvoted 3 times

🗨️ 👤 **anonymousarpanch** 4 months, 3 weeks ago

correct. at present custom security attributes can only be assigned to users and service principals. refer <https://learn.microsoft.com/en-us/entra/fundamentals/custom-security-attributes-overview>

upvoted 3 times

You have a Microsoft Entra tenant named contoso.com that contains an 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. Implement Microsoft Entra Connect sync.
- B. Create a guest user account in contoso.com.
- C. Configure the External collaboration settings.
- D. Run the New-MgUser cmdlet.

**Suggested Answer: B**

*Community vote distribution*

B (100%)

 **Shingie** 4 months, 2 weeks ago

**Selected Answer: B**

B. Create a guest user account in contoso.com.

Explanation:

-The contractor uses the user1@outlook.com credentials, meaning they are an external user who is not part of the contoso.com Microsoft Entra tenant.

-To allow them to access App1 while authenticating with their Outlook.com credentials, you should add them as a guest user in Microsoft Entra ID (formerly Azure AD).

-This is done by creating a guest user account in contoso.com using B2B (Business-to-Business) collaboration, which allows them to use their existing Outlook.com account for authentication.

upvoted 1 times

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2 and the users shown in the following table.

| Name  | Department | Member of |
|-------|------------|-----------|
| User1 | Marketing  | Group1    |
| User2 | marketing  | Group2    |
| User3 | HR         | Group1    |

Group2 is a member of Group1.

You configure cross-tenant synchronization with a partner organization named fabrikam.com by using the following configurations:

- Provisioning status: On
- Users and groups: Group1
- Prevent accidental deletion: 500
- Scope: Sync only assigned users and groups
- Scoping filter: Department EQUALS Marketing

From the Cross-tenant synchronization settings, you set Provisioning Mode to Automatic.

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

NOTE: Each correct selection is worth one point.

### Answer Area

#### Statements

Yes No

User1 will be provisioned in the Microsoft Entra tenant of fabrikam.com.

☐
☐

User2 will be provisioned in the Microsoft Entra tenant of fabrikam.com.

☐
☐

User3 will be provisioned in the Microsoft Entra tenant of fabrikam.com.

☐
☐

#### Answer Area

#### Statements

Yes No

**Suggested Answer:** User1 will be provisioned in the Microsoft Entra tenant of fabrikam.com.


☒
☐

User2 will be provisioned in the Microsoft Entra tenant of fabrikam.com.

☐
☒

User3 will be provisioned in the Microsoft Entra tenant of fabrikam.com.

☐
☒

 **Shingie** 4 months, 2 weeks ago

"User1 will be synchronized to fabrikam.com."

Yes → User1 is directly in Group1 and in the Marketing department.

"User2 will be synchronized to fabrikam.com."

No → Group2 is in Group1, but User2 is only inside Group2, not Group1 directly. Only Group1 and its direct members are selected for sync.

"User3 will be synchronized to fabrikam.com."

No → Even though User3 is in Group1, they are in HR, which does not meet the Marketing department filter.

upvoted 4 times



You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.

You need to ensure that you can control access to Microsoft 365 resources by using conditional access policies.

What should you do first?

- A. Disable the User consent settings.
- B. Disable Security defaults.
- C. Configure a multi-factor authentication (MFA) registration policy.
- D. Configure password protection for Windows Server Active Directory.

**Suggested Answer: B**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

Community vote distribution

B (100%)

 **Eltooth**  3 years, 7 months ago

Taken from article in answer: "If your tenant was created on or after October 22, 2019, it is possible security defaults are already enabled in your tenant. To protect all of our users, security defaults are being rolled out to all new tenants created."

To enable CAP you have to disable Security defaults - Answer is correct.

upvoted 22 times

 **a6792d4**  7 months, 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** 11 months, 1 week ago

**Selected Answer: B**

Correct

upvoted 1 times

 **kalyankrishna1** 1 year, 3 months ago

**Selected Answer: B**

Correct answer


upvoted 1 times

 **EmnCours** 1 year, 5 months ago

**Selected Answer: B**

B. Disable Security defaults


upvoted 1 times

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

**Selected Answer: B**

B. Disable Security defaults

upvoted 1 times

 **ShoaibPKDXB** 1 year, 7 months ago

**Selected Answer: B**

Correct B

upvoted 1 times

🗨️ 👤 **francescoc** 1 year, 9 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, 11 months ago

**Selected Answer: B**

Deshabilite los valores predeterminados de seguridad.

upvoted 1 times

🗨️ 👤 **Oknip** 1 year, 11 months ago

**Selected Answer: B**

Disable the security defaults to enable Conditional Access policies

upvoted 2 times

🗨️ 👤 **[Removed]** 2 years 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** 2 years, 2 months ago

On exam- 10/28/22

upvoted 2 times

🗨️ 👤 **Seed001** 2 years, 5 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, 6 months ago

**Selected Answer: B**

You need to disable Security defaults to enable Conditional access policies, si the answer is correctt

upvoted 3 times

🗨️ 👤 **shine98** 2 years, 6 months ago

On the exam - June 12, 2022

upvoted 1 times

🗨️ 👤 **stromnessian** 2 years, 10 months ago

**Selected Answer: B**

Yes, it's B.

upvoted 1 times

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%)

  **TRN80**  5 months, 3 weeks ago

**Selected Answer: D**

User1 (Global Administrator): This role has full access to manage all aspects of Microsoft Entra, including Internet Access1.

User2 (Global Secure Access Administrator): This role specifically includes permissions to manage Microsoft Entra Internet Access1.




User3 (Privileged Role Administrator): This role is focused on managing role assignments and does not include permissions to manage Microsoft Entra Internet Access1.

upvoted 5 times

  **csi\_2025** 4 months ago

FYI, your answer is correct but a GA has not full access to all aspects of Microsoft Entra. Custom Security Attributes can't be managed with a GA only Attribute Definition Administrator or Attribute Assignment Administrator can do that.

upvoted 3 times

  **nicolaslindt**  5 months, 3 weeks ago

**Selected Answer: D**

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

upvoted 2 times

  **Btn26** 5 months, 4 weeks 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 3 times

  **Sunth65** 6 months 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 3 times

Your company has a Microsoft 365 tenant.

The company has a call center that contains 300 users. In the call center, the users share desktop computers and might use a different computer every day. The call center computers are NOT configured for biometric identification.

The users are prohibited from having a mobile phone in the call center.

You need to require multi-factor authentication (MFA) for the call center users when they access Microsoft 365 services.

What should you include in the solution?

- A. a named network location
- B. the Microsoft Authenticator app
- C. Windows Hello for Business authentication
- D. FIDO2 tokens

**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** 4 years 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 11 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** 4 years, 1 month ago

The only logical option.

upvoted 25 times

Nivos23 **Most Recent** 1 year, 7 months ago

**Selected Answer: D**

Correct Answer is D

upvoted 2 times

EmnCours 1 year, 11 months ago

**Selected Answer: D**

Correct Answer: D

upvoted 1 times

dule27 2 years ago

**Selected Answer: D**

D. FIDO2 tokens

upvoted 1 times

ShoaibPKDXB 2 years, 1 month ago

**Selected Answer: D**

Correct D

upvoted 1 times

Aquintero 2 years, 5 months ago

**Selected Answer: D**

D. Fichas FIDO2

upvoted 2 times

Halwagy 2 years, 5 months ago

Selected Answer: D

The FiD02 token  
upvoted 1 times

🗨️ 👤 **[Removed]** 2 years, 6 months ago

Selected Answer: D

Ali\_Pin explained correctly. FIDO2 is the correct answer.  
upvoted 2 times

🗨️ 👤 **ali\_pin** 2 years, 12 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** 3 years 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** 3 years, 1 month 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, 7 months ago

No, Windows Hello Pin is store locally, they may change computer every day it says  
upvoted 2 times

🗨️ 👤 **bleedinging** 3 years, 1 month 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** 3 years, 2 months ago

The call center computers are NOT configured for biometric identification

Answer- C  
upvoted 1 times

🗨️ 👤 **PanBrown** 3 years, 2 months ago

FIDO2 key is the only option in this situation.  
upvoted 1 times

🗨️ 👤 **Yelad** 3 years, 3 months ago

On the exam - March 28, 2022  
upvoted 2 times

🗨️ 👤 **Jun143** 3 years, 3 months ago

just pass the exam today. This came in the question.  
upvoted 1 times

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

All users who run applications registered in Azure AD are subject to conditional access policies.

You need to prevent the users from using legacy authentication.

What should you include in the conditional access policies to filter out legacy authentication attempts?

- A. a cloud apps or actions condition
- B. a user risk condition
- C. a client apps condition
- D. a sign-in risk condition


**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 3 years, 1 month ago

Client apps condition is the correct answer  
upvoted 21 times

 **melatocaroca** Highly Voted 2 years, 11 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** 1 year, 5 months 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 7 months, 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** 9 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** 9 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** 11 months, 3 weeks ago

On the exam, 09/07/2023

upvoted 4 times

🗲️ 👤 **AMZ** 1 year ago

Question valid - 06/23

upvoted 3 times

🗲️ 👤 **mali1969** 1 year 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** 1 year ago

**Selected Answer: C**

C. a client apps condition

upvoted 1 times

🗲️ 👤 **ShoaibPKDXB** 1 year, 1 month ago

**Selected Answer: C**

C is correct

upvoted 1 times

🗲️ 👤 **Halwagy** 1 year, 5 months ago

**Selected Answer: C**

Client App

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 6 months ago

**Selected Answer: C**

Correct answer given.

upvoted 1 times

🗲️ 👤 **kerimnl** 1 year, 8 months ago

**Selected Answer: C**

C. a client apps condition

upvoted 1 times

🗲️ 👤 **Tokiki** 2 years ago

C is correct

upvoted 1 times

🗲️ 👤 **shine98** 2 years ago

On the exam - June 12, 2022

upvoted 2 times

🗲️ 👤 **Nilz76** 2 years, 2 months ago

This question was in the exam 28/April/2022

upvoted 2 times

🗲️ 👤 **Yelad** 2 years, 3 months ago

On the exam - March 28, 2022

upvoted 1 times



You have an Azure Active Directory (Azure AD) tenant.  
You open the risk detections report.  
Which risk detection type is classified as a user risk?

- A. impossible travel
- B. anonymous IP address
- C. atypical travel
- D. leaked credentials

**Suggested Answer: D**

Leaked credentials indicates that the user's valid credentials have been leaked.

Note:

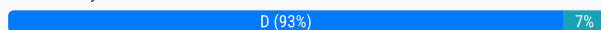
There are several versions of this question in the exam. The question can have other incorrect answer options, including the following:

- ⇒ 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



🗳️ 👤 **JakubK64** Highly Voted 👍 3 years, 1 month ago

Correct - leaked credentials. Rest belongs to sign-in risk  
upvoted 23 times

🗳️ 👤 **Nivos23** Most Recent 🕒 8 months ago

Selected Answer: D  
D. leaked credentials  
upvoted 1 times

🗳️ 👤 **sherifhamed** 9 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** 11 months, 2 weeks ago

Selected Answer: D  
Correct Answer: D  
upvoted 1 times

🗳️ 👤 **mali1969** 1 year 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** 1 year ago

Selected Answer: D  
D. leaked credentials  
upvoted 1 times

🗳️ 👤 **ShoaibPKDXB** 1 year, 1 month ago

Selected Answer: D  
correct D  
upvoted 1 times

🗨️ 👤 **francescoc** 1 year, 3 months 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** 1 year, 5 months ago

**Selected Answer: D**

D. credenciales filtradas

upvoted 1 times

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

**Selected Answer: D**

Leaked credentials is the correct answer. The other options are sign-in risk.

upvoted 1 times

🗨️ 👤 **BTL\_Happy** 1 year, 7 months ago

this came out with different multiple choice.

upvoted 1 times

🗨️ 👤 **Tokiki** 2 years ago

D is correct

upvoted 1 times

🗨️ 👤 **dangerdizzy** 2 years ago

**Selected Answer: D**

Leaked Credentials is the answer

upvoted 1 times

🗨️ 👤 **dangerdizzy** 2 years ago

**Selected Answer: D**

Leaked Credentials

upvoted 1 times

🗨️ 👤 **Davidf** 2 years, 1 month ago

**Selected Answer: D**

Absolutely D

upvoted 1 times

🗨️ 👤 **PanBrown** 2 years, 2 months ago

Leaked Credentials is correct, consider credentials are always classified.

upvoted 1 times

🗨️ 👤 **Jun143** 2 years, 3 months ago

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

upvoted 1 times

You have a Microsoft Entra 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 security key               | Group2 | Yes     |
| Microsoft Authenticator          | Group1 | Yes     |
| Certificate-based authentication | Group3 | Yes     |

Which users will sign in to cloud apps by using number matching?

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

**Correct Answer: A**

  **YesPlease** 4 months, 1 week ago

**Selected Answer: A**



Answer A) User1 only

- Microsoft Authenticator is only numeric

- FIDO2 key can be numeric or alphanumeric

- Certificate-based authentication contain alphanumeric content.

upvoted 1 times

  **csi\_2025** 4 months ago

Your explanation has nothing to do with the question. Its about the feature "number matching" not if it contains numeric. Number matching is a feature of MS Authenticator.

upvoted 1 times

  **anonymousarpanch** 5 months, 2 weeks ago

**Selected Answer: A**

Devil is in detail..it says 'number matching' which is why A

upvoted 2 times

  **armid** 4 months, 2 weeks ago

yeah Fido doesnt display any numbers, not to be confuse with RSA tokens or other hardware tokens

upvoted 1 times

You have a Microsoft 365 tenant.

All users have computers that run Windows 10. Most computers are company-owned and joined to Azure Active Directory (Azure AD). Some computers are user-owned and are only registered in Azure AD.

You need to prevent users who connect to Microsoft SharePoint Online on their user-owned computer from downloading or syncing files. Other users must NOT be restricted.

Which policy type should you create?

- A. a Microsoft Cloud App Security activity policy that has Microsoft Office 365 governance actions configured
- B. an Azure AD conditional access policy that has session controls configured
- C. an Azure AD conditional access policy that has client apps conditions configured
- D. a Microsoft Cloud App Security app discovery policy that has governance actions configured

**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 4 years, 1 month 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, 11 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, 11 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 4 years, 1 month 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, 12 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** 4 years, 1 month ago

This is right. Link explains everything.

upvoted 2 times

🗄️ 👤 **jim85** Most Recent 1 year 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 3 times

🗄️ 👤 **RemmyT** 1 year 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 4 times

🗄️ 👤 **Siraf** 1 year, 6 months 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, 7 months 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 3 times

🗄️ 👤 **haazybanj** 1 year, 7 months 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 2 times

🗄️ 👤 **ACSC** 1 year, 9 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 3 times

🗄️ 👤 **EmnCours** 1 year, 10 months ago

**Selected Answer: B**

Correct Answer is: B

upvoted 3 times

🗨️ 👤 **sehlohomoletsane** 1 year, 10 months ago

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions>

upvoted 1 times

🗨️ 👤 **hellawaits111** 1 year, 11 months ago

**Selected Answer: B**

B is the answer

<https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

upvoted 2 times

🗨️ 👤 **dule27** 1 year, 12 months ago

**Selected Answer: C**

Correction

C. an Azure AD conditional access policy that has client apps conditions configured

upvoted 1 times

🗨️ 👤 **mali1969** 2 years 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, 10 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** 2 years ago

C is the answer: <https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad>

upvoted 1 times

🗨️ 👤 **dule27** 2 years ago

**Selected Answer: B**

B. an Azure AD conditional access policy that has session controls configured

upvoted 2 times

🗨️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

**Selected Answer: B**

B correct

upvoted 2 times

🗨️ 👤 **jojoseph** 2 years, 5 months ago

**Selected Answer: B**

B or C could be right. But I am inclined to B

upvoted 2 times

🗨️ 👤 **Holii** 2 years 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

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, 7 months 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 164 times

🗳️ 👤 **NickHSO** 2 years, 4 months ago

Upvote for additional knowledge! thank you

upvoted 13 times

🗳️ 👤 **Official\_Fridaws** Highly Voted 2 years, 7 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension>

upvoted 5 times

🗳️ 👤 **haazybanj** Most Recent 7 months, 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** 11 months, 2 weeks ago

**Selected Answer: C**

Correct Answer: C

upvoted 1 times

🗳️ 👤 **mali1969** 1 year 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** 1 year ago

**Selected Answer: C**

C. Network Policy Server (NPS)

upvoted 1 times

🗲️ 👤 **ShoaibPKDXB** 1 year, 1 month ago

**Selected Answer: C**

Correct C

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 6 months ago

**Selected Answer: C**

C is correct.

upvoted 1 times

🗲️ 👤 **Zubairr13** 1 year, 11 months ago

On the exam, 7/23/2022.

upvoted 2 times

🗲️ 👤 **Tokiki** 2 years ago

Yes, NPS is needed

upvoted 1 times

🗲️ 👤 **shine98** 2 years ago

On the exam - June 12, 2022

upvoted 1 times

🗲️ 👤 **Yelad** 2 years, 3 months ago

On the exam - March 28, 2022

upvoted 1 times

🗲️ 👤 **Jun143** 2 years, 3 months ago

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

upvoted 1 times

🗲️ 👤 **Pravda** 2 years, 5 months ago

**Selected Answer: C**

On the exam 1/20/2022

upvoted 2 times



You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant is configured to sync with an on-premises Active Directory domain. The domain contains the servers shown in the following table.

| Name    | Operating system    | Configuration     |
|---------|---------------------|-------------------|
| Server1 | Windows Server 2019 | Domain controller |
| Server2 | Windows Server 2016 | Domain controller |
| Server3 | Windows Server 2019 | Azure AD Connect  |

The domain controllers are prevented from communicating to the internet.

You implement Azure AD Password Protection on Server1 and Server2.

You deploy a new server named Server4 that runs Windows Server 2019.

You need to ensure that Azure AD Password Protection will continue to work if a single server fails.

What should you implement on Server4?

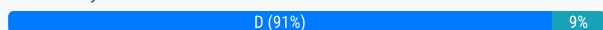
- A. Azure AD Connect
- B. Azure AD Application Proxy
- C. Password Change Notification Service (PCNS)
- D. the Azure AD Password Protection proxy service

**Suggested Answer:** D

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

Community vote distribution



**jhap** Highly Voted 3 years, 2 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 11 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** 1 year 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** 7 months, 1 week ago

As usual, the correct answer isn't necessarily the best answer as a long term solution.

upvoted 1 times

**EmnCours** 1 year, 5 months ago

**Selected Answer: D**

Correct Answer: D

upvoted 2 times

🗳️ 👤 **EmnCours** 1 year, 4 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

upvoted 1 times

🗳️ 👤 **mali1969** 1 year, 6 months 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, 6 months ago

**Selected Answer: D**

D. the Azure AD Password Protection proxy service

upvoted 1 times

🗳️ 👤 **ShoaibPKDXB** 1 year, 7 months ago

**Selected Answer: D**

D correct

upvoted 1 times

🗳️ 👤 **Marian2023** 1 year, 10 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, 11 months ago

**Selected Answer: D**

D. el servicio de proxy de protección con contraseña de Azure AD

upvoted 2 times

🗳️ 👤 **[Removed]** 2 years ago

**Selected Answer: D**

The answer given is a correct answer. Azure AD Password Protection proxy service.

upvoted 2 times

🗳️ 👤 **den5\_pepito83** 2 years, 1 month ago

ON EXAM 14/11/2022

upvoted 3 times

🗳️ 👤 **SangSang** 2 years, 1 month ago

which one do you choose in your exam?

upvoted 1 times

🗳️ 👤 **Imee** 2 years, 3 months ago

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

upvoted 1 times

🗳️ 👤 **Zubairr13** 2 years, 5 months ago

On the exam, 7/23/2022.

upvoted 1 times

🗳️ 👤 **rachee** 2 years, 5 months ago

would the answer not be A. Azure AD Connect? there are 2 domain controllers both configured with Azure AD Password Protection. The question is to ensure Azure AD Password protection will continue if a "single" server fails. If one of the DCs fail, the other will still be available. There is only 1 Azure AD Connect server; I would think you would configure a HA Azure AD connect server. Bad question, because the password list is cached on the DCs and only a single server failure.

upvoted 1 times

🗳️ 👤 **rachee** 2 years, 5 months ago

Reading the link where it says Azure AD Password Protection proxy for HA, I change the answer to D.

upvoted 3 times



  **sapien45** 2 years, 6 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

Choose one or more servers to host the Azure AD Password Protection proxy service. The following considerations apply for the server(s):



The host machine must be joined to any domain in that forest

upvoted 2 times

  **shine98** 2 years, 6 months ago

On the exam - June 12, 2022

upvoted 1 times

  **Nilz76** 2 years, 8 months ago

This question was in the exam 28/April/2022

upvoted 1 times

You have a Microsoft Entra tenant.

You have the devices shown in the following table.

| Name    | Operating system | Join type                  |
|---------|------------------|----------------------------|
| Device1 | Windows 11       | Microsoft Entra registered |
| Device2 | Windows 11       | None                       |
| Device3 | Windows 10       | Microsoft Entra joined     |
| Device4 | Windows 10       | Microsoft Entra registered |

You configure Microsoft Entra Internet Access for the tenant.

On which devices can you use Global Secure Access?

- A. Device1 only
- B. Device3 only
- C. Device1 and Device2 only
- D. Device1, Device3, and Device4 only
- E. Device1, Device2, Device3, and Device4

**Correct Answer: B**

  **\_kkl** 5 months, 2 weeks ago

**Selected Answer: B**

The learn link clearly states registered devices are not supported <https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-install-windows-client>  
upvoted 4 times

  **JFROG** 5 months, 3 weeks ago

**Selected Answer: B**

I'm going for option B. Look at the Prerequisites where it says Microsoft Entra registered devices aren't supported.  
<https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-install-windows-client>  
upvoted 4 times

  **TRN80** 5 months, 3 weeks ago

**Selected Answer: D**

To use Microsoft Entra Internet Access, the device must be associated with Microsoft Entra in some way, either through being Microsoft Entra Registered or Microsoft Entra Joined. This association ensures that the device can be managed and secured according to your organization's policies and access controls.

To use Microsoft Entra Internet Access, the device's operating system must be supported by Microsoft Entra. Here are the general OS requirements:

Windows: Windows 10 and later versions are supported. Ensure that the devices are updated with the latest security patches and updates.

macOS: macOS 10.15 (Catalina) and later versions are supported.

iOS/iPadOS: iOS 13 and later versions are supported.

Android: Android 8.0 (Oreo) and later versions are supported.

upvoted 1 times

  **9H3zmT6** 2 months ago

The prerequisites differ depending on the client OS. In the case of Windows, it must be Entra Joined or Hybrid Joined. Since all the client OS presented in this question are Windows, the answer is B.  
upvoted 1 times

DRAG DROP -

You have a Microsoft 365 E5 tenant.

You purchase a cloud app named App1.

You need to enable real-time session-level monitoring of App1 by using Microsoft Cloud App Security.

In which order should you perform the actions? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

### Actions

### Answer Area

From Microsoft Cloud App Security, create a session policy.

Publish App1 in Azure Active Directory (Azure AD).

Create a conditional access policy that has session controls configured.

From Microsoft Cloud App Security, modify the Connected apps settings for App1.



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 4 years 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 93 times

**Ed2learn** 4 years 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, 9 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** 3 years, 5 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, 6 months 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** 3 years, 1 month ago

Correct... perfect

upvoted 2 times

🗨️ 👤 **Ed2learn** Highly Voted 4 years 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, 11 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** 3 years, 1 month ago

Nop, the last two should be interchanged.

upvoted 3 times

🗨️ 👤 **Bloembar** 3 years, 11 months ago

Correct tested it on a lab envoriment

upvoted 4 times

🗨️ 👤 **w00t** 2 years, 9 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, 10 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, 11 months ago

On the exam, 09/07/2023

upvoted 2 times

🗨️ 👤 **dule27** 1 year, 12 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** 2 years ago

Question valid - 06/23

upvoted 2 times

🗳️ 👤 **eleazarrrd** 2 years, 2 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** 2 years, 3 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** 10 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** 2 years, 3 months ago

I agree with Jason

<https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-deployment-aad>

upvoted 1 times

🗳️ 👤 **[Removed]** 2 years, 6 months ago

Explanation is correct: <https://www.examttopics.com/exams/microsoft/sc-300/view/11/#:~:text=The%20correct%20order%20is,allowing%20session%20controlled%20policies>.

upvoted 1 times

🗳️ 👤 **Faheem2020** 2 years, 9 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, 9 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, 9 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, 11 months ago

On the exam, 7/23/2022.

upvoted 2 times

🗲️ 👤 **shine98** 3 years ago

On the exam - June 12, 2022

upvoted 1 times

🗲️ 👤 **RandomNickname** 3 years 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** 3 years, 2 months ago

This question was in the exam 28/April/2022

upvoted 1 times



You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a notification through the Microsoft Authenticator app
- B. 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



**stromnessian** Highly Voted 2 years, 10 months ago

**Selected Answer: C**

If you think it's anything other than C, maybe you need to consider a career change.

upvoted 25 times

**DiscGolfer** 1 year, 10 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** 1 year, 4 months ago

yeah, it's never too late..

upvoted 2 times

**Justin0020** 8 months, 2 weeks ago

I think its A ;)

Just kidding

upvoted 1 times

**Melwin86** Highly Voted 3 years, 1 month ago

Answer C in correct. Why everyone thinking that answer A is correct ?

upvoted 7 times

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

Selected Answer: C

Answer) C

The question is telling you that their phone will not have cellular access and no WiFi to connect to at the remote location. Although Microsoft Authenticator is able to work offline, answer "A" is wrong because the MS Authenticator App will not be able to get a notification. So the only other MFA option listed that will work is Windows Hello for Business.

upvoted 1 times

🗨️ 👤 **Frank9020** 5 months ago

Selected Answer: C

C: Windows Hello for Business is a passwordless authentication method that uses biometrics (fingerprint, facial recognition) or PINs to authenticate users.

It does not require internet or mobile network access at the time of authentication because the credentials are stored securely on the device and validated locally.

upvoted 1 times

🗨️ 👤 **Frank9020** 5 months ago

Microsoft Authenticator has two main ways to authenticate users:

- 1: A notification through the Microsoft Authenticator app" it refers to push notifications, which require an internet connection (Wi-Fi or mobile data).
- 2: A verification code from the Microsoft Authenticator app" The phrase "a verification code" suggests the use of a time-based one-time password (TOTP) Because TOTP works offline, this is a valid MFA method for remote users.

Authenticator Method Mentioned Needs Internet?

"A notification" (Push Notification) ✔ Yes

"A verification code" (TOTP Code) ✗ No

upvoted 1 times

🗨️ 👤 **Alcpt** 8 months ago

You need a career change. The answer is A. Authenticator did not need wifi or cell coverage to work.

upvoted 1 times

🗨️ 👤 **Frank9020** 5 months ago

Microsoft Authenticator has two main ways to authenticate users:

- 1: A notification through the Microsoft Authenticator app" it refers to push notifications, which require an internet connection (Wi-Fi or mobile data).
- 2: A verification code from the Microsoft Authenticator app" The phrase "a verification code" suggests the use of a time-based one-time password (TOTP) Because TOTP works offline, this is a valid MFA method for remote users.

Authenticator Method Mentioned Needs Internet?

"A notification" (Push Notification) ✔ Yes

"A verification code" (TOTP Code) ✗ No

upvoted 2 times

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

Selected Answer: C

C. Windows Hello for Business

upvoted 1 times

🗨️ 👤 **DasChi\_cken** 1 year, 4 months ago

You dont have cellular Connection so SMS wont Work

An App passcode is Not a MFA at all, its just an on-top Security layer

As mentioned from Cepheid a Hotspot could be used but IT was never mentioned in the question. You cant tell If the Hotspot Feature is disabled by Policy...

Windows hello is the only correct answer, even if the Laptop does not have any biometrics sensor you can use a PIN

upvoted 1 times

🗲️ 👤 **dule27** 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 correct

upvoted 1 times

🗲️ 👤 **SusanGlenn5** 1 year, 9 months ago

I think it's A

upvoted 1 times

🗲️ 👤 **ra1paul** 1 year, 10 months ago

Definitely C.

upvoted 1 times

🗲️ 👤 **Cepheid** 2 years 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** 2 years ago

I think it's A though

upvoted 1 times

🗲️ 👤 **Rearalfonsina** 2 years, 5 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, 6 months ago

**Selected Answer: C**

The answer C is correct . The question states " The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity ". so there is no way a user would get a notification through Microsoft Authenticator App. Windows Hello for business is also considered an MFA authentication method for Azure AD registered and Joined devices

upvoted 7 times

🗲️ 👤 **Rameshbetha** 2 years, 6 months ago

have in exam on June 21 2022.

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Azure portal, you configure the 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, 7 months ago

No indeed | Referenced to <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#block-and-unblock-users> with Fraud alert  
upvoted 5 times

 **syougun200x** Most Recent 8 months, 3 weeks ago

To enable the alert function.

Azure Entre -> security -> MFA -> Fraud Alert  
upvoted 1 times

 **EmnCours** 10 months, 2 weeks ago

Selected Answer: B

You need to configure the fraud alert settings.  
upvoted 2 times

 **mali1969** 1 year 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** 1 year ago

Selected Answer: B

B. No is the answer  
upvoted 1 times

 **ShoaibPKDXB** 1 year, 1 month ago

Selected Answer: B

Correct B. NO  
upvoted 1 times

 **Aquintero** 1 year, 5 months 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, 11 months ago

On the exam, 7/23/2022.

upvoted 1 times

🗨️ 👤 **DemekeAd** 2 years, 2 months ago

No.

to block user

Browse to Azure Active Directory > Security > MFA > Block/unblock users.

upvoted 2 times

🗨️ 👤 **Yelad** 2 years, 3 months ago

On the exam - March 28, 2022

upvoted 1 times

🗨️ 👤 **Jun143** 2 years, 3 months ago

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

upvoted 1 times

🗨️ 👤 **zmlapq99** 2 years, 4 months ago

On exam few days ago.

upvoted 1 times

🗨️ 👤 **Pravda** 2 years, 5 months ago

On the exam 1/20/2022

upvoted 1 times

🗨️ 👤 **Iamjudeicon** 2 years, 6 months ago

Indeed No

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Azure portal, you configure the Account lockout settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

B. No

**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** 10 months, 2 weeks ago

**Selected Answer: B**

B. No is the correct answer

upvoted 1 times

🗳️ 👤 **dule27** 1 year ago

**Selected Answer: B**

B. No is the correct answer

upvoted 1 times

🗳️ 👤 **jack987** 1 year, 6 months 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, 6 months ago

**Selected Answer: B**

Fraud Settings need to be configured, meaning this solution does not meet the goal.

upvoted 2 times

🗳️ 👤 **Zubairr13** 1 year, 11 months ago

On the exam, 7/23/2022.

upvoted 1 times

🗳️ 👤 **tqtuan1512** 2 years, 1 month ago

I think it should be B

upvoted 1 times

🗳️ 👤 **mzsf3c** 2 years, 2 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** 2 years, 1 month 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** 2 years, 3 months ago

On the exam - March 28, 2022

upvoted 1 times

  **TonytheTiger** 2 years, 3 months ago



On the exam today - March 4, 2022

upvoted 1 times

  **zmlapq99** 2 years, 4 months ago

On exam few days ago.

upvoted 1 times

  **Pravda** 2 years, 5 months ago

On the exam 1/20/2022

upvoted 1 times

  **KB10** 2 years, 7 months ago

No indeed | Referenced to <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#block-and-unblock-users> with Fraud alert

upvoted 3 times

  **casti** 2 years, 7 months ago

Should Be A

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout>

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Azure portal, you configure the Block/unblock users settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

B. No

**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%)

 **MORK2000** Highly Voted 3 years, 7 months ago

go to MFA>settings>Fraud Alert>allow>autoblock>on>save  
upvoted 11 times

 **Panama469** 11 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 1 year, 4 months ago

A is the correct answer, I was able to connect with the authenticator app without wifi  
upvoted 2 times

 **EmnCours** 1 year, 11 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, 11 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** 2 years ago

**Selected Answer: B**

B. No is the correct answer

upvoted 1 times



🗨️ 👤 **[Removed]** 2 years, 6 months ago

**Selected Answer: B**

Fraud Settings need to be configured, meaning this solution does not meet the goal.

upvoted 1 times

🗨️ 👤 **shoutiv** 2 years, 6 months ago

**Selected Answer: B**

B - No

It should be Azure Active Directory > Security > Multifactor authentication > Fraud alert -> Allow users to submit fraud alerts to On

Pay attention to the words - you need to block the users AUTOMATICALLY

Explanation from MS docs:

FRAUD ALERT

The fraud alert feature lets users report fraudulent attempts to access their resources. When an unknown and suspicious MFA prompt is received, users can report the fraud attempt by using the Microsoft Authenticator app or through their phone.

The following fraud alert configuration options are available:

- Automatically block users who report fraud.
- Code to report fraud during initial greeting.

BLOCK AND UNBLOCK USERS

If a user's device is lost or stolen, you can block Azure AD Multi-Factor Authentication attempts for the associated account. Any Azure AD Multi-Factor Authentication attempts for blocked users are automatically denied. Users remain blocked for 90 days from the time that they're blocked.

upvoted 3 times

🗨️ 👤 **Joshuaau** 2 years, 7 months ago

Is the given answer correct or incorrect? I would think the answer is A

upvoted 1 times

🗨️ 👤 **Zubairr13** 2 years, 11 months ago

On the exam, 7/23/2022.

upvoted 1 times

🗨️ 👤 **Yelad** 3 years, 3 months ago

On the exam - March 28, 2022

upvoted 1 times

🗨️ 👤 **TonytheTiger** 3 years, 3 months ago

On the exam today - March 4, 2022

upvoted 1 times

🗨️ 👤 **zmlapq99** 3 years, 4 months ago

On exam few days ago.

upvoted 2 times

🗨️ 👤 **Pravda** 3 years, 5 months ago

On the exam 1/20/2022

upvoted 1 times

🗨️ 👤 **KB10** 3 years, 7 months ago

Should be Yes referenced to <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#block-and-unblock-users-with-Fraud-alert>

upvoted 1 times

🗨️ 👤 **KB10** 3 years, 7 months ago

Sorry my fault, answer is right

upvoted 2 times

## HOTSPOT -

You have a Microsoft 365 tenant.

You need to identify users who have leaked credentials. The solution must meet the following requirements:

- ⇒ Identify sign-ins by users who are suspected of having leaked credentials.
- ⇒ Flag the sign-ins as a high-risk event.
- ⇒ Immediately enforce a control to mitigate the risk, while still allowing the user to access applications.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

To classify leaked credentials as high-risk, use:

|                                                                        |
|------------------------------------------------------------------------|
| Azure Active Directory (Azure AD) Identity Protection                  |
| Azure Active Directory (Azure AD) Privileged Identity Management (PIM) |
| Identity Governance                                                    |
| Self-service password reset (SSPR)                                     |

To trigger remediation, use:

|                                             |
|---------------------------------------------|
| Client apps not using Modern authentication |
| Device state                                |
| Sign-in risk                                |
| User location                               |
| User risk                                   |

To mitigate the risk, select:

|                                                |
|------------------------------------------------|
| Apply app enforced restrictions                |
| Block access                                   |
| Grant access but require app protection policy |
| Grant access but require password change       |

**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**  3 years, 10 months ago

It's correct

upvoted 14 times

 **BaderJ**  3 years, 9 months ago

Passed the exam today 23/09/2021

This question came in the exam.

upvoted 8 times

  **Ademola\_12** Most Recent 1 year, 4 months ago

I'm just about to take this exam soon .

upvoted 3 times

  **Tuvshinjargal** 1 year, 4 months 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

  **csi\_2025** 4 months ago

Wrong. User-Risk and change password is the correct solution.

upvoted 1 times

  **Tony416** 10 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, 11 months ago



It's correct

upvoted 1 times

  **Heshan** 1 year, 11 months ago

On the exam, 09/07/2023

upvoted 5 times

  **dule27** 1 year, 12 months ago

Azure AD Identity protection

User risk

Grant access but require password change

upvoted 2 times

  **chrisp1992** 2 years, 6 months ago

Answer is correct.

upvoted 1 times

  **Zubairr13** 2 years, 11 months ago

On the exam, 7/23/2022.

upvoted 4 times

  **rachee** 2 years, 11 months ago

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

upvoted 2 times

  **Xyz\_40** 3 years, 1 month ago

correct.

upvoted 2 times

  **Jun143** 3 years, 3 months ago

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

upvoted 2 times

  **Bluediamond** 3 years, 4 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** 3 years, 4 months ago

NVM. It is right...read it wrong

upvoted 3 times

  **Pravda** 3 years, 5 months ago

On the exam 1/20/2022

upvoted 2 times

## HOTSPOT -

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

| Name  | Role                             |
|-------|----------------------------------|
| User1 | Conditional Access administrator |
| User2 | Authentication administrator     |
| User3 | Security administrator           |
| User4 | Security operator                |

You plan to implement Azure AD Identity Protection.

Which users can configure the user risk policy, and which users can view the risky users report? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Configure the user risk policy:

View the risky users report:

### Answer Area

Suggested Answer:

Configure the user risk policy:

View the risky users report:

Reference:

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

 **oberte007**  2 years, 10 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 60 times

 **JCKD4Ni3L** 8 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 8 times

  **jack987** 1 year, 6 months ago

I agree with oberte007.



upvoted 1 times

  **DaBummer** 2 years, 9 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, 7 months 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, 9 months ago

agree your point

upvoted 2 times

  **007Ali**  2 years, 5 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 38 times

  **59e8fdb**  3 months, 3 weeks ago

This is managed with conditional access policies now, and will be deprecated in 2026 so not sure if it's still relevant...

upvoted 3 times

  **anonymousarpanch** 4 months, 3 weeks ago

if you see this link '<https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection>', you will notice that in the table you will see Security Administrator as having full access on ID protection and security operator as having access to reports except risky sign-ins report. NOTE: below the table you will see 'Conditional Access administrators can create policies that factor in user or sign-in risk as a condition. Find more information in the article Conditional Access: Conditions.' which clarifies that User 1, User 3 should be for box 1 and user1, 3, 4 for box 2.

upvoted 2 times

  **anonymousarpanch** 4 months, 3 weeks ago

in addition to the above, you can also look at this URL. <https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-configure-risk-policies>. The step by step instructions calls out that you have to sign in as 'Conditional Access Administrator'

upvoted 1 times

  **dule27** 1 year ago

Configure the user risk policy: User 3 only  
View the risky users report: User 3 and User 4 only  
upvoted 3 times

🗨️ 👤 **LeTrinh** 1 year, 4 months 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** 1 year, 5 months ago

configurar la politica solo el Usuario 3 y luego 3 y 4.  
upvoted 2 times

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

Oberte is correct User 3 and then 3 and 4.  
upvoted 2 times

🗨️ 👤 **Zubairr13** 1 year, 11 months ago

On the exam, 7/23/2022.  
upvoted 3 times

🗨️ 👤 **Silent\_Muzinde** 2 years, 2 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** 2 years, 3 months ago

just pass the exam today. This came in the question.  
upvoted 1 times

🗨️ 👤 **stromnessian** 2 years, 3 months ago

Tested to confirm:  
Configure: User 3 only  
Read report: Users 3 and 4  
upvoted 6 times

🗨️ 👤 **TonytheTiger** 2 years, 3 months ago

On the exam today - March 4, 2022  
upvoted 2 times

🗨️ 👤 **GPerez73** 2 years, 4 months ago

First box: User3 // Second box: User3 and User4  
Tested!  
upvoted 4 times

🗨️ 👤 **KennethYY** 2 years, 4 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** 2 years, 5 months ago

On the exam 1/20/2022  
upvoted 1 times

🗨️ 👤 **NawafAli** 2 years, 5 months ago

Tested in Lab, correct answer is -  
Configure the user risk policy - user3  
View the risky users report - user3 & user4  
upvoted 9 times

## HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains a group named Group3 and an administrative unit named Department1. Department1 has the users shown in the Users exhibit. (Click the Users tab.)

[Dashboard](#) > [ContosoAzureAD](#) > [Department1 Administrative Unit](#)

**Department1 Administrative Unit | Users (Preview)**  
ContosoAzureAD - Azure Active Directory

+ Add member Remove member Bulk operations Refresh Columns Preview features Got feedback?

This page includes previews available for your evaluation. View previews →

Search users Add filters

2 users found

|                          | Name  | User principal name               | User type | Directory synced |
|--------------------------|-------|-----------------------------------|-----------|------------------|
| <input type="checkbox"/> | User1 | User1@m365x629615.onmicrosoft.com | Member    | No               |
| <input type="checkbox"/> | User2 | User2@m365x629615.onmicrosoft.com | Member    | No               |

Department1 has the groups shown in the Groups exhibit. (Click the Groups tab.)

[Dashboard](#) > [ContosoAzureAD](#) > [Department1 Administrative Unit](#)

**Department1 Administrative Unit | Groups**  
ContosoAzureAD - Azure Active Directory

>> + Add Remove Refresh Columns Preview features Got feedback?

Search groups Add filters

|                          | Name   | Group Type | Membership Type |
|--------------------------|--------|------------|-----------------|
| <input type="checkbox"/> | Group1 | Security   | Assigned        |
| <input type="checkbox"/> | 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    |                                                    |      |                                                                       |
| <a href="#">Admin1</a> | <a href="#">Admin1@m365x629615.onmicrosoft.com</a> | User | <a href="#">Department1 Administrative Unit (Administrative unit)</a> |
| <a href="#">Admin2</a> | <a href="#">Admin2@m365x629615.onmicrosoft.com</a> | User | <a href="#">Directory</a>                                             |

The members of Group2 are shown in the Group2 exhibit. (Click the Group2 tab.)

[Dashboard](#) > [ContosoAzureAD](#) > [Groups](#) > [Group2](#)

**Group2 | Members**  
Group

>> + Add members Remove Refresh Bulk operations Columns Preview features Got feedback?

This page includes previews available for your evaluation. View previews →

Direct members

|                          | Name  | User type |
|--------------------------|-------|-----------|
| <input type="checkbox"/> | User3 | Member    |
| <input type="checkbox"/> | User4 | Member    |

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



NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

| Statements                                         | Yes                   | No                    |
|----------------------------------------------------|-----------------------|-----------------------|
| Admin1 can reset the passwords of User3 and User4. | <input type="radio"/> | <input type="radio"/> |
| Admin1 can add User1 to Group 2                    | <input type="radio"/> | <input type="radio"/> |
| Admin 2 can reset the password of User1.           | <input type="radio"/> | <input type="radio"/> |

Suggested Answer:

## Answer Area

| Statements                                         | Yes                              | No                               |
|----------------------------------------------------|----------------------------------|----------------------------------|
| Admin1 can reset the passwords of User3 and User4. | <input type="radio"/>            | <input checked="" type="radio"/> |
| Admin1 can add User1 to Group 2                    | <input type="radio"/>            | <input checked="" type="radio"/> |
| Admin 2 can reset the password of User1.           | <input checked="" type="radio"/> | <input type="radio"/>            |

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units>

 **Beitran** Highly Voted 4 years, 1 month ago

So the correct answer is No, Yes, Yes  
upvoted 113 times

 **NawafAli** 3 years, 5 months ago

Correct answer, tested in lab.  
upvoted 2 times

 **xDinoKoalax** 3 years, 3 months ago


Tested in lab on Mar.06, 2022, the answer is NO, YES, YES  
upvoted 8 times

 **GlenRMag16** 3 years, 4 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, 8 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, 10 months ago

Tested in my own lab. No, Yes, Yes is correct.

upvoted 13 times

  **d1e85d9**  3 months, 2 weeks ago

NO

YES


YES

upvoted 1 times

  **javifedz** 1 year, 3 months ago

Agree. Correct answer is No, Yes, Yes

upvoted 1 times

  **Nivos23** 1 year, 7 months ago

the correct answer is No, Yes, Yes



upvoted 2 times

  **Nyamnyam** 1 year, 7 months ago

NO, YES, YES!

Why don't the Examtopics contributors ever update the info?

upvoted 3 times

  **calom52** 7 months ago

Because its based in Hong Kong

upvoted 1 times

  **joe9527** 1 year, 8 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, 8 months ago

nvm. I'm making a fool of myself lol.

upvoted 2 times

  **joe9527** 1 year, 8 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, 11 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, 11 months ago

On the exam, 09/07/2023

upvoted 2 times

  **Sango** 1 year, 12 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 3 times

  **AMZ** 2 years ago

Question valid - 06/23

upvoted 2 times

  **dule27** 2 years ago

NO

YES

YES

upvoted 1 times

  **HelloItsSam** 2 years, 4 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** 2 years, 5 months ago

Para mi la respuesta es No, No, Si; Admin1 es administrador de de la unidad administrativa Department1, entonces el Grupo2 y el usuario1 pertenecen a la unidad administrativa de donde pertenece el administrador de AU Department1. que alguien me corrija si me equivoco pero el administrador de usuario de la unidad administrativa deberia gestionar los grupos y los usuarios de la AU

upvoted 1 times

  **Halwagy** 2 years, 5 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, 7 months ago

No, Yes, Yes. Confirmed in lab.

upvoted 2 times

  **Jhill777** 2 years, 7 months 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, 9 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 4 times

  **Hot\_156** 2 years, 9 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, 9 months ago

I wish I could delete messages... lol This is N, Y, Y...

upvoted 7 times

  **[Removed]** 2 years, 2 months ago

Respect coming back 2 weeks later to fix your response

upvoted 7 times

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

🗳️ 👤 **Iamjudeicon** Highly Voted 2 years, 6 months ago

Correct Answer A

upvoted 5 times

🗳️ 👤 **EmnCours** Most Recent 11 months, 2 weeks ago

Selected Answer: A

Report suspicious activity, the updated MFA Fraud Alert feature

upvoted 2 times

🗳️ 👤 **dule27** 1 year ago

Selected Answer: A

A. Yes is the correct answer

upvoted 1 times

🗳️ 👤 **Jhill777** 1 year, 7 months ago

Selected Answer: A

Correct answer is A.

upvoted 1 times

🗳️ 👤 **samir45** 1 year, 9 months ago

Selected Answer: A

Correct answer.

upvoted 1 times

🗳️ 👤 **Zubairr13** 1 year, 11 months ago

On the exam, 7/23/2022.

upvoted 1 times

🗳️ 👤 **mzsf3c** 2 years, 2 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** 2 years, 1 month ago

You're wrong, just check in the portal.

upvoted 3 times

  **Davidf** 2 years, 1 month 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** 2 years, 3 months ago



On the exam - March 28, 2022

upvoted 2 times

  **Dineshshri** 2 years, 3 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** 2 years, 3 months ago



On the exam today - March 4, 2022

upvoted 1 times

  **zmlapq99** 2 years, 4 months ago

On exam few days ago.

upvoted 1 times

  **Pravda** 2 years, 5 months ago

On the exam 1/20/2022

upvoted 1 times

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a notification through the Microsoft Authenticator app
- B. email
- C. security questions
- D. a verification code from the Microsoft Authenticator app

**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 login.

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 3 years, 2 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 9 times

🗳️ **DiscGolfer** 2 years, 4 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 3 years 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, 10 months ago

**Selected Answer: D**

6 digit verification code is useable offline

upvoted 3 times

🗳️ **stev\_au** 1 year, 11 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** 8 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, 11 months ago

**Selected Answer: D**

D. a verification code from the Microsoft Authenticator app

upvoted 1 times

🗨️ 👤 **dule27** 2 years ago

**Selected Answer: D**

D. a verification code from the Microsoft Authenticator app

upvoted 1 times

🗨️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

**Selected Answer: D**

correct

upvoted 1 times

🗨️ 👤 **VeIN** 2 years, 6 months ago

**Selected Answer: D**

Hope this will illustrate better if someone is confused:

<https://www.strath.ac.uk/professionalservices/is/cybersecurity/mfa/whatifidonthaveasignalorwi-ficonnectiononmyphone/>

upvoted 2 times

🗨️ 👤 **Fcnet** 2 years, 8 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, 8 months ago

oops my bad D solution is right as you can install the authenticator App from the windows store so you can validate the code, everything is fine :)

<https://www.microsoft.com/en-us/p/microsoft-authenticator/9nblgggzmj6?activetab=pivot:overviewtab>

upvoted 1 times

🗨️ 👤 **hieverybody** 2 years, 5 months ago

OS: Windows 10 Mobile version 14393.0 or higher, Windows 8 Mobile

No desktop versions.

upvoted 1 times

🗨️ 👤 **Fcnet** 2 years, 8 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, 8 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, 9 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, 9 months ago

Disregard, i'm a dumb dumb. Of course, there is no "Email" Azure MFA option.

Answer is D

upvoted 1 times



## HOTSPOT -

You have a Microsoft 365 tenant.

You create a named location named HighRiskCountries that contains a list of high-risk countries.

You need to limit the amount of time a user can stay authenticated when connecting from a high-risk country.

What should you configure in a conditional access policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Configure HighRiskCountries by using:

|                       |   |
|-----------------------|---|
|                       | ▼ |
| A cloud app or action |   |
| A condition           |   |
| A grant control       |   |
| A session control     |   |

Configure Sign-in frequency by using:

|                       |   |
|-----------------------|---|
|                       | ▼ |
| A cloud app or action |   |
| A condition           |   |
| A grant control       |   |
| A session control     |   |

**Answer Area**

Suggested Answer:

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**  2 years, 1 month ago

This is correct. CONDITION-->named LOCATION.

SESSION-->SIGN-IN FREQUENCY

upvoted 14 times

 **JCKD4Ni3L**  8 months ago

Correct answers!

upvoted 2 times

 **EmnCours** 11 months, 2 weeks ago

This is correct.

CONDITION-->named LOCATION.

SESSION-->SIGN-IN FREQUENCY

upvoted 3 times

  **AMZ** 1 year ago

Question valid - 06/23

upvoted 4 times

  **dule27** 1 year ago

High Risk Countires : A condition

Sign in frequency : A session control

upvoted 2 times

  **Aquintero** 1 year, 5 months ago

Correcto, primero la condición y despues el control de sesion

upvoted 2 times

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

Given answers are correct.

upvoted 2 times

  **RandomNickname** 2 years ago

Given answer correct

upvoted 4 times

## HOTSPOT -

A user named User1 attempts to sign in to the tenant by entering the following incorrect passwords:

- ⇒ Pa55w0rd12
- ⇒ Pa55w0rd12
- ⇒ Pa55w0rd12
- ⇒ Pa55w.rd12
- ⇒ Pa55w.rd123
- ⇒ Pa55w.rd123
- ⇒ Pa55w.rd123
- ⇒ Pa55word12
- ⇒ Pa55word12
- ⇒ Pa55word12
- ⇒ Pa55w.rd12

You need to identify how many sign-in attempts were tracked for User1, and how User1 can unlock her account before the 300-second lockout duration expires.

What should identify? To answer, select the appropriate

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Tracked sign-in attempts:

|    |   |
|----|---|
|    | ▼ |
| 4  |   |
| 5  |   |
| 10 |   |
| 11 |   |

Unlock by:

|                                                 |   |
|-------------------------------------------------|---|
|                                                 | ▼ |
| Clearing the browser cache                      |   |
| Signing in by using inPrivate browsing mode     |   |
| Performing a self-service password reset (SSPR) |   |

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>

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 16 times

  **Fijii** 4 months ago

Thank you for the article I was not aware of that ! However I think the keyword here is "attempts", in the end there may only be 5 times that it really counted but I think EVERY attempt is logged



upvoted 1 times

  **Hot\_156**  1 year, 8 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

  **YesPlease**  4 months, 1 week ago

Tracked sign-in attempts: 11

Unlock by: Performing a self-service password reset (SSPR)

For audit and security purposes, Azure logs ALL sign-in attempts. Smart-Lockout only tracks different wrong passwords for its own logic( 5 in this case), but the question is specifically asking about how many login attempts were tracked and every attempt to login is logged.

upvoted 1 times

  **Nyamnyam** 7 months, 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 5 times

  **armid** 4 months, 2 weeks ago

i am thinking smart lockout tracks password hashes, not sign-in attempts. So I am going to answer 11, as they are asking "sign-in attempts were tracked". And since they state she was locked out with a 300 value which is not default, I am going to assume someone modified their default settings, allowing the lockout to happen even though it shouldnt have had the samrt lockout feature been on.

upvoted 1 times

  **Nivos23** 7 months, 4 weeks 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** 8 months ago

11

SSRP

upvoted 2 times

  **JCKD4Ni3L** 8 months 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** 8 months 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 2 times

☐  **EmnCours** 10 months, 2 weeks ago

11

SSPR

upvoted 3 times

☐  **dule27** 12 months ago

11

SSPR

upvoted 2 times

☐  **Holii** 1 year 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** 1 year, 3 months 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** 1 year, 5 months 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** 1 year, 5 months ago

Good answer should be:

Tracked sign-in: 4

Unlock by: SSPR

Why 4?

"Smart lockout tracks the last three bad password hashes to avoid incrementing the lockout counter for the same password."

==> The last pwd was already provided. And then it's not five. Check the 3 last pwd

upvoted 1 times

☐  **BRoald** 1 year, 5 months ago

Your answer is wrong with the tracked sign ins:

I tested this in my tenant with User1 & User2;

I tried to login with all the passwords in the order that's described in the question.

Then i went to Portal.azure > AAD > Users > User 1 & User 2 > Sign-In Logs:

I got on both users 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, 6 months 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, 6 months ago

The given answer is correct.

upvoted 2 times

  **Jhill777** 1 year, 7 months 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, 7 months 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, 7 months 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** 1 year 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 2 times

## 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](#)

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users. [Learn more](#)

Name \*

Policy1 ✓

## Assignments

Users and groups ⓘ &gt;

Specific users included

Cloud apps or actions ⓘ &gt;

All cloud apps

Conditions ⓘ &gt;

0 conditions selected

## Access controls

Grant ⓘ &gt;

0 controls selected

Session ⓘ &gt;

0 controls selected

Include

Exclude

☐ None☐ All users☒ Select users and groups☐ All guest users (preview) ⓘ☐ Directory roles (preview) ⓘ☒ Users and groups

Select ⓘ &gt;

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



### 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 |

### Suggested Answer:

To ensure that User1 is prompted for authentication every eight hours, you must configure the **[answer choice]**.

|                          |
|--------------------------|
| Conditions settings      |
| Enable policy setting    |
| Grant settings           |
| Sessions settings        |
| Users and groups setting |

### Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa>

 **melatocaroca** Highly Voted 3 years, 11 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, 10 months ago


Hi friend, do you have exam dump for sc-300 ?

upvoted 2 times

 **jimmyjose** 1 year, 9 months ago

Hahahahahaha

upvoted 2 times

 **sergioandreslq** 2 years, 12 months ago


Perfect answer and very well explained.

upvoted 2 times

 **MajorUrs** Highly Voted 4 years, 1 month ago

Correct

upvoted 7 times

 **EmnCours** Most Recent 1 year, 11 months ago

Correct

upvoted 2 times

 **dule27** 2 years ago

Prompted for MFA: Grant settings


Prompted for authentication every 8 hours: Session settings

upvoted 4 times

 **[Removed]** 2 years, 6 months ago

Answer given is correct.

upvoted 1 times

 **Imee** 2 years, 9 months ago

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

upvoted 3 times

🗨️ 👤 **Nail** 8 months, 1 week ago

Did you get 100%? Cuz that's the only way it matters ;)

upvoted 1 times

🗨️ 👤 **Xyz\_40** 3 years, 1 month ago

Correct. This can easily be done in your Azure tenant

upvoted 1 times

🗨️ 👤 **Jun143** 3 years, 3 months ago

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

upvoted 2 times

🗨️ 👤 **Nhurexjayyy** 3 years, 6 months ago

Correct.... <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime>

upvoted 2 times

You have an Azure Active Directory (Azure AD) tenant that contains a user named SecAdmin1. SecAdmin1 is assigned the Security administrator role.

SecAdmin1 reports that she cannot reset passwords from the Azure AD Identity Protection portal.

You need to ensure that SecAdmin1 can manage passwords and invalidate sessions on behalf of non-administrative users. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

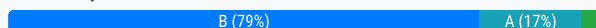
- A. Authentication administrator
- B. Helpdesk administrator
- C. Privileged authentication administrator
- D. Security operator

**Suggested Answer: C**

Reference:

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

Community vote distribution



**sezza\_blunt** Highly Voted 4 years 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** 1 year, 2 months ago

The Helpdesk admin does NO invalidate sessions capability.  
upvoted 1 times

**[Removed]** 3 years, 4 months ago

I think it's B too. Helpdesk Administrator seems to be the correct answer.  
upvoted 4 times

**Domza** 4 years ago

There you go - Help Desk Admin - "Users with this role can change passwords, invalidate refresh tokens"  
upvoted 5 times

**Jhill777** 2 years, 7 months ago

Authentication Administrator Role Permissions includes:  
microsoft.directory/users/invalidateAllRefreshTokens  
Force sign-out by invalidating user refresh tokens.  
upvoted 7 times

**rozgonyi** Highly Voted 4 years, 1 month 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 66 times

  **Acbrownit** 3 years, 2 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, 8 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 invalidated them ( invalidated refresh token)

upvoted 26 times

  **Holii** 2 years 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

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

Selected Answer: B

both helpdesk administrator and authentication administrator can do similar tasks asked here. the least privileged is helpdesk administrator as the authentication administrator can also modify authentication related settings which is what a helpdesk administrator cannot do

upvoted 1 times

  **Sunth65** 6 months ago

Selected Answer: A

A.

Authentication administrator is the correct answer.

Authentication Administrator can only reset non admin accounts password

upvoted 1 times

  **Nail** 8 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** 1 year, 2 months ago

Selected Answer: B

Help Desk Admin - "Users with this role can change passwords, invalidate refresh tokens"

upvoted 1 times

  **NICKTON81** 1 year, 2 months 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** 1 year, 4 months 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, 6 months 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, 7 months 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, 7 months 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, 7 months 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, 7 months 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, 8 months ago

**Selected Answer: B**

I think it's B

upvoted 2 times

🗨️ 👤 **sherifhamed** 1 year, 9 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, 12 months ago

**Selected Answer: A**

A. Authentication administrator

upvoted 1 times

🗨️ 👤 **Sango** 1 year, 12 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** 2 years ago

**Selected Answer: B**

Answered correctly in similar question.

upvoted 2 times

You configure Azure Active Directory (Azure AD) Password Protection as shown in the exhibit. (Click the Exhibit tab.)

### Custom smart lockout

Lockout threshold ⓘ  ✓

Lockout duration in seconds ⓘ  ✓

### 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?

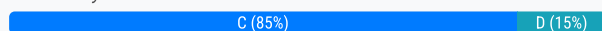
- A. Pr0jectlitw@re and T@ilw1nd only
- B. C0nt0s0 only
- C. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd
- D. C0nt0s0 and T@ilw1nd only
- E. C0nt0s0 and Pr0jectlitw@re only

**Suggested Answer: C**

Reference:

<https://blog.enablingtechcorp.com/azure-ad-password-protection-password-evaluation>

Community vote distribution



arghhh Highly Voted 3 years, 1 month ago

Test on tenant, all three are blocked.

Answer is C

upvoted 38 times

Goseu Highly Voted 3 years, 1 month 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** 1 year 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** 1 year ago

To add; this is definitely C. Not to misguide anyone with my curiosity lol.

upvoted 2 times

  **Holii** 1 year ago

After theoretical testing, I tried the following:

Tailw%nd! - Password Accepted

Tailw!nd! - 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

"Tailw!nd!" = "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**  7 months ago

**Selected Answer: C**

Answer is C

upvoted 1 times

  **dule27** 12 months ago

**Selected Answer: C**

C. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd

upvoted 1 times



🗳️ 👤 **Aquintero** 1 year, 5 months ago

**Selected Answer: C**

C. C0nt0s0, Pr0jectlitw@re y T@ilw1nd  
upvoted 1 times

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

**Selected Answer: C**

All passwords will be blocked.  
upvoted 1 times

🗳️ 👤 **Jhill777** 1 year, 7 months 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, 7 months ago

Correct answer C. I tested all 3 in my lab and they were all blocked. The first 2 are blocked based on policy but the last one is only 7 characters so it didn't meet the password minimum characters of 8.  
upvoted 1 times

🗳️ 👤 **kerimnl** 1 year, 7 months ago

**Selected Answer: C**

Correct Answer is C  
upvoted 1 times

🗳️ 👤 **gunjant25** 1 year, 9 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, 10 months ago

**Selected Answer: D**

Tested  
upvoted 2 times

🗳️ 👤 **Tokiki** 2 years ago

yes. it need 5 pts.  
upvoted 2 times

🗳️ 👤 **Nilz76** 2 years, 2 months ago

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

🗳️ 👤 **Nilz76** 2 years, 2 months ago

**Selected Answer: C**

Tested in my tenant, Answer is C  
upvoted 1 times

🗳️ 👤 **Yelad** 2 years, 3 months ago

On the exam - March 28, 2022  
upvoted 1 times

🗳️ 👤 **Jun143** 2 years, 3 months ago

just pass the exam today. This came in the question.  
upvoted 1 times

🗳️ 👤 **stromnessian** 2 years, 3 months ago

**Selected Answer: C**

The answer is C. Can't understand why people can't just use "password" as it's much easier to remember.  
upvoted 5 times

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a verification code from the Microsoft Authenticator app
- B. security questions
- C. voice
- D. SMS

**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:

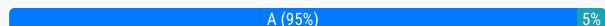
B: Security questions are not used as an authentication method but can be used during the self-service password reset (SSPR) process.

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



**bobicos** Highly Voted 3 years, 8 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, 6 months ago

The default behaviour of the Authenticator app is to send a notification to your phone, which does require mobile connectivity. However, the user can choose "Sign in another way" and then "Use a verification code from my mobile app" - this method does not require mobile connectivity. So yes, the correct answer is A "a verification code from the Microsoft Authenticator app" upvoted 18 times

**melatocaroca** 3 years, 5 months ago

WRONG do not have Wi-Fi access or mobile phone connectivity. upvoted 2 times

**Acbrownit** 2 years, 8 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, 11 months ago

no it is correct. TOTP also works offline. upvoted 3 times

**J4U** 3 years, 2 months ago

Yes, it Authenticator app don't need phone connectivity.


<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, 6 months ago

Thanks for the link. This is correct, it specifically says that no data connection is needed under the heading "Verification codes when connected".

upvoted 1 times

  **lime568** 2 years, 9 months ago

but need internet. no Wifi no mobile phone

upvoted 1 times

  **tinhd** 1 year, 3 months ago


All OTP apps or FIDO2 don't need internet connection to work.

upvoted 1 times

  **Benkyoujin** 2 years, 7 months ago



Incorrect and you can test this.

upvoted 1 times

  **Cheif** 3 years, 7 months ago



But they don't have mobile phones? how will they access the mobile authenticator app?

upvoted 1 times

  **tinhd** 1 year, 3 months 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, 7 months ago

but they do :) All users have mobile phones and laptops.

upvoted 4 times

  **Cheif** 3 years, 7 months ago

Scratch that A is the correct answer, doesn't need internet IMO

upvoted 7 times

  **Ed2learn** 3 years, 6 months ago



doesn't need internet but the question states "no connectivity" which to me means no signal to receive. Not sure the right answer is here.

upvoted 2 times

  **Ed2learn** 1 year, 2 months 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** 9 months, 1 week ago

hahaha

upvoted 1 times

  **melatocaroca** 3 years, 5 months ago

WRONG do not have Wi-Fi access or mobile phone connectivity.

upvoted 1 times

  **leeuw86**  3 years, 6 months ago

Had this question in exam today. Option C) voice was replaced by Windows Hello for Business.

Also Option a) was notification from Authenticator App

upvoted 18 times

  **Ed2learn** 3 years, 6 months ago


Windows Hello solves the mobile phone connectivity issue. The biometric info is stored on the local machine so this will work. It doesn't require internet or mobile connectivity. Looks like Microsoft corrected the answer choices.

upvoted 4 times

  **sezza\_blunt** 3 years, 6 months ago

That changes it a bit. The notification requires mobile connectivity. Did you choose WHFB as the correct answer?

upvoted 2 times

  **easypeacy**  1 year, 3 months ago

maybe they are considering that you set the laptop as hotspot for your mobile and then use auth app ....

upvoted 1 times

🗨️ 👤 **EmnCours** 1 year, 5 months ago

**Selected Answer: A**

Correct Answer: A  
upvoted 1 times

🗨️ 👤 **dule27** 1 year, 5 months ago

**Selected Answer: A**

A. a verification code from the Microsoft Authenticator app  
upvoted 1 times

🗨️ 👤 **LeTrinh** 1 year, 10 months ago

<https://drake.teamdynamix.com/TDClient/2025/Portal/KB/ArticleDet?ID=50929>  
upvoted 2 times

🗨️ 👤 **[Removed]** 2 years ago

**Selected Answer: A**

Correct answer.  
upvoted 2 times

🗨️ 👤 **PadyLoki** 2 years, 5 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** 2 years, 5 months ago

A is the correct answer. Authentication app no need Internet. We can change by input One-time Password Code in App auto random in 30s.  
upvoted 1 times

🗨️ 👤 **Tokiki** 2 years, 6 months ago

A is correct  
upvoted 1 times

🗨️ 👤 **sapien45** 2 years, 6 months ago

Verification codes when connected

Q: Do I need to be connected to the Internet or my network to get and use the verification codes?

A: The codes don't require you to be on the Internet or connected to data, so you don't need phone service to sign in. Additionally, because the app stops running as soon as you close it, it won't drain your battery.  
upvoted 1 times

🗨️ 👤 **shine98** 2 years, 6 months ago

On the exam - June 12, 2022  
upvoted 1 times

🗨️ 👤 **YetiSpaghetti** 2 years, 6 months ago

**Selected Answer: A**

A is obviously the answer. Voice needs mobile connectivity. MFA authenticators do not.  
upvoted 1 times

🗨️ 👤 **RandomNickname** 2 years, 6 months 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 0365 is a phone number, irrespective of what type.

This is something I've implemented before.  
upvoted 1 times

🗨️ 👤 **RandomNickname** 2 years, 7 months 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, 7 months ago

you can put your phone into airplane mode and test this A is correct you can still use the code,

upvoted 1 times

🗨️ 👤 **sunilkms** 2 years, 7 months ago

**Selected Answer: A**

the question says it clearly that no wifi access to mobile phone connectivity, hence, voice, and SMS is not an option, hence authenticator app is the correct option.

upvoted 1 times

🗨️ 👤 **Nilz76** 2 years, 8 months ago

This question was in the exam 28/April/2022

upvoted 1 times

## HOTSPOT -

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

| Name  | Role                                    |
|-------|-----------------------------------------|
| User1 | Security administrator                  |
| User2 | Privileged authentication administrator |
| User3 | Service support administrator           |

User2 reports that he can only configure multi-factor authentication (MFA) to use the Microsoft Authenticator app.

You need to ensure that User2 can configure alternate MFA methods.

Which configuration is required, and which user should perform the configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Configuration:

|                                                       |   |
|-------------------------------------------------------|---|
|                                                       | ▼ |
| Enable access reviews.                                |   |
| Enable Azure AD Privileged Identity Management (PIM). |   |
| Modify security defaults.                             |   |

User:

|                      |   |
|----------------------|---|
|                      | ▼ |
| User1 only           |   |
| User2 only           |   |
| User3 only           |   |
| User1 and User2 only |   |
| User1 and User3 only |   |
| User2 and User3 only |   |

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.


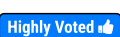
Incorrect:

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**  2 years, 3 months ago


Checked in SC300 MOC book. The answer is correct

upvoted 12 times

 **Cepheid**  2 years 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 10 times

 **BB6919** 1 year, 12 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 3 times



 **kanew** 1 year, 7 months ago

Agree. Security Defaults is the only correct answer I can see. I haven't tested it but it makes sense and here is the statement from MS that I believe supports it. It suggests that the Authenticator App is the only enabled MFA option in Sec Defaults.

"Requiring all users and admins to register for MFA using the Microsoft Authenticator app or any third-party application using OATH TOTP."

<https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-turn-on-mfa?view=o365-worldwide&tabs=secdefaults>


upvoted 3 times

 **9H3zmT6**  2 months ago

The provided answer is correct.

Microsoft Entra admin center > Identity > Overview > Properties > Manage security defaults > Disabled

upvoted 1 times

 **csi\_2025** 4 months ago

If you take "modifying security defaults" as turning them off than it makes a whole lot more sense.

upvoted 1 times

 **JuanZ** 8 months, 1 week ago

Modify security settings  
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** 10 months, 2 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** 1 year, 1 month ago

Security Defaults  
User2  
upvoted 3 times

🗨️ 👤 **SFAY** 11 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

🗨️ 👤 **armid** 4 months, 2 weeks ago

he is unable to do the task bacauce security defaults are on  
upvoted 1 times

🗨️ 👤 **armid** 4 months, 2 weeks ago

and those can be turned off by at least security administrator  
upvoted 1 times

🗨️ 👤 **dule27** 1 year, 6 months ago

Modify security defaults  
User1 only  
upvoted 3 times

🗨️ 👤 **ShoaibPKDXB** 1 year, 7 months ago

Correct  
upvoted 1 times

🗨️ 👤 **BB6919** 1 year, 12 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** 2 years 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]** 2 years ago

Agree with DeepMoon. Security Defaults cannot be modified, it must be PIM. 2nd answer is correct.  
upvoted 3 times

🗨️ 👤 **ooltie** 2 years, 1 month ago

Correct. Security Defaults requires "Require all users to register for Azure AD Multi-Factor Authentication"

Users have 14 days to register for Azure AD Multi-Factor Authentication by using the Microsoft Authenticator app or any app supporting OATH TOTP.

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults#require-all-users-to-register-for-azure-ad-multi-factor-authentication>  
upvoted 3 times

🗨️ 👤 **DeepMoon** 2 years, 3 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

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%)

🗳️ 👤 **9H3zmT6** 2 months ago

**Selected Answer: C**

When administrators require one method be used to reset a password, verification code is the only option available.

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#mobile-app-and-sspr>

upvoted 1 times

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

When administrators require one method be used to reset a password, verification code is the only option available

upvoted 2 times

🗳️ 👤 **sherifhamed** 1 year, 3 months 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** 1 year, 5 months ago

**Selected Answer: C**

Correct Answer: C

upvoted 1 times

  **dule27** 1 year, 6 months ago

**Selected Answer: C**

C. a mobile app code


upvoted 1 times

  **ShoaibPKDXB** 1 year, 7 months ago

**Selected Answer: C**

C is correct



upvoted 1 times

  **jojoseph** 1 year, 11 months ago

**Selected Answer: C**

definitely C

upvoted 1 times

  **Boogs** 2 years, 3 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** 2 years, 3 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, 11 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

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'.

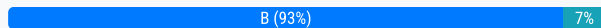
Notes: Currently, the 'Confirm user compromised' option is only available in 'Risky users' report.

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



**Buzz8** Highly Voted 1 year, 7 months 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 login. Less effort than reconfiguring a user risk policy.

upvoted 9 times

**Sunth65** Most Recent 6 months 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 2 times

**dule27** 1 year ago

**Selected Answer: B**

B. Mark User1 as compromised



upvoted 2 times

**ShoaibPKDXB** 1 year, 1 month ago

**Selected Answer: B**

B is correct

upvoted 2 times

  **kanew** 1 year, 1 month ago

**Selected Answer: B**

Correct and less effort than A which will impact all users

upvoted 2 times

  **Aquintero** 1 year, 5 months ago

**Selected Answer: B**

Teniendo en cuenta que hay que minimizar los esfuerzos administrativos la respuesta es: B. Marcar Usuario1 como comprometido.

upvoted 2 times

  **Cepheid** 1 year, 6 months 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, 6 months ago

**Selected Answer: B**

Given answer is correct.

upvoted 2 times

  **kerimnl** 1 year, 7 months ago

**Selected Answer: A**

I think the correct answer is A.

upvoted 2 times

## HOTSPOT -

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

| Name  | Member of      | Multi-factor authentication (MFA) |
|-------|----------------|-----------------------------------|
| User1 | Group1         | Enabled but never used            |
| User2 | Group2         | Disabled                          |
| User3 | Group1, Group2 | Enforced and used                 |

In Azure AD Identity Protection, you configure a user risk policy that has the following settings:

⇒ Assignments:

- Users: Group1

- User risk: Low and above

⇒ Controls:

- Access: Block access

⇒ Enforce policy: On

In Azure AD Identity Protection, you configure a sign-in risk policy that has the following settings:

⇒ Assignments:

- Users: Group2

- Sign-in risk: Low and above

⇒ Controls:

- Access: Require multi-factor authentication

⇒ Enforce policy: On

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

NOTE: Each correct selection is worth one point.

Hot Area:

| Statements                                      | Yes                   | No                    |
|-------------------------------------------------|-----------------------|-----------------------|
| User1 can sign in from an anonymous IP address. | <input type="radio"/> | <input type="radio"/> |
| User2 can sign in from an anonymous IP address. | <input type="radio"/> | <input type="radio"/> |
| User3 can sign in from an anonymous IP address. | <input type="radio"/> | <input type="radio"/> |

Suggested Answer:

| Statements                                      | Yes                              | No                               |
|-------------------------------------------------|----------------------------------|----------------------------------|
| User1 can sign in from an anonymous IP address. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 can sign in from an anonymous IP address. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User3 can sign in from an anonymous IP address. | <input type="radio"/>            | <input checked="" type="radio"/> |

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, 10 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 66 times

🗲️ 👤 **existingname** 2 years, 10 months ago

On the exam today, I answered Yes No Yes

upvoted 11 times

🗲️ 👤 **kanew** 2 years, 1 month ago

Perfectly explained - I agree it's Y,N,Y

upvoted 6 times

🗲️ 👤 **mcas** 2 years, 6 months 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, 6 months 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** 2 years, 4 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** 2 years 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, 9 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

🗲️ 👤 **Obyte** Highly Voted 2 years, 8 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 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

🗲️ 👤 **d1e85d9** Most Recent 3 months, 2 weeks ago

YES

NO

YES

upvoted 1 times

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

Anonymous IP applies to "Sign-in Risk Policy" ONLY

Yes - User1 is not a member of Group2, so they are not affected by Group2 Sign-in Policy and can sign in

No - User2 is a member of Group2 and does not have MFA enabled, so they are blocked from sign-in

Yes - User3 is a member of Group2 and has MFA, so they can login

upvoted 1 times

🗨️ 👤 **enklaui** 8 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 anonymous ips

upvoted 1 times

🗨️ 👤 **emartiy** 1 year, 3 months 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 sign-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 sign-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** 1 year, 5 months 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 never know what MS is after so it is always a gamble.. It is not like you can defend your answer.

upvoted 2 times

🗨️ 👤 **MatExam** 1 year, 5 months 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, 8 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, 10 months ago

Yes

No

Yes

upvoted 2 times



🗨️ 👤 **dule27** 2 years ago

Yes

No

Yes

upvoted 2 times

🗨️ 👤 **TomasValtor** 2 years 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** 2 years, 5 months ago

para mi la respuesta correcta es Yes, No, Yes

upvoted 1 times

🗨️ 👤 **jojoseph** 2 years, 5 months ago

Yes No Yes

upvoted 1 times

🗨️ 👤 **jack987** 2 years, 6 months ago

The correct answer is Yes - No - No

I agree with zokaniedereenheth:

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, 6 months 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

🗨️ 👤 **zokaniedereenheth** 2 years, 6 months 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, 6 months 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, 6 months 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, 6 months ago

Given answer is correct!

upvoted 1 times

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

You configure self-service password reset (SSPR) by using the following settings:

- ⇒ Require users to register when signing in: Yes
- ⇒ Number of methods required to reset: 1

What is a valid authentication method available to users?

- A. an email to an address outside your organization
- B. a smartcard
- C. an FIDO2 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 2 years 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 7 times

🗳️ 👤 **HartMS** Most Recent 9 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, 5 months ago

**Selected Answer: A**

A. an email to an address outside your organization

upvoted 2 times

🗳️ 👤 **ShoaibPKDXB** 1 year, 7 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

🗳️ 👤 **Jawad1462** 2 years, 1 month ago

**Selected Answer: A**

Is the correct answer

upvoted 1 times

🗳️ 👤 **TheMCT** 2 years, 2 months ago

The given answer is correct!

upvoted 1 times

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

| Name  | Member of |
|-------|-----------|
| User1 | Group1    |
| User2 | Group2    |
| User3 | Group3    |

The tenant has the authentication methods shown in the following table.

| Method                      | Target | Enabled |
|-----------------------------|--------|---------|
| FIDO2                       | Group2 | Yes     |
| Microsoft Authenticator app | Group1 | Yes     |
| SMS                         | Group3 | Yes     |

Which users will sign in to cloud apps by matching a number shown in the app with a number shown on their phone?

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

**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** 11 months, 1 week ago



Imo it should also be the sms categorie, right? Like; they also read something in numeric form from their mobiledevice lol.  
upvoted 1 times

  **Nail** 8 months, 1 week ago

That wouldn't be "matching" though.  
upvoted 2 times

  **9H3zmT6** 2 months ago

This question likely tests knowledge of the Microsoft Authenticator app but uses ambiguous wording to confuse. Since SMS also delivers a 6-digit code matched with the cloud app, SMS could also be a valid answer.  
upvoted 1 times

  **emartiy** 1 year, 3 months 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** 1 year, 3 months ago

For 3 options, only Microsoft Authenticaiton app provide code (it also works offline).

Answer is User1 Only

upvoted 2 times

🗳️ 👤 **EmnCours** 1 year, 11 months ago

**Selected Answer: A**

Answer is A

upvoted 2 times

🗳️ 👤 **dule27** 2 years ago

**Selected Answer: A**

A. User1 only (MA App)

upvoted 2 times

🗳️ 👤 **jojoseph** 2 years, 5 months ago

**Selected Answer: A**

A is right

upvoted 1 times

🗳️ 👤 **zokaniedereenheth** 2 years, 6 months ago

SMS is a preview feature, might also work?!

upvoted 1 times

🗳️ 👤 **ZauberSRS** 2 years, 6 months 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, 7 months 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, 8 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** 2 years, 1 month 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, 9 months ago

The answer makes sense it is the only possible answer. But the question doesn't make sense.

upvoted 4 times

🗳️ 👤 **[Removed]** 2 years, 2 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]** 2 years, 2 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, 9 months ago

I find this question a bit confusing.

Well Authenticator app is on the phone. It may have OATH code that you enter into a webpage.

what is this?

"Which users will sign in to cloud apps by matching a number shown in the app with a number shown on their phone?"

Can someone make sense of this?

upvoted 1 times

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

| Name      | Status      | Conditional access requirement           |
|-----------|-------------|------------------------------------------|
| CAPolicy1 | On          | Users connect from a trusted IP address. |
| CAPolicy2 | On          | Users' devices are marked as compliant.  |
| CAPolicy3 | Report-only | The sign-in risk of users is low.        |

You need to evaluate which policies will be applied to User1 when User1 attempts to sign-in from various IP addresses.

Which feature should you use?

- A. Access reviews
- B. Identity Secure Score
- C. The What If tool
- D. the Microsoft 365 network connectivity test tool

**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, 9 months ago

Correct.

upvoted 6 times

 **shoutiv** Highly Voted 1 year, 6 months 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 11 months, 2 weeks ago

**Selected Answer: C**

Correct Answer: C

upvoted 2 times

 **dule27** 1 year ago

**Selected Answer: C**

C. The What If tool

upvoted 1 times

 **ShoaibPKDXB** 1 year, 1 month ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **Aquintero** 1 year, 5 months ago

**Selected Answer: C**

de acuerdo la respuesta es: C. La herramienta What If  
upvoted 1 times



You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. an app password
- B. voice
- C. Windows Hello for Business
- D. security questions

**Suggested Answer: A**

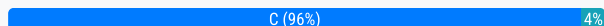
The Microsoft Authenticator app provides an additional level of security to your Azure AD work or school account or your Microsoft account and is available for

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



**birrach** Highly Voted 2 years, 9 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, 10 months ago

**Selected Answer: C**

C should be the answer.  
upvoted 9 times

**Panama469** Most Recent 11 months, 3 weeks ago

Exam has 311 questions... well minus 50 for the number of times this question pops up!  
upvoted 2 times

**emartiy** 1 year, 3 months 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** 1 year, 5 months 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, 7 months ago

Selected Answer: C

Windows Hello for Business is the correct answer.

upvoted 1 times

🗳️ 👤 **BenLam** 1 year, 8 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, 8 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, 11 months ago

Selected Answer: C

C is correct

upvoted 1 times

🗳️ 👤 **dule27** 2 years ago

Selected Answer: C

C. Windows Hello for Business

upvoted 1 times

🗳️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

🗳️ 👤 **kanew** 2 years, 1 month ago

Selected Answer: C

C is the correct answer. A is legacy authentication and would bypass MFA

upvoted 1 times

🗳️ 👤 **Aquintero** 2 years, 5 months ago

Selected Answer: C

Windows Hello

upvoted 2 times

🗳️ 👤 **chrisp1992** 2 years, 6 months ago

Selected Answer: C

App Passwords are legacy

upvoted 4 times

🗳️ 👤 **[Removed]** 2 years, 6 months ago

Selected Answer: C

Windows Hello for Business is the correct answer.

upvoted 4 times

🗳️ 👤 **samir45** 2 years, 9 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, 8 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, 9 months ago

**Selected Answer: C**

C is the answer

upvoted 5 times

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*



 **9H3zmT6** 2 months ago

**Selected Answer: A**

This functionality allows services like Microsoft Graph, Microsoft Entra ID, SharePoint Online, and Exchange Online to see the actual source IP address.

<https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-source-ip-restoration#enable-global-secure-access-signaling-for-conditional-access>

upvoted 1 times

You create a conditional access policy that blocks access when a user triggers a high-severity sign-in alert.

You need to test the policy under the following conditions:

- ⇒ A user signs in from another country.
- ⇒ A user triggers a sign-in risk.

What should you use to complete the test?

- A. the Conditional Access What If tool
- B. sign-ins logs in Azure Active Directory (Azure AD)
- C. the activity logs in Microsoft Defender for Cloud Apps
- D. access reviews in Azure Active Directory (Azure AD)

**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** 9 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 4 times

🗳️ 👤 **EmnCours** 11 months, 2 weeks ago

**Selected Answer: A**

Correct Answer: A

upvoted 1 times

🗳️ 👤 **dule27** 1 year ago

**Selected Answer: A**

A. the Conditional Access What If tool

upvoted 1 times

🗳️ 👤 **kmk\_01** 1 year, 2 months ago

**Selected Answer: A**

Agreed

upvoted 1 times

🗳️ 👤 **Aquintero** 1 year, 5 months ago

**Selected Answer: A**

A. la herramienta What If de acceso condicional

upvoted 1 times

🗨️ 👤 **BRoald** 1 year, 5 months ago

**Selected Answer: A**

So easy it feels like a trick  
upvoted 2 times

🗨️ 👤 **shoutiv** 1 year, 6 months 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, 6 months ago

**Selected Answer: A**

Given answer is correct.

upvoted 1 times

## HOTSPOT -

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

| Name  | Member of | Multi-factor authentication (MFA) |
|-------|-----------|-----------------------------------|
| User1 | Group1    | Disabled                          |
| User2 | Group2    | Enforced                          |

You have the locations shown in the following table.

| Name      | Private address space | Public NAT address space |
|-----------|-----------------------|--------------------------|
| Location1 | 10.10.0.0/16          | 20.93.15.0/24            |
| Location2 | 192.168.0.0/16        | 193.17.17.0/24           |

The tenant contains a named location that has the following configurations:

- ⇒ Name: Location1
- ⇒ Mark as trusted location: Enabled

IPv4 range: 10.10.0.0/16 -

MFA has a trusted IP address range of 193.17.17.0/24.

- ⇒ Name: CAPolicy1
- ⇒ Assignments
  - Users or workload identities: Group1
  - Cloud apps or actions: All cloud apps
- ⇒ Conditions
  - Locations: All trusted locations
- ⇒ Access controls
- Grant
  - Grant access: Require multi-factor authentication
  - Session: 0 controls selected
- ⇒ Enable policy: On

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

NOTE: Each correct selection is worth one point.

Hot Area:

| Statements                                                                                       | Yes                   | No                    |
|--------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.  | <input type="radio"/> | <input type="radio"/> |
| If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.  | <input type="radio"/> | <input type="radio"/> |
| If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA. | <input type="radio"/> | <input type="radio"/> |

## 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.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA. | <input checked="" type="radio"/> | <input type="radio"/>            |

Box 1: No -

10.10.0.150 is from a trusted location.

Note: The trusted IPs feature of Azure AD Multi-Factor Authentication bypasses multi-factor authentication prompts for users who sign in from a defined IP address range. You can set trusted IP ranges for your on-premises environments. When users are in one of these locations, there's no Azure AD Multi-Factor

Authentication prompt. The trusted IPs feature requires Azure AD Premium P1 edition.

Box 2: No -

10.10.1.160 is from a trusted location

Box 3: Yes -

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

  **dejo**  2 years, 9 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** 2 years, 2 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** 8 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** 1 year, 4 months ago


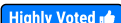
fmm.. so then the answer should be N Y Y if user2 must be authenticated cause of enforce setting.

upvoted 1 times

  **Nail** 8 months, 1 week ago

No, because in the last case User2 is coming from a trusted IP range. NYN.

upvoted 2 times

  **hyc1983**  2 years, 7 months 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 21 times

  **MrPrasox** 2 years, 7 months ago

Fully agree with NYN answers and with posted explanation.

upvoted 1 times

  **mibur** 2 years, 6 months ago

Last one is Y so NYY. a MFA Enforced users is prompted for MFA even when logging in from a whitelisted/trusted location.

upvoted 4 times

  **wooyourdaddy** 2 years, 5 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** 2 years, 1 month 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** 2 years, 1 month 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, 8 months ago

I agree with you

no

yes

no

upvoted 2 times

  **b233f0a** 2 years 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

  **d1e85d9** Most Recent 3 months, 2 weeks ago

NO

YES

NO

upvoted 1 times

  **anonymousarpanch** 4 months, 2 weeks ago

1. it wont prompt for MFA. actually the question here is missing a key input which is 'Locations - Trusted locations' should be in exclude state and not include. who keeps trusted location with MFA. hence user 1 coming from trusted location dont need MFA

2. Yes - User 2 is not part of Group 1 so CA policy does not apply and secondly its MFA state says enforced, which means he is obliged to go via MFA.

3. Yes - still the same. User2 is obliged to go via MFA as he is in enforced state. Sorry, i couldnt see any trusted microsoft links that state that CA policy dominates per-user MFA. if anyone could find pl. share. And I cannot trust chatgpt, copilot or any GenAI model to provide correct answers. pl. understand they only tell what is taught them with enough conviction. so only trusted links if anyone can share..

upvoted 1 times

  **csi\_2025** 4 months ago

1. Should be doesn't mean it is.

upvoted 1 times

  **armid** 4 months, 2 weeks ago

I think its

1. YES - the first table refers to legacy per user authentication and that is not being evaluated when conditional access is used. User 1 is signing in from trusted location, but the policy still states grant access but require MFA

2. YES - conditional access does not apply to this user because the scope of the policy is group1 only. Therefore his legacy per user MFA will kick in and that requires him to use MFA unless he is not logging in from the legacy MFA trusted IP of 193.17.17.0/24 which in this case he is not

3. NO - this time around he is signing in from the per user MFA trusted IP of 193.17.17.0/24

Don't let the private ranges fool you. MS will only evaluate the public IPs, you only need to verify the corresponding private addresses match to the public ones.

upvoted 1 times

  **RemmyT** 1 year 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** 1 year, 1 month 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 2 times

🗨️ 👤 **emartiy** 1 year, 3 months 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 from any IP range user2 will be prompted MFA.

3) YES - Same above option 2.

NO - YES - YES.

upvoted 1 times

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

🗨️ 👤 **Shuihe** 1 year, 4 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, 7 months 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, 9 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

  **Hawkix** 2 years 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, 9 months ago



User1 MFA is disabled, so user1 can't be prompted isn't it?

upvoted 1 times

  **ivzdf** 1 year, 11 months ago

Completely agree

upvoted 1 times

  **ivzdf** 1 year, 11 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** 2 years, 1 month 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** 2 years, 1 month 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** 2 years, 2 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** 2 years, 1 month 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** 2 years 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** 2 years 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** 2 years, 2 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** 2 years, 2 months ago

Sorry, it is No Yes NO (made a mistake on the 3rd one)

upvoted 1 times

  **iwantmyexamsobad** 2 years, 2 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 therefor 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

## 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** 9 months 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** 1 year, 2 months ago

Correct, and was on exam today.

upvoted 4 times

🗨️ 👤 **mfarhat1994** 1 year, 2 months ago

how was the exam and were these questions in the exam ?

upvoted 2 times

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

Users:Guest 3 Only

Valid: 30 minutes

upvoted 3 times

🗨️ 👤 **EmnCours** 1 year, 5 months 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, 6 months ago

Users:Guest 3 Only

Valid: 30 minutes

upvoted 4 times

🗨️ 👤 **Pedro2021** 1 year, 12 months ago

Guest 3 and 30 minutes

upvoted 3 times

🗨️ 👤 **[Removed]** 2 years ago

Answers correct.

upvoted 1 times

🗨️ 👤 **kk1** 2 years, 2 months ago



It is correct for 30 min. access

upvoted 1 times

🗨️ 👤 **gwajwara** 2 years, 4 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, 11 months ago

Great link! The given answers are correct in this case

upvoted 2 times

  **existingname** 2 years, 4 months ago

correct, in the exam today

upvoted 4 times



You have a Microsoft 365 tenant.

You currently allow email clients that use Basic authentication to connect to Microsoft Exchange Online.

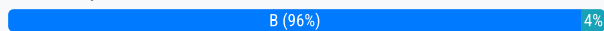
You need to ensure that users can connect to Exchange only from email clients that use Modern authentication protocols.

What should you implement?

- A. an OAuth policy in Microsoft Defender for Cloud Apps
- B. a conditional access policy in Azure Active Directory (Azure AD)
- C. a compliance policy in Microsoft Endpoint Manager
- D. an application control profile in Microsoft Endpoint Manager

**Suggested Answer: D**

Community vote distribution



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

**Selected Answer: B**

B is correct.

upvoted 1 times

**Nyamnyam** 1 year, 1 month 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** 1 year, 3 months 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

**OutLawTheBoyyz** 1 year, 4 months 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** 1 year, 5 months ago

Selected Answer: B

Correct Answer: D

upvoted 2 times

🗳️ 👤 **dule27** 1 year, 6 months ago

Selected Answer: B

B. a conditional access policy in Azure Active Directory (Azure AD)

upvoted 3 times

🗳️ 👤 **Aidanjl** 1 year, 6 months 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, 6 months 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, 6 months ago

B is correct

The easiest way to block legacy authentication across your entire organization is by configuring a Conditional Access policy that applies specifically to legacy authentication clients and blocks access.

upvoted 1 times

🗳️ 👤 **ShoaibPKDXB** 1 year, 7 months ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **sbnpj** 1 year, 8 months ago

Selected Answer: B

Conditional access policy is used for blocking legacy auth.

upvoted 1 times

🗳️ 👤 **Guestie** 1 year, 10 months ago

Selected Answer: B

The question says nothing about what type of device or what the application being used is so setting an App control policy will not do anything. CA policies allow legacy auth to be blocked regardless of device.

upvoted 1 times

🗳️ 👤 **wsrudmen** 1 year, 11 months ago

Selected Answer: B

B also

upvoted 1 times

🗳️ 👤 **Oknip** 1 year, 11 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, 11 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, 11 months ago

Selected Answer: B

as you can block legacy connection to Exchange from CA

upvoted 1 times

🗳️ 👤 **RobbieBoyBlue** 1 year, 11 months ago

B for me

upvoted 1 times

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**  5 months, 4 weeks 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 6 times

 **AcTiVeGrEnAdE** 2 months ago

This is the correct answer

upvoted 2 times

 **Btn26** 5 months, 4 weeks 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 4 times

🗄️ 👤 **AcTiVeGrEnAdE** 2 months ago

Thats just to use GSA which doesnt answer the question. Private access can be joined, hybrid joined or registered which is what the question asks. Answer is E.

upvoted 1 times

🗄️ 👤 **Giuseppe\_Geraci** Most Recent 1 month, 1 week ago

**Selected Answer: B**

Microsoft Entra Private Access (formerly part of Global Secure Access in Microsoft Entra) is a Zero Trust Network Access (ZTNA) solution that allows secure access to private resources (e.g., internal apps).

To use Microsoft Entra Private Access, devices must meet the following requirement:

Be Microsoft Entra joined (not just registered).

upvoted 1 times

🗄️ 👤 **9H3zmT6** 2 months ago

**Selected Answer: C**

The requirements vary depending on the platform OS.

For WINDOWS, the device must be either Microsoft Entra joined or Microsoft Entra hybrid joined.

<https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-install-windows-client>

For ANDROID, the device must be Microsoft Entra registered.

<https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-install-android-client?tabs=device-administrator>

upvoted 4 times

🗄️ 👤 **AcTiVeGrEnAdE** 2 months ago

**Selected Answer: B**

B is the answer. Per the prerequisites defined in the MS docs:

A managed device joined to the onboarded tenant. The device must be either Microsoft Entra joined or Microsoft Entra hybrid joined. Microsoft Entra registered devices aren't supported.

upvoted 1 times

🗄️ 👤 **AcTiVeGrEnAdE** 2 months ago

Actually I stand corrected, the answer is actually E. The question throws you for a loop with talking about deploying GSA. Regardless of GSA, registered and joined devices can both use Private Access.

upvoted 1 times

🗄️ 👤 **c8754bf** 5 months, 2 weeks ago

**Selected Answer: B**

only join

<https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-install-windows-client>

upvoted 2 times

🗄️ 👤 **AcTiVeGrEnAdE** 2 months ago

Thats just to use GSA which doesnt answer the question. Private access can be joined, hybrid joined or registered which is what the question asks. Answer is E.

upvoted 1 times

🗄️ 👤 **anonymousarpanch** 5 months, 2 weeks ago

**Selected Answer: B**

answer is B. check this link... <https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-install-windows-client>.

For GSA you need Microsoft Entra joined or MS entra hybrid JOINED devices. Microsoft entra registered devices are not supported.

upvoted 2 times

🗄️ 👤 **AcTiVeGrEnAdE** 2 months ago

Thats just to use GSA which doesnt answer the question. Private access can be joined, hybrid joined or registered which is what the question asks. Answer is E.

upvoted 1 times

🗄️ 👤 **barlar** 6 months 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 3 times

  **AcTiVeGrEnAdE** 2 months ago

Thats just to use GSA which doesnt answer the question. Private access can be joined, hybrid joined or registered which is what the question asks. Answer is E.

upvoted 1 times

You have an Azure subscription that contains an Azure SQL database named db1.

You deploy an Azure App Service web app named App1 that provides product information to users that connect to App1 anonymously.

You need to provide App1 with access to db1. The solution must meet the following requirements:

- Credentials must only be available to App1.
- Administrative effort must be minimized.

Which type of credentials should you use?

- A. a system-assigned managed identity
- B. an Azure Active Directory (Azure AD) user account
- C. a SQL Server account
- D. a user-assigned managed identity

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ **mali1969** Highly Voted 1 year, 6 months 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 7 times

🗳️ **emartiy** Most Recent 9 months ago

**Selected Answer: A**

A system-assigned managed identity

upvoted 1 times

🗳️ **haazybanj** 1 year, 1 month 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** 1 year, 5 months ago

**Selected Answer: A**

Correct Answer: A

upvoted 1 times

🗳️ **dule27** 1 year, 6 months ago

Selected Answer: A

A. a system-assigned managed identity  
upvoted 1 times

🗨️ 👤 **ShoaibPKDXB** 1 year, 7 months ago

Selected Answer: A

A is correct  
upvoted 1 times

🗨️ 👤 **chikorita** 1 year, 9 months ago

A is correct: system assigned MI  
upvoted 1 times

🗨️ 👤 **Oknip** 1 year, 11 months ago

Selected Answer: A

A is correct  
upvoted 2 times

🗨️ 👤 **Halwagy** 1 year, 11 months ago

Selected Answer: A

Anser is correct  
upvoted 2 times



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 2 years, 1 month ago

I have cleared 3 certifications and can confirm the answer is F  
upvoted 23 times

  **UKG** 1 year, 11 months ago



loooooool  
upvoted 4 times

  **voituredecourse** Highly Voted 1 year, 12 months ago

I have cleared 19 certifications, it is definitely C  
upvoted 12 times

  **AcTiVeGrEnAdE** Most Recent 2 months ago

**Selected Answer: C**  
C is for cookie....  
upvoted 1 times

  **Rackup** 3 months, 3 weeks ago

**Selected Answer: C**  
Role2 is an Azure subscription role, so it can be cloned for the new custom role.  
You can also clone built-in Azure subscription roles (e.g., Reader, Contributor, etc.).  
Hence, the only valid sources to clone when creating Role3 (a custom subscription role) are:

Role2 and any built-in Azure subscription roles.  
upvoted 2 times

  **YesPlease** 4 months ago

**Selected Answer: E**  
Answer E) Role1, Role2, built-in Azure subscription roles, and built-in Azure AD roles

The question is stating that the two listed roles, Role1 and Role2, are custom roles. The key to the question is "clone" from an "existing role"...

So you are able to clone from the two existing custom roles listed as well as from the built-in Azure subscription and built-in Azure AD roles to use as baselines for the new role.

upvoted 1 times

🗨️ **csi\_2025** 4 months ago

Maybe focus on the entirety of the question instead of just the key. The question asks what roles you can clone to create role3 and role3 being an Azure subscription role.

upvoted 1 times

🗨️ **barlar** 6 months ago

**Selected Answer: C**

I have never cleared a certification, but i would still pick C

upvoted 2 times

🗨️ **Panama469** 11 months, 3 weeks ago

C:

All your base are belong to us

upvoted 2 times

🗨️ **emartiy** 1 year, 3 months 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, 6 months ago

**Selected Answer: C**

you can clone Azure subscription roles to make new Azure subscription roles.

upvoted 3 times

🗨️ **kijken** 1 year, 7 months ago

am I the only one thinking that the 2 answers in C are the same?

Maybe I misunderstand the question

upvoted 2 times

🗨️ **Alscoran** 1 year, 7 months 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 6 times

🗨️ **kijken** 1 year, 6 months ago

Thank you for clarifying. Now I understand the question and answer is C :)

upvoted 1 times

🗨️ **haazybanj** 1 year, 7 months ago

I have cleared 29 certifications but can't confirm the answer.

upvoted 3 times

🗨️ **dule27** 2 years ago

**Selected Answer: C**

C. built-in Azure subscription roles and Role2 only

upvoted 5 times

🗨️ **kmk\_01** 2 years, 2 months ago

**Selected Answer: C**

I have passed AZ-104 & AZ-305, I would go for Option C too.

upvoted 5 times

🗨️ **chikorita** 2 years, 3 months ago

i have cleared 2 certifications



i can confirm its C: built-in Azure subscription roles and Role2 only

upvoted 3 times

🗨️ **topzz** 2 years, 2 months ago



thanks for confirming that you cleared 2 certs, otherwise your statement wouldn't have been as valuable.

upvoted 10 times

  **kmk\_01** 2 years, 2 months ago

LOL. I have passed AZ-104 & AZ-305, I would go for Option C too.

upvoted 3 times


  **Zak366** 2 years, 4 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** 2 years, 4 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** 2 years, 5 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

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.

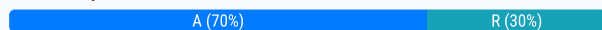
You plan to implement multi-factor authentication (MFA).

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



**Holii** 2 years ago

I swear if I see this question again with the selected answer being "An App Password" im gonna scream  
upvoted 17 times

**cpaljhc4** 1 year, 5 months ago

You sure not an App passcode?  
upvoted 3 times

**rohitrc8521** 1 year, 8 months ago

looooooooooool  
upvoted 2 times

**kevin\_office** 2 years, 5 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** 10 months ago

A for sure  
upvoted 1 times

**Logitech** 1 year, 9 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** 2 years ago

Selected Answer: A

A. Windows Hello for Business

upvoted 1 times

🗨️ 👤 **ShoaibPKDXB** 2 years, 1 month ago

Selected Answer: A

A is correct

upvoted 1 times

🗨️ 👤 **Ignaci0s** 2 years, 3 months ago

Windows 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** 2 years, 3 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** 2 years, 2 months ago

That told Nacho.

upvoted 4 times

🗨️ 👤 **mayleni** 2 years, 4 months ago

Selected Answer: A

WHFB!! Totally

upvoted 1 times

🗨️ 👤 **faeem** 2 years, 5 months ago

Selected Answer: A

Should be A. Windows Hello for business > app password. This question comes up several times and many users indicate that Windows hello for business is what should be the answer.

upvoted 1 times

🗨️ 👤 **Oknip** 2 years, 5 months ago

Windows Hello for Business

upvoted 3 times

🗨️ 👤 **chikorita** 2 years, 3 months ago

R? lol

upvoted 4 times

🗨️ 👤 **ydecac** 2 years, 5 months ago

Selected Answer: A

This question comes up several times and many users indicate Windows hello

upvoted 1 times

🗨️ 👤 **Halwagy** 2 years, 5 months ago

Selected Answer: A

Windows Hello for Business

upvoted 2 times

## HOTSPOT -

Your on-premises network contains an Active Directory domain that uses Microsoft Entra Connect sync to sync with a Microsoft Entra tenant.

You need to configure Microsoft Entra Connect sync to meet the following requirements:

- Microsoft Entra sign-ins must be authenticated by an Active Directory domain controller.
- Active Directory domain users must be able to use Microsoft Entra self-service password reset (SSPR).
- Minimize administrative effort.

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

Correct 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

 **Rackup** 3 months, 3 weeks ago

To require that all sign-ins be validated on-premises by an Active Directory domain controller while allowing self-service password resets to flow back to on-premises AD—and to keep the solution as simple as possible—you would configure:

Authentication by the domain controller:

Pass-through authentication

This validates user credentials directly against the on-premises domain controller without the overhead of setting up and managing AD FS.

SSPR (Self-Service Password Reset):

Password writeback

This ensures that when a user resets their password in the cloud, the new password is written back to the on-premises Active Directory, keeping both directories in sync.

upvoted 1 times

  **YesPlease** 4 months ago

- 1) Passthrough Authentication
- 2) Password writeback

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

<https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr-writeback>

upvoted 1 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. voice
- B. Windows Hello for Business
- C. email
- D. security questions

**Suggested Answer: A**

Community vote distribution

B (100%)

🗳️ 👤 **Holii** Highly Voted 2 years ago

WFHB \*internal screaming\*

upvoted 20 times

🗳️ 👤 **gusherinos** 1 year, 10 months ago

Best answer!

upvoted 2 times

🗳️ 👤 **Nabgre** Highly Voted 2 years, 5 months ago

**Selected Answer: B**

Given response is not correct. The right response is B

upvoted 7 times

🗳️ 👤 **dule27** Most Recent 2 years ago

**Selected Answer: B**

B. Windows Hello for Business

upvoted 1 times

🗳️ 👤 **Selvaraj\_Rajan** 2 years, 2 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** 2 years, 2 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** 2 years, 3 months ago

Windows Hello is just the first step to authenticate a User so the answer should be "voice".

upvoted 2 times

🗨️ 👤 **Ruslan23** 2 years, 3 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** 2 years, 4 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** 9 months, 4 weeks ago

Where did you read about a landline available in this scenario?

upvoted 1 times

🗨️ 👤 **Zak366** 2 years, 4 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** 2 years, 5 months ago

**Selected Answer: B**

Windows Hello for Business

upvoted 3 times

🗨️ 👤 **Oknip** 2 years, 5 months ago

**Selected Answer: B**

Windows Hello for Business

upvoted 2 times

🗨️ 👤 **ydecac** 2 years, 5 months ago

**Selected Answer: B**

mobile phone connectivity = No Voice

upvoted 3 times

🗨️ 👤 **chikorita** 2 years, 3 months ago

upvote maxxxxxxxxxxx

upvoted 1 times

🗨️ 👤 **Halwagy** 2 years, 5 months ago

**Selected Answer: B**

Windows Hello for Business

upvoted 2 times

## HOTSPOT -

You have an Azure subscription named Sub1 that is linked to a Microsoft Entra tenant. The tenant contains the users shown in the following table.

| Name  | Member of |
|-------|-----------|
| User1 | Group1    |
| User2 | Group2    |
| User3 | Group3    |

Sub1 contains a resource group named RG1.

The tenant contains the groups shown in the following table.

| Name   | Role                             | On resource |
|--------|----------------------------------|-------------|
| Group1 | Virtual Machine Local User Login | Sub1        |
| Group2 | Virtual Machine User Login       | RG1         |
| Group3 | Virtual Machine Contributor      | VM1         |

You deploy a virtual machine named VM1 to RG1. VM1 runs Windows Server and has Microsoft Entra login enabled.

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


NOTE: Each correct selection is worth one point.

## Answer Area

| Statements                | Yes                   | No                    |
|---------------------------|-----------------------|-----------------------|
| User1 can sign in to VM1. | <input type="radio"/> | <input type="radio"/> |
| User2 can sign in to VM1. | <input type="radio"/> | <input type="radio"/> |
| User3 can sign in to VM1. | <input type="radio"/> | <input type="radio"/> |

## Correct Answer:

| Statements                | Yes                              | No                    |
|---------------------------|----------------------------------|-----------------------|
| User1 can sign in to VM1. | <input checked="" type="radio"/> | <input type="radio"/> |
| User2 can sign in to VM1. | <input checked="" type="radio"/> | <input type="radio"/> |
| User3 can sign in to VM1. | <input checked="" type="radio"/> | <input type="radio"/> |

 **northgaterebel** Highly Voted 5 months, 1 week ago

YYN.

Virtual Machine Contributor role does not have login privileges. <https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/compute#virtual-machine-contributor>

upvoted 10 times

 **d1e85d9** Most Recent 3 months, 2 weeks ago

YES

YES

NO - contributor cannot login; only can manage.

upvoted 1 times

 **YesPlease** 4 months ago

1) Yes, User1 has rights to all sub-groups of Sub1 as a "Virtual Machine Local User Login". They are able to "log in to a virtual machine as a regular user".

2) Yes, User2 has permissions from their Group2 with "Virtual Machine User Login" rights to RG1 resources. VM1 is part of RG1.

3) No, "Virtual Machine Contributor" has rights to manage the VM, but does not have permissions to log directly into it as a user.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/compute#virtual-machine-contributor>  
upvoted 2 times

HOTSPOT

-

You have an Azure subscription that contains the following virtual machine:

- Name: V1
- Azure region: East US
- System-assigned managed identity: Disabled

You create the managed identities shown in the following table.

| Name     | Location |
|----------|----------|
| Managed1 | East US  |
| Managed2 | East US  |
| Managed3 | West US  |

You perform the following actions:

- Assign Managed1 to V1.
- Create a resource group named RG1 in the West US region.

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

NOTE: Each correct selection is worth one point.

### Answer Area

#### Statements

Yes

No

You can assign Managed2 to V1.

☐☐

You can assign Managed3 to V1.

☐☐

You can assign VM1 the Owner role for RG1.

☐☐

#### Answer Area

Suggested Answer:

#### Statements

Yes

No

You can assign Managed2 to V1.

☒☐

You can assign Managed3 to V1.

☒☐

You can assign VM1 the Owner role for RG1.

☐☒

YYN.

You can use user assigned managed identities in more than one Azure region.

upvoted 18 times

  **wooyourdaddy** 1 year, 11 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 7 times

  **Obyte**  1 year, 2 months 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 12 times

  **Nyamnyam** 1 year, 1 month 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**  6 months, 3 weeks 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 enabled 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 2 times

  **RemmyT** 6 months, 3 weeks ago

NO

System-assigned managed identity: Disabled

upvoted 1 times

  **AK\_1234** 1 year, 2 months ago

- Y

- Y

- N

upvoted 2 times



  **EmnCours** 1 year, 4 months ago

YES

YES

YES

upvoted 1 times

  **nils241** 1 year, 5 months ago

The first two are definite yes / yes. For the third, it depends on the scenario;

Scenario 1:

I give one of the user assigned identities the owner role. Problem: Every service with the identity would be owner. 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 Assigned 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, 6 months 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, 6 months ago

YES

YES

YES

upvoted 1 times

🗨️ **ITAdmin2019** 1 year, 7 months 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, 9 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** 1 year, 5 months ago

You can add "user assigned identities" without enable "system assigned" on the VM

upvoted 1 times

🗨️ **chikorita** 1 year, 9 months ago

i feel the same too

upvoted 1 times

🗨️ **cris\_exam** 1 year, 9 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, 9 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, 10 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, 11 months ago

I believe VM1 should be Managed 1 here. So answer is No.

upvoted 1 times

🗨️ 👤 **natazar** 1 year, 11 months ago

I think it should be YNN

upvoted 1 times

🗨️ 👤 **kevin\_office** 1 year, 11 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 50 times

## HOTSPOT

-

You have an Azure subscription that contains the key vaults shown in the following table.

| Name      | In resource group | Number of days to retain deleted key vaults | Purge protection |
|-----------|-------------------|---------------------------------------------|------------------|
| KeyVault1 | RG1               | 15                                          | Enabled          |
| KeyVault2 | RG1               | 10                                          | Disabled         |

The subscription contains the users shown in the following table.

| Name   | Role                           |
|--------|--------------------------------|
| Admin1 | Key Vault Administrator        |
| Admin2 | Key Vault Contributor          |
| Admin3 | Key Vault Certificates Officer |
| Admin4 | Owner                          |

On June 1, Admin4 performs the following actions:

- Deletes a certificate named Certificate1 from KeyVault1
- Deletes a secret named Secret1 from KeyVault2

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

NOTE: Each correct selection is worth one point.

**Answer Area****Statements****Yes****No**

Admin1 can recover Secret1 on June 7.

☐☐

Admin2 can purge Certificate1 on June 12.

☐☐

Admin3 can purge Certificate1 on June 14.

☐☐



### Answer Area

Suggested Answer:

#### 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 1 year, 5 months 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 21 times

  **Holii** 1 year 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** 1 year ago

Forgive me, I am blind. There are dates quite literally listed in the question. Still the same.  
upvoted 3 times

  **Markus** Highly Voted 1 year, 5 months 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 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 3 times

  **EmnCours** 11 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** 1 year ago

YES

NO

NO

upvoted 1 times

  **OK2020** 1 year ago

<https://learn.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview>

upvoted 2 times

  **OK2020** 1 year ago

<https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli>

upvoted 1 times

You have an Azure AD tenant.

You open the risk detections report.


Which risk detection type is classified as a user risk?

- A. password spray
- B. anonymous IP address
- C. unfamiliar sign-in properties
- D. Azure AD threat intelligence

**Suggested Answer: D**

Community vote distribution

D (100%)

 **ThotSlayer69** Highly Voted 1 year, 11 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, 11 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 9 months 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** 1 year, 2 months ago

User Risk - D

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

upvoted 1 times

🗨️ 👤 **EmnCours** 1 year, 5 months ago

**Selected Answer: D**

D. Azure AD threat intelligence

upvoted 1 times

🗨️ 👤 **dule27** 1 year, 6 months ago

**Selected Answer: D**

D. Azure AD threat intelligence

upvoted 1 times

🗨️ 👤 **ShoaibPKDXB** 1 year, 7 months ago

**Selected Answer: D**

D correct

upvoted 1 times

🗨️ 👤 **wsrudmen** 1 year, 11 months ago

**Selected Answer: D**

Correct

upvoted 2 times



You have a management group named Group1 that contains two Azure subscriptions named Sub1 and Sub2. The subscriptions are linked to a Microsoft Entra tenant that contains a user named User1.

You need to ensure that User1 can onboard Sub1 to Permissions Management. The solution must follow the principle of least privilege.

Which permission should you grant to User1?

- A. Microsoft.Authorization/roleAssignments/read for Sub1
- B. Microsoft.Authorization/roleAssignments/write for Group1
- C. MicrosoftAuthorization/roleAssignments/write for Sub1
- D. Microsoft.Authorization/roleAssignments/read for Group1

**Correct Answer:** C

  **d1e85d9** 3 months, 2 weeks ago

**Selected Answer: C**

In this scenario, User1 needs to onboard Sub1 to Permissions Management. This requires role assignment permissions at the subscription level.

Analysis of Options:

Correct Answer:

C. Microsoft.Authorization/roleAssignments/write for Sub1

This permission grants User1 the necessary write access at the subscription level to onboard Sub1 to Permissions Management while adhering to the principle of least privilege.

upvoted 1 times

  **YesPlease** 4 months ago

**Selected Answer: A**

Answer A) Least permission is on SUB1.

Microsoft.Authorization/roleAssignments/read for Sub1

"C" is not even written in the right format

<https://learn.microsoft.com/en-us/entra/permissions-management/onboard-azure#explanation:~:text=This%20app%20requires%20%27reader%27%20permissions%20on%20the%20subscriptions>  
upvoted 3 times

  **YesPlease** 3 months, 1 week ago

Answer C

I must have been wired on too many redbulls... you need write to onboard.

upvoted 1 times

  **rvln7** 3 months, 3 weeks ago



Prerequisites

To add Permissions Management to your Microsoft Entra tenant:

You must have a Microsoft Entra user account and an Azure command-line interface (Azure CLI) on your system, or an Azure subscription. If you don't already have one, create a free account.

You must have Microsoft.Authorization/roleAssignments/write permission at the subscription or management group scope to perform these tasks. If you don't have this permission, you can ask someone who has this permission to perform these tasks for you.

upvoted 1 times



  **csi\_2025** 4 months ago

You are wrong. If you read the source you provide carefully you understand that when your tenant is onboarded an App is created and this App requires the reading permissions.

In the Prerequisites its clearly stated what permission is required to do the task and logically its a write permission "You must have Microsoft.Authorization/roleAssignments/write permission at the subscription or management group scope to perform these tasks."

The correct answer is C and most likely a typo by the creator of the question.

upvoted 3 times

  **Oskarma** 4 months, 3 weeks ago

**Selected Answer: C**

The minimum priviledge level is at the subscription.

upvoted 3 times

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

You configure self-service password reset (SSPR) by using the following settings:

- Require users to register when signing in: Yes
- Number of methods required to reset: 1

What is a valid authentication method available to users?

- A. a 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, 10 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 13 times

  **armid** 4 months, 2 weeks ago

agree, otherwise Q28 Topic 2 would be invalidated by answer B

if i see this i will go with D even though it is incomplete answer, hpefully the have fixed it since

upvoted 1 times

  **7ka4maakn** **Most Recent**  3 months ago

**Selected Answer: 0**

[illegible]

upvoted 1 times

  **YesPlease** 4 months ago

**Selected Answer: B**

Answer b) a mobile app code

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#mobile-app-and->

sspr:~:text=When%20administrators%20require%20one%20method%20be%20used%20to%20reset%20a%20password%2C%20verification%20code%20is%20t

upvoted 1 times

  **YesPlease** 4 months ago

Answer D

I was wrong, the answer is still "email"...regardless if it is external.

You are not allowed to have Authenticator App as the only method for SSPR.

[https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#authentication-](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#authentication)

methods:~:text=Authenticator%20can%27t%20be%20selected%20as%20the%20only%20authentication%20method%20when%20only%20one%20method%

upvoted 1 times

  **Matt19** 6 months, 1 week 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 2 times

🗨️ 👤 **Nyamnyam** 1 year, 1 month 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** 1 year, 4 months 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 2 times

🗨️ 👤 **Shri96** 1 year, 3 months 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** 1 year, 5 months ago

**Selected Answer: B**

Correct Answer: B

upvoted 1 times

🗨️ 👤 **dule27** 1 year, 6 months ago

**Selected Answer: B**

B. a mobile app code

upvoted 1 times

🗨️ 👤 **JN\_311** 1 year, 6 months ago

**Selected Answer: B**

When administrators require one method be used to reset a password, verification code is the only option available.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#mobile-app-and-sspr>

upvoted 3 times

🗨️ 👤 **roman\_cat** 1 year, 4 months ago

question is asking for users, not administrators

upvoted 1 times

🗨️ 👤 **BigDogAG** 9 months, 1 week ago

Yes but in this instance the admin is who put the requirements in place.

upvoted 1 times

🗨️ 👤 **kanew** 1 year, 7 months ago

This isn't as straight forward as it seems and from what I can read it depends on whether the converged registration method(MFA & SSPR) is being used. If using the current SSPR registration then the answer would be D as you can't use the App when only one method is required because it is not an available method on sign-up.

"This requirement is because the current SSPR registration experience doesn't include the option to register the authenticator app. The option to register the authenticator app is included with the new combined registration experience."

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#authentication-methods>

It's the other way around if the combined registration is used as email is only valid for SSPR and users won't be required to register it on sign up. It can be a secondary method. I can't tell from the question whether it's SSPR or combined registration. maybe someone else can? Guess I'll go with the consensus of B but ...?

upvoted 1 times



🗨️ 👤 **francescoc** 1 year, 9 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, 11 months ago

**Selected Answer: B**

correct explanation by wooyou

upvoted 1 times

🗨️ 👤 **Halwagy** 1 year, 11 months ago

D also a valid option

upvoted 1 times

🗨️ 👤 **kevin\_office** 1 year, 11 months ago

yeah but D comes when B is not available

upvoted 2 times

🗨️ 👤 **wooyourdaddy** 1 year, 11 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

🗨️ 👤 **csi\_2025** 4 months ago

I think you are wrong and the wording from Microsoft is bad which is why they added a table underneath it that clarifies it.

upvoted 1 times

You create a new Microsoft 365 E5 tenant.

You need to ensure that when users connect to the Microsoft 365 portal from an anonymous IP address, they are prompted to use multi-factor authentication (MFA).

What should you configure?

- A. a sign-in risk policy
- B. a user risk policy
- C. an MFA registration policy

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **BRoald** Highly Voted 1 year, 5 months 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** 6 months, 3 weeks 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 6 times

🗳️ 👤 **EmnCours** Most Recent 11 months, 2 weeks ago  
Selected Answer: A  
A. a sign-in risk policy  
upvoted 1 times

🗳️ 👤 **dule27** 1 year ago  
Selected Answer: A  
A. a sign-in risk policy  
upvoted 1 times

🗳️ 👤 **ShoaibPKDXB** 1 year, 1 month ago  
Selected Answer: A  
A correct  
upvoted 1 times

🗳️ 👤 **rajbne** 1 year, 2 months ago  
its "new" tenancy so could be C as well  
upvoted 1 times

🗳️ 👤 **bda92b3** 1 year, 3 months ago  
Correct  
upvoted 1 times

🗳️ 👤 **Jotest** 1 year, 5 months ago  
sign-in risk policy seems to be correct

upvoted 2 times

HOTSPOT

You have a Microsoft 365 tenant.

You configure a conditional access policy as shown in the Conditional Access policy exhibit. (Click the Conditional Access policy tab.)

Home > ContosoAzureAD > Security > Conditional Access

## 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.)

## Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

 Edit

### Activation

| Setting                                  | State                |
|------------------------------------------|----------------------|
| Activation maximum duration (hours)      | 8 hour(s)            |
| Require justification on activation      | Yes                  |
| Require ticket information on activation | No                   |
| On activation, require Azure MFA         | Yes                  |
| Require approval to activate             | Yes                  |
| Approvers                                | 1 Member(s), 0 Group |

### Assignment

| Setting                                                        | State      |
|----------------------------------------------------------------|------------|
| Allow permanent eligible assignment                            | No         |
| Expire eligible assignments after                              | 15 day(s)  |
| Allow permanent active assignment                              | No         |
| Expire active assignments after                                | 1 month(s) |
| Require Azure Multi-Factor Authentication on active assignment | No         |
| Require justification on active assignment                     | No         |

You view the User administrator role assignments as shown in the Role assignments exhibit. (Click the Role assignments tab.)




## User Administrator | Assignments

Privileged Identity Management | Azure AD roles

» [+ Add assignments](#) [Settings](#) [Refresh](#) [Export](#) | [Got feedback?](#)

**Eligible assignments** Active assignments Expired assignments

 Search by member name or principal name

| Name                      | Principal name                     | Type | Scope     | Membership |
|---------------------------|------------------------------------|------|-----------|------------|
| <b>User Administrator</b> |                                    |      |           |            |
| Admin1                    | Admin1@m365x629615.onmicrosoft.com | User | Directory | Direct     |
| Admin2                    | Admin2@m365x629615.onmicrosoft.com | User | Directory | Direct     |
| Admin3                    | Admin3@m365x629615.onmicrosoft.com | User | Directory | Direct     |

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

NOTE: Each correct selection is worth one point.

| Statements                                                                                                                                                                                               | Yes                   | No                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.                                                                             | <input type="radio"/> | <input type="radio"/> |
| Admin2 can request activation of the User administrator role for a period of two hours.                                                                                                                  | <input type="radio"/> | <input type="radio"/> |
| If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice. | <input type="radio"/> | <input type="radio"/> |

|                   | Statements                                                                                                                                                                                               | Yes                              | No                               |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| Suggested Answer: | Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.                                                                             | <input checked="" type="radio"/> | <input type="radio"/>            |
|                   | Admin2 can request activation of the User administrator role for a period of two hours.                                                                                                                  | <input checked="" type="radio"/> | <input type="radio"/>            |
|                   | If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice. | <input type="radio"/>            | <input checked="" type="radio"/> |

  **Halwagy** Highly Voted 2 years, 5 months ago

Correct


upvoted 18 times

  **SFAY** 1 year, 5 months ago

Tested and verified in the Lab.

YYN

upvoted 3 times

  **chikorita** Highly Voted 2 years, 3 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** 2 years, 3 months ago

I would also go with YYY as you explained, it makes sense.

upvoted 1 times

  **cris\_exam** 2 years, 3 months ago

take back what I said - Require MFA on Active assignment is set to NO. so it's YYN.

upvoted 3 times



  **chikorita** 2 years, 3 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, 12 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 MSAAuthenticator, then you would get another

MFA request but that is not the case here so YYN


upvoted 6 times

  **Holii** 2 years 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** 9 months, 3 weeks ago

Yes, its mentioned 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 2 times

  **leedsbarber** Most Recent 1 month ago

I have just been reading about statement 2. It appears that the activation maximum duration becomes a default option. You may only require 2 hours, but you can't choose 2 hours, only 8 hours. Or have I misunderstood?

[https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings#on-activation-require-multi-factor-authentication states:](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings#on-activation-require-multi-factor-authentication-states)

"Activation maximum duration.

Use the Activation maximum duration slider to set the maximum time, in hours, that an activation request for a role assignment remains active before it expires. This value can be from one to 24 hours."

upvoted 1 times

  **OneplusOne** 4 weeks, 1 day ago

On activation you can change the default of 8 hours to something less.

upvoted 1 times

  **Rackup** 3 months, 3 weeks ago

It says in the policy on activation require MFA so Y/Y/Y.

upvoted 1 times

  **Siraf** 1 year, 6 months 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, 8 months ago

Correct

upvoted 1 times

  **EmnCours** 1 year, 11 months ago


Yes Yes No

upvoted 3 times

  **Heshan** 1 year, 11 months ago

On the exam, 09/07/2023

upvoted 2 times



  **dule27** 2 years ago

Yes

Yes

No

upvoted 3 times

  **217f3c9** 2 years, 2 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** 2 years ago

Tested and confirmed. YYN.

upvoted 1 times

  **f2bf85a** 2 years, 2 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



HOTSPOT

-

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

| Name  | User risk level |
|-------|-----------------|
| User1 | Low             |
| User2 | Medium          |
| User3 | High            |

You have the Azure AD Identity Protection policies shown in the following table.

| Type                | Users     | User risk     | Sign-in risk | Controls     |
|---------------------|-----------|---------------|--------------|--------------|
| User risk policy    | All users | Low and above | Unconfigured | Block access |
| Sign-in risk policy | All users | Unconfigured  | High         | Block access |

You review the Risky users report and the Risky sign-ins report and perform actions for each user as shown in the following table.

| User  | Action                   |
|-------|--------------------------|
| User1 | Confirm user compromised |
| User2 | Confirm sign-in safe     |
| User3 | Dismiss user risk        |
| User2 | Confirm user compromised |

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

NOTE: Each correct selection is worth one point.

| Statements                                                    | Yes                   | No                    |
|---------------------------------------------------------------|-----------------------|-----------------------|
| User1 can sign in by using multi-factor authentication (MFA). | <input type="radio"/> | <input type="radio"/> |
| User2 can sign in by using multi-factor authentication (MFA). | <input type="radio"/> | <input type="radio"/> |
| User3 can sign in from an anonymous IP address.               | <input type="radio"/> | <input type="radio"/> |

| Statements                                                    | Yes                              | No                               |
|---------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 can sign in by using multi-factor authentication (MFA). | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 can sign in by using multi-factor authentication (MFA). | <input checked="" type="radio"/> | <input type="radio"/>            |
| User3 can sign in from an anonymous IP address.               | <input type="radio"/>            | <input checked="" type="radio"/> |

Suggested Answer:

 doch  2 years, 5 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 32 times

  **c18525f** 2 years, 4 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.

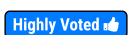
Machine learning stuff :- what do you think ?

upvoted 3 times

  **ExamStudy68** 2 years, 2 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

  **ThotSlayer69**  2 years, 5 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** 8 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 2 times

  **d1e85d9**  3 months, 2 weeks ago

NO

NO

YES

upvoted 1 times

  **Fijii** 4 months ago

From what I learned/tested and read from the comments, I think :

User 1 : No, because it was flagged comprised so it is blocked by the User risk policy

User 2 : No, for the same reason, the sign-in risk was dismissed but the user risk was flagged compromised, so it is blocked by the User risk policy

User 3 : Yes, it was initially a high risk user, but the risk was dismissed by the admin. It is now safe from being blocked by the User risk policy.

Connecting from anonymous IP address represent a sign-in risk, I was not able to find if it is medium or high, I think it might depends on the IP ? If it is medium, then sign in is allowed because the Sign-in risk policy only blocks high-risk sign-ins.

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

Here's an interesting article on how to simulate risk

<https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-simulate-risk>

upvoted 1 times

🗨️ 👤 **Frank9020** 5 months ago

User1: No, because the User Risk Policy blocks all users with Low risk and above, even if MFA is available.

User2: No, because User2 is marked as compromised and the User Risk Policy blocks Medium risk and above.

User3: No, because the User Risk Policy already blocks them based on their previous High risk status, and their risk was only dismissed, not cleared for access. Even if User3's user risk was dismissed, their sign-in risk from an anonymous IP would likely be categorized as High.

Since the Sign-in Risk Policy blocks High sign-in risk, User3 would still be blocked when trying to sign in from an anonymous IP.

upvoted 1 times

🗨️ 👤 **perkp** 5 months, 2 weeks ago

N N Y

In Azure, sign-ins from anonymous IP addresses (such as those using Tor browsers or anonymous VPNs) are considered a medium sign-in risk.

upvoted 1 times

🗨️ 👤 **naveenbio** 6 months, 3 weeks 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** 1 year 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** 1 year, 2 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 + User 3 has the following action performed on his account : "Dismiss User Risk"

upvoted 1 times

🗨️ 👤 **ANIMOSITYOP** 1 year, 4 months 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, 9 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, 6 months 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, 8 months ago

I agree, thanks for the explanation

N

N

y

upvoted 2 times

🗨️ 👤 **Nivos300** 1 year, 7 months ago

I agree

N

N

Y

upvoted 2 times

🗨️ 👤 **EmnCours** 1 year, 10 months ago

N

N

Y

upvoted 1 times

🗨️ 👤 **Tweety1972** 1 year, 11 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** 2 years 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 Protection sets Risk Level to None -

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/troubleshooting-identity-protection-faq#how-do-the-feedback->

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** 2 years ago

No

No

Yes

upvoted 2 times

  **wsrudmen** 2 years, 5 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** 2 years, 2 months ago



agree with this

upvoted 1 times

  **dobriv** 2 years, 4 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** 2 years, 1 month 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** 2 years, 5 months ago

the user risk policy is block access

N N Y

upvoted 5 times

You have an Azure subscription that contains a user named User1.

You need to meet the following requirements:

- Prevent User1 from being added as an owner of newly registered apps.
- Ensure that User1 can manage the application proxy settings.
- Ensure that User1 can register apps.
- Use the principle of least privilege.

Which role should you assign to User1?

- A. Application developer
- B. Cloud application administrator
- C. Service support administrator
- D. Application administrator

**Suggested Answer: D**

Community vote distribution

D (100%)

 **doch**  1 year, 11 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 10 times

 **Halwagy**  1 year, 11 months ago

**Selected Answer: D**

Correct Answer given

upvoted 5 times

 **baz**  11 months, 1 week ago

D. Application Administrator - other roles can manage Application Proxy settings

upvoted 2 times

 **Shena2021** 1 year, 3 months 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** 1 year, 4 months ago

**Selected Answer: D**



D. Application administrator

upvoted 2 times

 **dule27** 1 year, 6 months ago

Selected Answer: D

D. Application administrator  
upvoted 2 times



  **dejo** 1 year, 10 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** 1 year ago

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#application-administrator>  
upvoted 1 times

  **dobriv** 1 year, 10 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 13 times

## DRAG DROP

-

You have a Microsoft 365 E5 subscription and an Azure subscription.

You need to meet the following requirements:

- Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials.
- Delegate the ability to create new virtual machines.

What should you use for each requirement? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

| Features                                     |   | Answer Area                                                                                                            |
|----------------------------------------------|---|------------------------------------------------------------------------------------------------------------------------|
| Azure AD built-in roles                      | • | Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials: <input type="text"/> |
| Azure AD managed identities                  | • |                                                                                                                        |
| Azure role-based access control (Azure RBAC) | • | Delegate the ability to create new virtual machines: <input type="text"/>                                              |

**Suggested Answer:**

| Answer Area                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials: <input type="text" value="Azure role-based access control (Azure RBAC)"/> |
| Delegate the ability to create new virtual machines: <input type="text" value="Azure AD built-in roles"/>                                                                   |

**dobriv** Highly Voted 2 years, 1 month 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 23 times

**mancio** Highly Voted 2 years, 1 month 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** 8 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, 10 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

**d1e85d9** Most Recent 3 months, 2 weeks ago

Given answers are correct.

upvoted 1 times

**Rackup** 3 months, 3 weeks ago

A quick way to see why both requirements use Azure RBAC is to remember that:

Letting users sign in to an Azure VM with their M365 (Entra) credentials requires assigning them either the Virtual Machine Administrator Login or Virtual Machine User Login role at the VM (or resource group/subscription) scope. Those roles are part of Azure role-based access control (RBAC),



not Azure AD built-in roles or managed identities.

Delegating VM creation is also an Azure RBAC task, typically by assigning a built-in role such as "Contributor" or "Virtual Machine Contributor" on the desired scope.

Therefore, both "Allow users to sign in to Azure VMs with Microsoft 365 credentials" and "Delegate the ability to create new VMs" are accomplished via Azure RBAC.

upvoted 1 times

🗨️ 👤 **RemmyT** 1 year ago

RBAC : Virtual Machine User Login

RBAC : VM Contributor

upvoted 1 times

🗨️ 👤 **emartiy** 1 year, 3 months ago

Both are Azure role-based 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** 1 year, 3 months 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, 8 months ago

Both RBAC There is no Azure AD built in roles to delegate creation of VM's that's in Azure built in Roles (without AD ;) )

upvoted 1 times

🗨️ 👤 **stack120566** 2 years, 1 month 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** 2 years, 2 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** 2 years, 5 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** 2 years, 4 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** 2 years, 5 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** 2 years, 5 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** 2 years, 5 months ago

Azure AD managed Identities  
Azure Role-based access control  
upvoted 5 times

  **Halwagy** 2 years, 5 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

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 11 months, 1 week 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 8 months, 3 weeks ago

Hello? Is it this question youre looking for?  
upvoted 5 times

🗳️ 👤 **roman\_cat** Most Recent 10 months, 1 week 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** 10 months, 1 week 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** 11 months, 1 week ago

Selected Answer: D

Correct Answer: D  
upvoted 1 times

🗳️ 👤 **dule27** 1 year ago

Selected Answer: D

D. Windows Hello for Business  
upvoted 3 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.



The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their 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. SMS
- C. an app password
- D. a notification through the Microsoft Authenticator app

**Correct Answer: A**

  **Shingie** 4 months, 2 weeks ago

**Selected Answer: A**

The correct answer is:

A. A verification code from the Microsoft Authenticator app

Explanation:

The users are in remote locations with no Wi-Fi or mobile phone connectivity, but they do have internet access via a wired network.

Analysis of Each Option:

A. A verification code from the Microsoft Authenticator app (Correct)

The Authenticator app generates time-based one-time passwords (TOTP) that do not require internet or cellular connectivity.

This method works entirely offline, making it the best choice for remote locations.

B. SMS (Incorrect)

Requires mobile network connectivity, which the scenario states is not available.

C. An app password (Incorrect)

App passwords are only used for legacy authentication, which should be avoided in modern security setups.

Microsoft is deprecating app passwords as part of stronger MFA enforcement.

D. A notification through the Microsoft Authenticator app (Incorrect)

Push notifications require an internet connection, which is not available via mobile in this scenario.

upvoted 1 times

HOTSPOT

-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant. The AD DS domain contains the organizational units (OUs) shown in the following table.

| Name | Description                        |
|------|------------------------------------|
| OU1  | Syncs with Azure AD                |
| OU2  | Does <b>NOT</b> sync with Azure AD |

You need to create a break-glass account named BreakGlass.

Where should you create BreakGlass, and which role should you assign to BreakGlass? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Location:

▼

Azure AD  
OU1  
OU2

Role:

▼

Billing Administrator  
Global Administrator  
Owner  
Privileged Role Administrator

## Answer Area

Suggested Answer:

Location:

Azure AD

OU1

OU2

Role:

Billing Administrator

Global Administrator

Owner


Privileged Role Administrator

 **DoMing**  1 year, 8 months ago

AzureAD and Global Admin

<https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access#how-to-create-an-emergency-access-account>

upvoted 41 times

 **topzz** 1 year, 8 months ago

break-glass account = emergency access account

upvoted 6 times

 **ANiMoSiTYOP** 10 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 3 times

 **kmk\_01**  1 year, 8 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

 **d1e85d9**  3 months, 2 weeks ago

If the resource is on-prem then the answer must be => OU1.

Otherwise, the answer is => Azure AD.

From the below link, take note this paragraph (Federation Guidance):

Federation guidance

The emergency access for on-premises systems and the emergency access for cloud services should be kept distinct, with no dependency of one on the other.

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access#how-to-create-an-emergency-access-account>

upvoted 1 times

 **HartMS** 9 months ago

Azure AD and Global Admin

upvoted 3 times

 **emartiy** 9 months 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 4 times

🗨️ 👤 **kijken** 1 year, 1 month ago

Sorry, but a break glass account for what? For Azure or for on prem AD?

upvoted 1 times

🗨️ 👤 **norkis97** 1 year, 1 month ago

Break glass account must be only azure ad account !

Break glass account also must be Global Administrator

upvoted 4 times

🗨️ 👤 **sherifhamed** 1 year, 3 months 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** 1 year, 4 months 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** 1 year, 4 months 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** 1 year, 5 months ago

AzureAD and Global Admin

upvoted 2 times

🗨️ 👤 **dule27** 1 year, 6 months ago

Azure AD

Global Admin

Break-glass account has emergency access

upvoted 3 times

🗨️ 👤 **caef525** 1 year, 8 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

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, 8 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 9 months ago

**Selected Answer: B**

Access Packages



upvoted 2 times

  **EmnCours** 1 year, 5 months ago

**Selected Answer: B**

B. Create an access package.

upvoted 1 times

  **dule27** 1 year, 6 months ago

**Selected Answer: B**

B. Create an access package.

upvoted 1 times



HOTSPOT

-

You have an Azure subscription.

You need to create two custom roles named Role1 and Role2. The solution must meet the following requirements:

- Users that are assigned Role1 can manage application security groups.
- Users that are assigned Role2 can manage Azure Firewall.

Which resource provider permissions are required for each role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Role1:   
Microsoft.App  
Microsoft.Computer  
Microsoft.Network  
Microsoft.Security

Role2:   
Microsoft.App  
Microsoft.Management  
Microsoft.Network  
Microsoft.Security

### Answer Area

Suggested Answer:

Role1:   
Microsoft.App  
Microsoft.Computer  
**Microsoft.Network**  
Microsoft.Security

Role2:   
Microsoft.App  
Microsoft.Management  
**Microsoft.Network**  
Microsoft.Security

 **DoMing**  2 years, 2 months ago

Correct

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



upvoted 16 times

 **Nail** 8 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** 2 years, 2 months ago

Thanks for providing the link.


upvoted 3 times

  **dvmhike** Most Recent 7 months, 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, 11 months ago

Role1: Microsoft.Network

Role2: Microsoft.Network

upvoted 2 times

  **dule27** 1 year, 12 months ago

Role1: Microsoft.Network

Role2: Microsoft.Network

upvoted 2 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

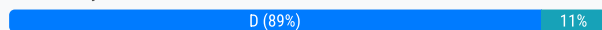
You plan to implement multi-factor authentication (MFA).

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



🗳️ **sbettani** Highly Voted 2 years, 1 month ago

without internet ... D? We answer to 10 question with app password. Then B  
upvoted 5 times

🗳️ **Frank9020** Most Recent 5 months, 1 week ago

**Selected Answer: D**

Microsoft Authenticator app. The code is generated locally on the app and does not require internet or mobile connectivity.  
upvoted 1 times

🗳️ **Phax** 8 months ago

Answer should be B, there's no internet and phone connectivity, how can the app be working. While the only connectivity initiated was the wired connection.  
upvoted 1 times

🗳️ **emartiy** 1 year, 3 months 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** 1 year, 4 months ago

**Selected Answer: B**

how do you receive verification code without internet...?  
i would answer B  
upvoted 1 times

🗳️ **Tony416** 9 months, 4 weeks 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, 11 months ago

**Selected Answer: D**

D. a verification code from the Microsoft Authenticator app  
upvoted 1 times

🗨️ 👤 **dule27** 2 years ago

**Selected Answer: D**

D. a verification code from the Microsoft Authenticator app

upvoted 1 times

🗨️ 👤 **ahmedkmicha** 2 years 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

You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server.

You enable Microsoft Entra login for the virtual machines.

Users report that they cannot sign in to the virtual machines by using their Microsoft Entra credentials.

You need to ensure that the users can sign in to the virtual machines.

What should you do first?

- A. From the Microsoft Entra admin center, delete the device registrations of the virtual machines.
- B. Revoke the primary refresh token.
- C. Enable SSH client support for OpenSSH.
- D. Ensure that the virtual machines can access <https://enterpriseregistration.windows.net>.

**Correct Answer:** D

  **YesPlease** 4 months ago

**Selected Answer:** D

Answer D

<https://www.testpreptraining.com/tutorial/steps-to-configure-azure-ad-join/>  
upvoted 1 times

DRAG DROP

-

You have a Microsoft 365 E5 tenant.

You purchase a cloud app named App1.

You need to enable real-time session-level monitoring of App1 by using Microsoft Defender for Cloud Apps.

In which order should you perform the actions? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

### Actions

### Answer Area

Publish App1 in Azure AD.

Create a conditional access policy that has session controls configured.

From Microsoft Defender for Cloud Apps, create a session policy.

From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1.



### Answer Area

Publish App1 in Azure AD.

From Microsoft Defender for Cloud Apps, modify the Connected apps settings for App1.

From Microsoft Defender for Cloud Apps, create a session policy.

Create a conditional access policy that has session controls configured.

### Suggested Answer:

**DoMing** Highly Voted 2 years, 2 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 42 times

**d1e85d9** 3 months, 2 weeks ago

Correct  
upvoted 1 times

**HartMS** 1 year, 2 months ago

correct  
upvoted 2 times

**hml\_2024** Most Recent 10 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 2 times

  **EmnCours** 1 year, 11 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, 12 months ago

1. Publish App1 in Azure AD.
2. Create a conditional access policy that has session controls configured.
3. From Microsoft Defender for Cloud Apps modify the Connected apps settings for app1
4. From Microsoft Defender for Cloud Apps create a session policy

upvoted 1 times

## HOTSPOT

-

## Case Study

-

## Overview

-

ADatum Corporation is a consulting company in Montreal.

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

Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

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

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | None                              |
| User2 | None                              |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner | Members                        |
|-------------|----------|-----------------|-------|--------------------------------|
| IT_Group1   | Security | Assigned        | None  | All users in the IT department |
| AdatumUsers | Security | Assigned        | None  | User1, User2                   |

Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.



- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

#### Requirements. Planned Changes

-

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

#### Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You implement the planned changes for SSPR.

What occurs when User3 attempts to use SSPR? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

Number of authentication methods required:

▼

1  
2  
3  
4

Authentication methods that can be used:

▼

Microsoft Authenticator only  
Security questions only  
Email and phone only  
Phone and Microsoft Authenticator only  
Email, phone, and Microsoft Authenticator only  
Email, phone, Microsoft Authenticator, and security questions

#### Answer Area

Number of authentication methods required:

1  
2  
3  
4

Suggested Answer:

Authentication methods that can be used:

Microsoft Authenticator only  
Security questions only  
Email and phone only  
Phone and Microsoft Authenticator only  
Email, phone, and Microsoft Authenticator only  
Email, phone, Microsoft Authenticator, and security questions

 **marsot**  1 year, 11 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 31 times

 **Fijii** 4 months ago

This is correct, under SSPR in Entra, it is said :


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.

upvoted 1 times

 **Shivz0903** 11 months, 1 week ago

It says security defaults are disabled, does this not make a difference?

upvoted 1 times

 **9H3zmT6** 1 month, 4 weeks ago

If you do not disable this setting, you cannot apply or exclude MFA under specific conditions or for specific users or groups.

upvoted 1 times

 **SFAY** 1 year, 5 months 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

 **armid** 4 months, 2 weeks ago

because the requirements stated in the questions apply for "users" not administrators

upvoted 1 times



 **SFAY**  1 year, 5 months 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 10 times

  **survivor** 7 months, 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** 1 year, 4 months 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

  **d1e85d9**  3 months, 2 weeks ago

Correct Answer:

Number of Auth Method: => 1

Auth Method CAN BE use: => Email, Phone, & The Microsoft Authenticator app

Because Admin cannot use security question as authentication method for SSPR.

upvoted 1 times



  **Arash123** 7 months, 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** 1 year, 3 months ago

1 method since question 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** 7 months, 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, 11 months ago

I think authen methods should be 2, password + one of those MFA methods

upvoted 1 times

🗨️ 👤 **Peeeedor** 1 year, 11 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, 8 months ago

You are contradicting yourself :)

upvoted 5 times

🗨️ 👤 **marsot** 1 year, 11 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

## HOTSPOT

-

## Case Study

-

## Overview

-

ADatum Corporation is a consulting company in Montreal.

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

Existing Environment. ADatum Environment

The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

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

The tenant contains the users shown in the following table.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | None                              |
| User2 | None                              |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

| Name        | Type     | Membership type | Owner | Members                        |
|-------------|----------|-----------------|-------|--------------------------------|
| IT_Group1   | Security | Assigned        | None  | All users in the IT department |
| AdatumUsers | Security | Assigned        | None  | User1, User2                   |

Existing Environment. Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment. Problem Statements

ADatum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.

- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role to IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non-administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

#### Requirements. Planned Changes

-

ADatum plans to implement the following changes:

- Configure self-service password reset (SSPR).
- Configure multi-factor authentication (MFA) for all users.
- Configure an access review for an access package named Package1.
- Require admin approval for application access to organizational data.
- Sync the AD DS users and groups of litware.com with the Azure AD tenant.
- Ensure that only users that are assigned specific admin roles can invite guest users.
- Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

#### Requirements. Technical Requirements

ADatum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
  - Email
  - Phone
  - Security questions
  - The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

You need to support the planned changes and meet the technical requirements for MFA.

Which feature should you use, and how long before the users must complete the registration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Feature:

- An authentication method policy
- A Conditional Access policy
- An MFA registration policy
- The Multi-Factor Authentication Server settings

Grace period:

- 7 days
- 14 days
- 28 days

### Answer Area

Suggested Answer:

Feature:

- An authentication method policy
- A Conditional Access policy
- An MFA registration policy
- The Multi-Factor Authentication Server settings

Grace period:

- 7 days
- 14 days
- 28 days

 **marsot** Highly Voted 11 months, 1 week 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 12 times

 **JCKd4Ni3L** Highly Voted 8 months, 1 week ago

Answer is Correct !

upvoted 5 times

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 9 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 10 months ago

i think user risk, sign in risk & conditional Access for anonymous IP

upvoted 7 times

🗄️ 👤 **rvln7** 4 months ago

1000%, if a resource was ACCESSED from an anonymous IP address it has nothing to do with sign-in or user risk policy

upvoted 1 times

🗄️ 👤 **1c67a2c** Most Recent 11 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** 8 months 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** 8 months ago

Actually you can read on the SC-300 web page that this exam will be updated on Oct 30th 2023. So if you pass this exam after this point, it's safe to assume it's Conditional Access Policy.

Exam page: <https://learn.microsoft.com/en-us/credentials/certifications/exams/sc-300/>

The important notice states: "The English language version of this exam will be updated on October 30, 2023."

upvoted 2 times

🗄️ 👤 **penatuna** 9 months, 2 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** 9 months, 2 weeks ago

BTW, here's a good video about the subject.

[https://youtu.be/zV\\_MBngLND0](https://youtu.be/zV_MBngLND0)

upvoted 2 times

🗄️ 👤 **EmnCours** 11 months, 1 week ago

Correct

upvoted 2 times

A user named User1 receives an error message when attempting to access the Microsoft Defender for Cloud Apps portal.

You need to identify the cause of the error. The solution must minimize administrative effort.

What should you use?

- A. Log Analytics
- B. sign-in logs
- C. audit logs
- D. provisioning logs

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **Panama469** 11 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** 1 year, 3 months 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** 1 year, 4 months ago

Sign-in logs

upvoted 1 times

🗳️ 👤 **haazybanj** 1 year, 7 months 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, 8 months ago

Correct , Sign-in Logs for Msft Defender for Cloud Apps

upvoted 1 times

🗳️ 👤 **rohitrc8521** 1 year, 8 months ago

absolutely correct

upvoted 2 times

🗳️ 👤 **ServerBrain** 1 year, 10 months ago

**Selected Answer: B**

Correct

upvoted 3 times

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps and Yammer.

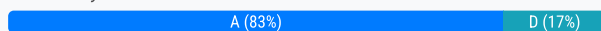
You need prevent users from signing in to Yammer from high-risk locations.

What should you do in the Microsoft Defender for Cloud Apps portal?

- A. Create an access policy.
- B. Create an activity policy.
- C. Unsanction Yammer.
- D. Create an anomaly detection policy.

**Suggested Answer: A**

Community vote distribution



🗳️ 👤 **Panama469** 11 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** 1 year, 3 months ago

**Selected Answer: A**

Create an access policy. based on user risk level!

upvoted 2 times

🗳️ 👤 **ELQUMS** 1 year, 4 months ago

Access Policy

upvoted 1 times

🗳️ 👤 **Nyamnyam** 1 year, 7 months ago

OK, it sounds a bit heretical, but:

I can configure named locations for high-risk countries and create a CAP for Yammer cloud app specifically.

Where is this setting in Defender Cloud Apps? I can configure Cloud Apps access policy and specify Location, but I cannot specify Yammer as the only target app in scope.

upvoted 1 times

🗳️ 👤 **JimboJones99** 1 year, 8 months ago

**Selected Answer: A**

A - Access Policy

upvoted 3 times

🗳️ 👤 **Anonymouse1312** 1 year, 8 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, 8 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, 10 months ago

**Selected Answer: A**

correct

upvoted 2 times

  **1c67a2c** 1 year, 11 months ago

seems correct <https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad>


upvoted 2 times

  **Anonymouse1312** 1 year, 8 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, 8 months ago

disregard my comment.

Given answer is CORRECT.

Not anomaly detection between that does not prevent users from signing-in! '

upvoted 1 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

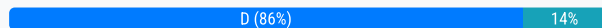
You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. SMS
- B. email
- C. security questions
- D. a verification code from the Microsoft Authenticator app

**Suggested Answer: D**

*Community vote distribution*



🗲️ 👤 **ServerBrain** Highly Voted 1 year, 10 months ago

**Selected Answer: D**

i think this is appearing for the 5th time.  
upvoted 7 times

🗲️ 👤 **NickGhouse** Most Recent 7 months ago

**Selected Answer: D**

5th time, if verification code is available that is the answer... otherwise it is email. \*shrug\*  
upvoted 1 times

🗲️ 👤 **ELQUMS** 1 year, 4 months ago

Verification Code - In Exam  
upvoted 2 times

🗲️ 👤 **Kronos** 1 year, 4 months ago

Answer is D  
upvoted 1 times

🗲️ 👤 **MacDanorld** 1 year, 7 months ago

**Selected Answer: A**

The correct answer is A  
upvoted 1 times

## HOTSPOT -

You have an Azure subscription named Sub1 that contains three users named User1, User2, and User3. Sub1 has a storage account named storage1 that contains the resources shown in the following table.

| Name   | Type       | Contents |
|--------|------------|----------|
| cont1  | Container  | File1    |
| share1 | File share | File2    |

Sub1 contains the users shown in the following table.

| Name  | Role                     | Scope    |
|-------|--------------------------|----------|
| User1 | Reader                   | Sub1     |
| User2 | Reader                   | Sub1     |
| User2 | Storage Blob Data Reader | storage1 |
| User3 | Storage Contributor      | storage1 |

Which users can read File1, and which users can read File2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

File1:   
User2 only  
User3 only  
User1 and User2 only  
User2 and User3 only  
User1, User2, and User3

File2:   
User2 only  
User3 only  
User1 and User2 only  
User2 and User3 only  
User1, User2, and User3

## Answer Area

Correct Answer:

File1:   
User2 only  
User3 only  
User1 and User2 only  
User2 and User3 only  
User1, User2, and User3

File2:   
User2 only  
User3 only  
User1 and User2 only  
User2 and User3 only  
User1, User2, and User3

59e8fdb 4 months ago

Given answer is correct, Storage Blob Container reader can read containers data but cannot read azure file shares since this role is specifically designed for blob containers. File 1-Blob storage User 2 and 3, Contributor is highly privileged role can read anything pretty much and the second File is only user 3 since user 2 cannot read Azure File Shares with Blob containers reader role nor the user 1 which is reader only.

upvoted 3 times

armid 4 months, 2 weeks ago

uh oh this one is tough couldnt find clear differentiators on learn, but will go with user2 and 3 in both cases. Both storage contributor and data reader seem to have the rights needed to view content of the files. But for the Reader roles, it seems they are able to read the CONTROL plane, not the data plane.

upvoted 1 times

🗨️ 👤 **armid** 4 months, 2 weeks ago

Reader

View all resources, but does not allow you to make any changes.

This role includes the \*/read action for the control plane. Users that are assigned this role can read control plane information for all Azure resources.

upvoted 1 times

🗨️ 👤 **armid** 4 months, 2 weeks ago

i changed my mind, i think the answer provided in the solution is actually correct

to read file share file, you need the:

Microsoft.Storage/storageAccounts/fileServices/files/reads

none of the roles have it except for Storage Account Contributor ( i wasnt able to find Storage Contributor role so i assume they meant Storage Account Contributor and not Storage Account Blob Data Contributor ) . So that would mean File2 can only be accessed by User3

upvoted 1 times

🗨️ 👤 **anonymousarpanch** 4 months, 3 weeks ago

if i understood this correctly, it says reading contents 'file 1 & file 2' within the resources. This means that 'reader' role won't suit. leaves to storage blob data reader which makes sense for reading both type of file1 & file 2. Storage contributor (Storage account contributor as per Azure RBAC) is not meant to read contents..so only answer could be 'User2' in both the boxes

upvoted 2 times

🗨️ 👤 **Oskarma** 4 months, 3 weeks ago

I think it's all of them in both questions:

- Reader: View all resources, but does not allow you to make any changes.

- Storage Account Contributor: Lets you manage storage accounts, including accessing storage account keys which provide full access to storage account data.

upvoted 1 times

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

I change my mind.

- File1: User2 (Storage Blob Data Reader) & User3 (Storage Contributor)

- File2: User3 (Storage Contributor)

upvoted 1 times

🗨️ 👤 **Sunth65** 5 months ago

File1 - user2 and user3,

File2 - user1 and user2

upvoted 2 times



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

You open the risk detections report.

Which risk detection type is classified as a user risk?

- A. impossible travel
- B. anonymous IP address
- C. malicious IP address
- D. Azure AD threat intelligence

**Suggested Answer:** D

Community vote distribution

D (100%)

🗲️ 👤 **emartiy** 9 months ago

**Selected Answer: D**

D. Azure AD threat intededtelligence

Why? A, B, C risk detections are related to Risky Sign-in .. not Risky User..

upvoted 1 times

🗲️ 👤 **ELQUMS** 10 months, 1 week ago

D - in Exam

upvoted 3 times

🗲️ 👤 **ServerBrain** 1 year, 4 months ago

**Selected Answer: D**

corrctet

upvoted 1 times

🗲️ 👤 **Charlie33** 1 year, 4 months ago

**Selected Answer: D**

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

upvoted 2 times

🗲️ 👤 **EmnCours** 1 year, 4 months ago

**Selected Answer: D**

Correct Answer: D

upvoted 1 times

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

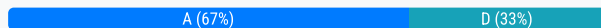
B. 60 days

C. 90 days

D. 180 days

**Suggested Answer: A**

Community vote distribution



**d1e85d9** 3 months, 2 weeks ago

**Selected Answer: C**

C) confirmed 90 Days

Ref Link: <https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-investigate-risk#how-to-investigate-risky-users>

upvoted 2 times

**rvln7** 4 months ago

**Selected Answer: A**

This table reflects the latest information on retention periods for Microsoft Entra Free, P1, and P2 as of February 26, 2025. I just had to mark the answer, but as I said...there is no limit for risky users. "Risky users and workload identities are not deleted until the risk has been remediated."

-----  
| Feature | Microsoft Entra Free | P1 | P2 |

-----  
| Audit Logs | 7 days | 30 days | 30 days |

-----  
| Sign-ins | 7 days | 30 days | 30 days |

-----  
| Multifactor Authentication Usage | 30 days | 30 days | 30 days |

-----  
| Risky Users | No limit | No limit | No limit |

-----  
| Risky Sign-ins | 7 days | 30 days | 90 days |

-----  
upvoted 2 times

**Rahgu** 5 months, 1 week ago

**Selected Answer: C**

It's 90 days, so C.

upvoted 1 times

**Btn26** 5 months, 3 weeks ago

**Selected Answer: C**

Why 90 days is the better answer in this context:

The question specifically asks about "risky user activity," implying the use of Identity Protection features.

Identity Protection, with its detailed risk assessments and reporting, is a core component of Premium P2.



Premium P2 has a 90-day retention for risky sign-ins.

upvoted 2 times

  **anonymousarpnach** 5 months, 2 weeks ago

sorry, if i understand the question, it is asking for Risky user logs and this URL says '<https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-reports-data-retention>' that risky users there is 'No Limit'. am i not correctly understanding this?

upvoted 2 times

  **Phax** 7 months, 4 weeks ago

90 days, logs of risky user activity are usually retained for 90 days...

upvoted 2 times

  **murcao** 8 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** 8 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 4 times



  **Tony416** 9 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 3 times

  **Tony416** 9 months, 4 weeks 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** 11 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's risk 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%20>  
upvoted 1 times

🗨️ 👤 **ELQUMS** 1 year, 4 months ago

A - in Exam

upvoted 2 times

🗨️ 👤 **Sozo** 1 year, 4 months 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 2 times

🗨️ 👤 **baz** 1 year, 5 months 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** 1 year, 5 months 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** 1 year, 5 months 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

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%)

🗳️ 👤 **Futfuyfyfj** 7 months, 1 week 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** 12 months ago

Correct Answer is: B

It is actually the only valid answer in the choices.

upvoted 1 times

🗳️ 👤 **Anonymouse1312** 1 year, 2 months ago

Correct

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#authentication-methods>

upvoted 3 times

HOTSPOT

-

You have an Azure subscription.

From Entitlement management, you plan to create a catalog named Catalog1 that will contain a custom extension.

What should you create first, and what should you use to distribute Catalog1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

First create:

- A managed account
- An Azure Automation account
- An Azure logic app

Distribute Catalog1 by using:

- A playbook
- A workflow
- An access package

### Answer Area

Suggested Answer:

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 1 year, 2 months ago

Seems to be correct:

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-logic-apps-integration>  
upvoted 8 times

 **OrangeSG** 1 year, 1 month 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](https://www.youtube.com/watch?v=tl1GZ_JGMBk&ab_channel=CloudIdentity%7CJefTek)  
upvoted 4 times

 **Alcpt** 7 months, 3 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 10 months, 1 week ago

Correct answers

upvoted 2 times

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

| Name  | Role                   |
|-------|------------------------|
| User1 | User Administrator     |
| User2 | Password Administrator |
| User3 | Security Reader        |
| User4 | User                   |

You enable self-service password reset (SSPR) for all the users and configure SSPR to require security questions as the only authentication method.

Which users must use security questions when resetting their password?

- A. User4 only
- B. User3 and User4 only
- C. User1 and User4 only
- D. User1, User3, and User4 only
- E. User1, User2, User3, and User4

**Suggested Answer: B**

Community vote distribution

B (88%)

13%

 **Obyte**  1 year, 2 months ago

**Selected Answer: B**

Correct answer.

Basically, some administrative roles, by design can only use strong, two-gate password reset policy, regardless of SSPR settings.

User Administrator and Password Administrator will be always forced to use two methods and cannot use security questions.

Security Reader and User will use whatever is set under SSPR, so security questions in this case.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences>

upvoted 15 times

 **d1e85d9**  3 months, 2 weeks ago

**Selected Answer: A**


User1 (User Administrator) – Admins are not allowed to use security questions for SSPR because it's considered a weaker authentication method.

User2 (Password Administrator) – As an admin role, User2 cannot use security questions for SSPR.

User3 (Security Reader) – Security roles are still considered privileged, so User3 cannot use security questions for SSPR.


User4 (Standard User) – User4, being a regular user with no admin privileges, can use security questions for SSPR, as they're the target audience for this method.

upvoted 2 times

 **be9z** 1 year, 1 month 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** 1 year, 1 month 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 2 times

🗨️ 👤 **haazybanj** 1 year, 1 month 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 4 times

🗨️ 👤 **Alcpt** 7 months, 3 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** 7 months, 3 weeks ago

Security Reader is not an Admin role subjected to "admin" SSPR rules.

upvoted 1 times

🗨️ 👤 **Nivos23** 1 year, 1 month ago

**Selected Answer: B**

I agree with ObyteThe answer is b

upvoted 1 times

🗨️ 👤 **Lekong** 1 year, 2 months ago

I think it should be Username only

upvoted 1 times

🗨️ 👤 **Lekong** 1 year, 2 months ago

I mean User 4 only. A

upvoted 1 times

🗨️ 👤 **Alcpt** 7 months, 3 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** 1 year, 2 months ago

Administrator accounts can't use security questions as verification method with SSPR.

upvoted 1 times

🗨️ 👤 **Trappie** 1 year, 2 months ago

Correct:

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-security-questions>

upvoted 1 times



You have an Azure AD tenant.

You need to implement smart logout 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%)

 **Obyte** Highly Voted 1 year, 2 months ago

**Selected Answer: B**

Correct answer.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-logout#manage-microsoft-entra-smart-logout-values>

upvoted 6 times

 **Siraf** Most Recent 12 months ago

Correct Answer is B

upvoted 1 times

 **e1ec325** 1 year, 2 months ago

**Selected Answer: B**

Correct

upvoted 1 times

You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.

You need to ensure that you can control access to Microsoft 365 resources by using conditional access policies.

What should you do first?

- A. Disable Security defaults.
- B. Configure password protection for the Azure AD tenant.
- C. Configure a multi-factor authentication (MFA) registration policy.
- D. Disable the User consent settings.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **59e8fdb** 4 months ago

**Selected Answer: A**

A is correct, if you want to use Conditional Access Policies you first must disable the Entra security defaults  
upvoted 1 times

🗳️ 👤 **Siraf** 12 months ago

Answer is A  
upvoted 2 times

🗳️ 👤 **JimboJones99** 1 year, 2 months ago

**Selected Answer: A**

Correct as the tenant is new and security defaults will be on by default.  
upvoted 3 times

You have a Microsoft 365 tenant.

An on-premises Active Directory domain is configured to sync with the Azure AD tenant. The domain contains the servers shown in the following table.

| Name    | Operating system    | Configuration     |
|---------|---------------------|-------------------|
| Server1 | Windows Server 2019 | Domain controller |
| Server2 | Windows Server 2016 | Domain controller |
| Server3 | Windows Server 2019 | Azure AD Connect  |

The domain controllers are prevented from communicating to the internet.

You implement Azure AD Password Protection on Server1 and Server2.

You deploy a new server named Server4 that runs Windows Server 2022.

You need to ensure that Azure AD Password Protection will continue to work if a single server fails.

What should you implement on Server4?

- A. Azure AD Connect
- B. Azure AD Application Proxy
- C. Password Change Notification Service (PCNS)
- D. the Azure AD Password Protection proxy service

**Suggested Answer: D**

Community vote distribution

D (100%)

 **csi\_2025** 4 months ago

**Selected Answer: D**

I am confused, isn't Server 3 and 4 both SPoF and to satisfy the question that it still works after a single Server fails wouldn't you need to make both redundant?


upvoted 1 times

 **Sozo** 10 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** 1 year, 2 months 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** 1 year, 2 months ago

**Selected Answer: D**

Answer is correct.

upvoted 3 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. voice
- B. email
- C. security questions
- D. a verification code from the Microsoft Authenticator app

**Suggested Answer:** D

Community vote distribution

D (100%)

🗲️ 👤 **NickGhouse** 7 months ago

**Selected Answer: D**

Ahh.. we meet again  
upvoted 3 times

🗲️ 👤 **GummyBear95** 9 months, 2 weeks ago

**Selected Answer: D**

Same as all the others  
upvoted 1 times

🗲️ 👤 **Robin\_Cegeka** 1 year, 2 months 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, 8 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

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** Highly Voted 6 months 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 5 times

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

**Selected Answer: C**

To enable Microsoft Entra Private Access, you must first configure and enable a Private Access profile, which is managed under the Security profiles blade in the Microsoft Entra admin center.

Steps to enable Private Access:

Go to the Microsoft Entra admin center.

Navigate to Global Secure Access.

Select Security profiles.

Configure and enable the Private Access profile.

This ensures that Microsoft Entra Private Access can securely publish on-premises applications without requiring a traditional VPN.

upvoted 3 times

 **YesPlease** 4 months ago

**Selected Answer: B**

Answer B) Traffic Forwarding

<https://learn.microsoft.com/en-us/entra/global-secure-access/concept-traffic-forwarding#private-access>

upvoted 2 times

## HOTSPOT

-

You have an Azure subscription that contains the resources shown in the following table.

| Name   | Type            |
|--------|-----------------|
| User1  | User            |
| User2  | User            |
| Vault1 | Azure Key Vault |

You need to configure access to Vault1. The solution must meet the following requirements:

- Ensure that User1 can manage and create keys in Vault1.
- Ensure that User2 can access a certificate stored in Vault1.
- Use the principle of least privilege.

Which role should you assign to each user? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User1:  ▼

- Key Vault Certificates Officer
- Key Vault Crypto Officer
- Key Vault Secrets Officer

User2:  ▼

- Key Vault Certificates Officer
- Key Vault Crypto Officer
- Key Vault Secrets Officer

**Answer Area****Suggested Answer:**

User1:  ▼

- Key Vault Certificates Officer
- Key Vault Crypto Officer**
- Key Vault Secrets Officer

User2:  ▼

- Key Vault Certificates Officer**
- Key Vault Crypto Officer
- Key Vault Secrets Officer

🗨️ 👤 **Siraf** Highly Voted 👍 12 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 6 times

 **penatuna** Most Recent 1 year, 2 months 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** 1 year, 2 months ago


Correct

upvoted 1 times

 **AK\_1234** 1 year, 2 months ago

- Key Vault Crypto Officer
- Key Vault Certificates Officer

upvoted 2 times

 **Julesy** 1 year, 2 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



You have an Azure AD tenant that has multi-factor authentication (MFA) enforced and self-service password reset (SSPR) enabled.

You enable combined registration in interrupt mode.

You create a new user named User1.

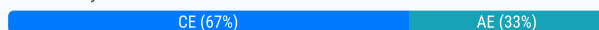
Which two authentication methods can User1 use to complete the combined registration process? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. a FIDO2 security key
- B. a hardware token
- C. a one-time passcode email
- D. Windows Hello for Business
- E. the Microsoft Authenticator app

**Suggested Answer:** CE

Community vote distribution



**penatuna** Highly Voted 1 year, 8 months ago

**Selected Answer:** CE

- A. FIDO2 security keys, can only be added in Manage mode. Question says "You enable combined registration in interrupt mode."
- B. Hardware token – You cannot register with hardware token.
- C. Email is supported.
- D. Windows Hello for Business is not supported.
- E. Microsoft Authenticator app is supported.

upvoted 14 times

**Alcpt** 1 year ago

Passkey (FIDO2), can only be added in Manage mode on <https://aka.ms/mysecurityinfo>.

A is not an option in interrupt mode

upvoted 1 times

**Nyamnyam** Highly Voted 1 year, 7 months ago

AE is NOT correct. CE is the only possibility. Why?

- A. FIDO2 security keys, can only be added in Manage mode
- B. Hardware tokens cannot be used in combined registration.
- D. Windows Hello for business cannot be used in combined registration. In fact, this is a passwordless authentication platform (with PIN and biometric methods)

Read the table and the Notes sections here:

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-registration-mfa-sspr-combined#methods-available-in-combined-registration>

upvoted 6 times

**Labelfree** Most Recent 7 months, 2 weeks ago

**Selected Answer:** CE


E. is given, C. is only other option since a OTP (One Time Passcode) is generated from Email.

FIDO2 is supported for Combined Registration Mode, but not for Interrupt mode. Reference this doc about 2/5 to 1/2 way down:

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-registration-mfa-sspr-combined>

Reference

upvoted 2 times



  **methosgr** 10 months, 3 weeks ago

**Selected Answer: AE**

Methods available in combined registration

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-registration-mfa-sspr-combined>

upvoted 1 times

  **Labelfree** 7 months, 2 weeks ago

Correct article, but wrong answer. If you scroll down a little further of where you found that answer (you are looking at combined, but not interrupt specifically), then you'll see this comment for interrupt -



When the user chooses to register, two methods are required:

The user is shown Microsoft Authenticator app and phone by default.

The user can choose to register email instead of Authenticator app or phone.

So, aside from the given E/Authenticator app, has to be C. OTP (generated from email)

upvoted 2 times

  **psp65** 1 month, 1 week ago

I see in the article that A,C,E are all correct now...

upvoted 1 times

  **a6792d4** 1 year, 1 month ago

<https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr>

Choose the Methods available to users that your organization wants to allow. For this tutorial, check the boxes to enable the following methods:

Mobile app notification

Mobile app code

Email

Mobile phone

upvoted 1 times

  **curtmcgirt** 1 year, 6 months ago

redundant comment, just voting to correct the distribution:

Read the table and the Notes sections here:

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-registration-mfa-sspr-combined#methods-available-in-combined-registration>

upvoted 2 times


  **JCKD4Ni3L** 1 year, 8 months ago

**Selected Answer: AE**

As per Microsoft's documentation, A and E in the available choices.

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-registration-mfa-sspr-combined#methods-available-in-combined-registration>

upvoted 1 times

  **JCKD4Ni3L** 1 year, 8 months ago

I stand corrected, A is not valid, as stated by others, FIDO2 security keys, can only be added in Manage mode on <https://aka.ms/mysecurityinfo>.

So correct Answer would be C & E.

upvoted 2 times

  **syounun200x** 1 year, 8 months ago

I think the answer C & E is correct.

On the link page, it goes like this.

FIDO2 security keys, can only be added in Manage mode on <https://aka.ms/mysecurityinfo>.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-registration-mfa-sspr-combined>

Meaning I think through the combined registration process the user cannot choose FIDO2 but only on their own 365 security page.

upvoted 4 times

🗨️ 👤 **cgonIT** 1 year, 8 months ago

As per the official documentation: <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-registration-mfa-sspr-combined>

- Hardware token is not an option to register.
- a one-time passcode email is not even listed.
- Windows Hello for Business is not even listed.

Correct responses:

- A. a FIDO2 security key
- E. the Microsoft Authenticator app

upvoted 3 times

🗨️ 👤 **curtmcgirt** 1 year, 6 months ago

as per the link you provided: the exact words "one time passcode email" are not listed, but "email" definitely is. and right below the table that says "FIDO2 security keys: YES\*" (note the asterisk) there is a big purple box that says "\*FIDO2 security keys can only be added in Manage mode on <https://aka.ms/mysecurityinfo>."

CE

upvoted 1 times

🗨️ 👤 **JimboJones99** 1 year, 8 months ago

Agree with this based off the documentation

upvoted 1 times

🗨️ 👤 **666Forest** 1 year, 8 months ago

**Selected Answer: AE**

A. a FIDO2 security key: Users can use a FIDO2 security key, which is a hardware device that provides strong authentication, typically in the form of a USB key or a biometric-enabled key.

E. the Microsoft Authenticator app: Users can use the Microsoft Authenticator app, which supports multi-factor authentication (MFA) and can generate one-time passcodes or be used for push notifications for MFA approval.

So, User1 can use these two methods to complete the combined registration process.

upvoted 4 times

## DRAG DROP

-

You have an Azure AD tenant that contains a user named Admin1.

Admin1 uses the Require password change for high-risk users policy template to create a new Conditional Access policy.

Who is included and excluded by default in the policy assignment? To answer, drag the appropriate options to the correct target. Each option may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point

**Options**

Admin1

All guest and external users

All users

Directory roles

None

**Answer Area**


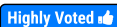
Include:

Exclude:

**Suggested Answer:****Answer Area**

Include: All users

Exclude: None

 **penatuna**  1 year, 8 months ago

Include: All users

Exclude: Admin1

These are the settings for the Require Password Change for High-Risk Users template:

Users: All Users are Included – The current user creating the policy will be excluded

Apps: All apps

User Risk: Risk levels: High

Access Control: Grant access – Require multifactor authentication AND Require password change

Conditional Access template policies will exclude only the user creating the policy from the template. If your organization needs to exclude other accounts, you will be able to modify the policy once they are created. You can find these policies in the Microsoft Entra admin center > Protection > Conditional Access > Policies. Select a policy to open the editor and modify the excluded users and groups to select accounts you want to exclude.

<https://sccmentor.com/2023/03/26/just-dropped-in-to-see-what-condition-my-conditional-access-rule-was-in-part-6-require-password-change-for-high-risk-users/>

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policy-common?tabs=zero-trust#template-categories>

upvoted 30 times

 **Nyamnyam** 1 year, 7 months ago

Nice catch!

upvoted 1 times

  **Kmkz83510** 1 year, 6 months ago

This is correct. Viewing the template shows Included: All users, Excluded: Current user (which is Admin1)

upvoted 2 times

  **cgonIT**  1 year, 8 months ago

Wrong answer.


Include: All Users

Exclude: Current User (Admin1 in this case)

Tested in lab.

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

upvoted 7 times

  **agittunc** 1 year, 8 months ago

This is wrong, your link also doesn't say admin is excluded.

All users

guest/external as they are not managed by the specific tenant.

upvoted 2 times

  **emartiy** 1 year, 3 months ago

Current user which is creating policy is excluded mean Admin1 who is performing operation :)

upvoted 2 times

  **d1e85d9**  3 months, 2 weeks ago

Include: All Users

Exclude: Admin1 (current user, which is already inside all users)

upvoted 1 times

  **criminal1979** 11 months, 3 weeks ago

Just tested. Include: All Users, Exclude: Current User

upvoted 1 times

  **RemmyT** 1 year ago

Include: None

Exclude: None

The default settings when creating any new CA policy:

Users

0 users and groups selected

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.

Include

- None : default

- All users

- Select users and groups

Exclude

Select the users and groups to exempt from the policy

- Guest or external users : Unchecked

- Directory roles : Unchecked

- Users and groups : Unchecked

Policy can be enforced with "Enable policy".

upvoted 1 times

  **Peeeedor** 1 year, 8 months ago

- All users
- All guest and external users

My thinking:

The reason for excluding these is because they login with external credentials! We do not manage their identity and therefore cannot enforce a PW reset?

Also in the real world I would exclude the breakglass account also (as mentioned in ms documentation)

upvoted 1 times

🗨️ 👤 **AK\_1234** 1 year, 8 months ago

- All users
- All guest and external users

upvoted 2 times

🗨️ 👤 **F\_Dias** 1 year, 8 months ago

The correct is:

Include: All Users

Exclude: Current User (Admin1 in this example)

upvoted 4 times

🗨️ 👤 **DasChi\_cken** 1 year, 8 months ago

All User & none... Microsoft even warns you in their Docs to Test CAPs in Report only Mode before you Lock yourself Out

And logically If you say all User in the First place you cant say anything Else the none as 2nd answer because the First answer wouldnt be all the ;)

upvoted 3 times

🗨️ 👤 **AK\_1234** 1 year, 8 months ago

- All users
- All guest and external users

upvoted 1 times

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptops to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).


Which MFA authentication method can the users use from the remote location?

- A. SMS
- B. Windows Hello for Business
- C. voice
- D. a notification through the Microsoft Authenticator app

**Suggested Answer: B**

*Community vote distribution*

B (100%)

  **JCKD4Ni3L** 1 year, 2 months ago

**Selected Answer: B**

B is correct.



upvoted 2 times

  **ANIMOSITYOP** 10 months ago

Windows Hello for Business is an enterprise-grade biometric verification mechanism available in Windows 10. It uses facial recognition or fingerprint scan to authenticate users, thus providing a high level of security without the need for Wi-Fi access or mobile phone connectivity.

On the other hand, options like SMS, voice and a notification through the Microsoft Authenticator app would require either a mobile connectivity or an internet connection on the mobile device, which is stated not to be available in the remote locations in the question. Therefore, Windows Hello for Business would be the most suitable method in this case.

upvoted 2 times

  **cgonIT** 1 year, 2 months ago

B. Windows Hello for Business.

It's the only option when no internet connectivity or access to a mobile phone device.

upvoted 2 times

DRAG DROP -

You have a Microsoft 365 E5 subscription. The subscription contains 500 devices that run Windows.

You deploy the Global Secure Access client to the devices.

You need to prevent users from accessing <https://contoso.com> from the devices.

Which three actions should you perform in sequence? To answer move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

#### Actions

- Create an app protection policy.
- Create a Conditional Access policy.
- Create a remote network.
- Configure a security profile.
- Create a web content filtering policy.

#### Answer Area

**Correct Answer:**

| Actions                                | Answer Area |
|----------------------------------------|-------------|
| Create an app protection policy.       |             |
| Create a Conditional Access policy.    |             |
| Create a remote network.               |             |
| Configure a security profile.          |             |
| Create a web content filtering policy. |             |

👤 **YesPlease** 4 months ago

Answer is Correct..

High Level Steps to configure web content filtering:

- Step 1) Enable internet traffic forwarding.
- Step 2) Create a web content filtering policy.
- Step 3) Create a security profile.
- Step 4) Link the security profile to a Conditional Access policy.
- Step 5) Assign users or groups to the traffic forwarding profile.

<https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-configure-web-content-filtering#high-level-steps>

upvoted 1 times

👤 **armid** 4 months, 2 weeks ago

answer is correct

upvoted 3 times



You have a Microsoft 365 tenant.

You currently allow email clients that use Basic authentication to connect to Microsoft Exchange Online.

You need to ensure that users can connect to Exchange Online only from email clients that use Modern authentication protocols.

What should you implement?

- A. a conditional access policy in Azure AD
- B. a compliance policy in Microsoft Intune
- C. an OAuth policy in Microsoft Defender for Cloud Apps
- D. an application control profile in Microsoft Intune

**Suggested Answer: D**

*Community vote distribution*

A (100%)

🗳️ **thetootall** 11 months, 2 weeks ago

**Selected Answer: A**

To "enforce Modern authentication protocols" we need to use a Conditional Access policy.  
upvoted 1 times

🗳️ **Nyamnyam** 1 year, 7 months ago

**Selected Answer: A**

Exactly. A. And in the previous occurrence, we clarified that "app control" is for approved apps. This will not block basic auth from, e.g. personal computers ;)  
upvoted 3 times

🗳️ **Obyte** 1 year, 8 months ago

**Selected Answer: A**

Agree. A is the correct answer

<https://learn.microsoft.com/en-gb/entra/identity/conditional-access/howto-conditional-access-policy-block-legacy>

upvoted 4 times

🗳️ **JCKD4Ni3L** 1 year, 8 months ago

**Selected Answer: A**

A, Conditional Access Policy that blocks Legacy Authentication Clients apps (Exchange ActiveSync and Other clients).  
upvoted 2 times

🗳️ **JimboJones99** 1 year, 8 months ago

**Selected Answer: A**

a conditional access policy in Azure AD  
upvoted 2 times

🗳️ **DasChi\_cken** 1 year, 8 months ago

**Selected Answer: A**

Should be A, this question was mentioned a couple of questions before as well  
upvoted 3 times

🗳️ **666Forest** 1 year, 8 months ago

**Selected Answer: A**

The correct answer is A  
upvoted 1 times

🗳️ **shuhaidawahab** 1 year, 8 months ago

The correct answer is A. a conditional access policy in Azure AD.

upvoted 1 times

You plan to deploy a new Azure AD tenant.

Which multifactor authentication (MFA) method will be enabled by default for the tenant?

- A. Microsoft Authenticator
- B. SMS
- C. voice call
- D. email OTP

**Suggested Answer: A**

*Community vote distribution*

A (100%)

penatuna  8 months ago

**Selected Answer: A**

It's a new Azure tenant, so security defaults are enabled. With security defaults, Microsoft Authenticator is the default authentication method.

"Security defaults users are required to register for and use multifactor authentication using the Microsoft Authenticator app using notifications. Users might use verification codes from the Microsoft Authenticator app but can only register using the notification option. Users can also use any third party application using OATH TOTP to generate codes."

<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#authentication-methods>

upvoted 7 times

59e8fdb  4 months ago

**Selected Answer: A**

Correct answer!

upvoted 1 times

iduard15 7 months, 2 weeks ago

D, OTP email

upvoted 1 times

JCKD4Ni3L 8 months, 1 week ago

**Selected Answer: A**

Security Defaults are usually turned on on new tenants, therefore Microsoft Authenticator is the correct Answer.

upvoted 2 times

rikicm 8 months, 3 weeks ago

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

upvoted 1 times

## HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

| Name  | Member of      |
|-------|----------------|
| User1 | Group1         |
| User2 | Group2         |
| User3 | Group1, Group2 |

The users have the devices shown in the following table.

| Name    | Platform   | Azure AD join type  |
|---------|------------|---------------------|
| Device1 | Windows 11 | None                |
| Device2 | Windows 10 | Azure AD joined     |
| Device3 | Android    | Azure AD registered |

You create the following two Conditional Access policies:

- Name: CAPolicy1
- Assignments
  - o Users or workload identities: Group1
  - o Cloud apps or actions: Office 365 SharePoint Online
  - o Conditions
    - Filter for devices: Exclude filtered devices from the policy
    - Rule syntax: device.displayName -startsWith "Device"
  - o Access controls
    - Grant: Block access
    - Session: 0 controls selected
  - o Enable policy: On

- Name: CAPolicy2
- Assignments
  - o Users or workload identities: Group2
  - o Cloud apps or actions: Office 365 SharePoint Online
  - o Conditions: 0 conditions selected
  - Access controls
    - o Grant: Grant access
    - Require multifactor authentication
    - o Session: 0 controls selected
  - Enable policy: On

All users confirm that they can successfully authenticate using MFA.

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

NOTE: Each correct selection is worth one point.

| Statements                           | Yes                   | No                    |
|--------------------------------------|-----------------------|-----------------------|
| User1 can access Site1 from Device1. | <input type="radio"/> | <input type="radio"/> |
| User2 can access Site1 from Device2. | <input type="radio"/> | <input type="radio"/> |
| User3 can access Site1 from Device3. | <input type="radio"/> | <input type="radio"/> |



| Suggested Answer: | Statements                           | Yes                              | No                               |
|-------------------|--------------------------------------|----------------------------------|----------------------------------|
|                   | User1 can access Site1 from Device1. | <input type="radio"/>            | <input checked="" type="radio"/> |
|                   | User2 can access Site1 from Device2. | <input checked="" type="radio"/> | <input type="radio"/>            |
|                   | User3 can access Site1 from Device3. | <input type="radio"/>            | <input checked="" type="radio"/> |

  **vaaws** Highly Voted 1 year, 8 months ago

Azure Conditional Access policies can only apply to devices that are registered or joined in Azure Active Directory. If a device is not registered or joined, the policy will not be able to read the device name.

N Y Y

upvoted 17 times

  **Alcpt** 1 year, 1 month ago

Wrong reason.

Microsoft Entra ID uses device authentication to evaluate device filter rules. For a device that is unregistered with Microsoft Entra ID, all device properties are considered as null values and the device attributes cannot be determined since the device does not exist in the directory. The best way to target policies for unregistered devices is by using the negative operator since the configured filter rule would apply. If you were to use a positive operator, the filter rule would only apply when a device exists in the directory and the configured rule matches the attribute on the device.

upvoted 2 times



  **Ody** 1 year, 4 months ago

I agree.

For a device that is unregistered with Microsoft Entra ID, all device properties are considered as null values and the device attributes cannot be determined since the device does not exist in the directory. The best way to target policies for unregistered devices is by using the negative operator since the configured filter rule would apply. If you were to use a positive operator, the filter rule would only apply when a device exists in the directory and the configured rule matches the attribute on the device.



<https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-condition-filters-for-devices>

upvoted 4 times

  **Florian74** Highly Voted 1 year, 8 months ago


If the CAPolicy1 included the filtered devices it would be YNY. But the policy excludes them. So YYY for me

upvoted 10 times

  **Saynot** 1 year, 4 months ago

If the device isn't registered at least, conditional access policy filter can't evaluate the name, so for me it is NYY

upvoted 5 times

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

User1 is in Group1 only.

Policy1 would block access for Group1 users if they used a device not excluded, but since all "Device\*" machines are excluded, User1 is not blocked and can access SharePoint Online from any of those devices.

User2 is in Group2 only.

Only Policy2 applies, requiring MFA. User2 confirms MFA is working, so User2 can access Site1 from any device, including Device2.



User3 is in Group1 and Group2.

Policy1 does not apply because Device3 is excluded by name.

Policy2 requires MFA, which User3 can do.

Therefore, User3 can also access Site1 from Device3.

upvoted 2 times

  **Frank9020** 5 months ago

User1 ✖ No Blocked by CAPolicy1 (not excluded).

User2 ✔ Yes Allowed via CAPolicy2 (MFA required).

User3 ✔ Yes Excluded from CAPolicy1, so only CAPolicy2 applies (MFA required).

In Conditional Access, exclusions override inclusions, meaning an excluded user/device is not affected by the policy!

upvoted 1 times

  **Sunth65** 5 months ago

NB! Filter for devices: Exclude filtered devices from the policy !

upvoted 1 times


  **Sunth65** 5 months ago

Name: CAPolicy1

Filter for devices: Exclude filtered devices from the policy

Rule syntax: device.displayName -startsWith "Device"

upvoted 1 times

  **Frank9020** 4 months, 3 weeks ago

You cannot use CA Policy filter for a device that is not registered in AD. Device1 is not registered in Azure AD, that is why User1 is blocked by the policy, cause the filter will not recognize an unregistered device.

upvoted 2 times

  **Nail** 8 months, 1 week ago

Let's take this one user at a time.

User1: Tries to access Site1. They belong to Group1 so CAPolicy1 is applied. The CAP considers the device name null so the user is not excluded and the user is blocked. Answer: N

User2: Tries to access Site1. They belong to Group2 so CAPolicy2 is applied. They can access Site1 if they do MFA. Answer: Y

User3: Tries to access Site1. They belong to Group1 and Group2 so both CA policies are applied. CAPolicy1 reads the device name and excludes the user so they can access. CAPolicy2 is applied and allows the user to access if they do MFA. Answer: Y

Summary: NYY

upvoted 7 times

  **CubicTeach** 1 year, 1 month ago


First is NO since the device is not registered or joined, user 2 is yes, user 3 is yes, the policy says exclude any who's device name starts with "Device" .that my opinion i could be wrong but that's my answer .

upvoted 2 times

  **klayytech** 1 year, 2 months ago

Microsoft Entra ID uses device authentication to evaluate device filter rules. For a device that is unregistered with Microsoft Entra ID, all device properties are considered as null values and the device attributes cannot be determined since the device does not exist in the directory.

upvoted 1 times

  **Nielll** 1 year, 3 months ago

Device1 is not Azure AD joined and its name starts with "Device", so it's affected by CAPolicy1 which blocks access for Group1 members.

So, User1 cannot access Site1 from Device1. The answer is No.

Device2 is Azure AD joined and its name starts with "Device", so it's affected by CAPolicy1. However, User2 is not a member of Group1, so CAPolicy1 doesn't apply.

User2 is a member of Group2, and CAPolicy2 applies to Group2. CAPolicy2 grants access with MFA, and User2 can successfully authenticate using MFA.

So, User2 can access Site1 from Device2. The answer is Yes.

Device3 is Azure AD registered and its name starts with "Device", so it's affected by CAPolicy1 which blocks access for Group1 members. However, User3 is also a member of Group2, and CAPolicy2 applies to Group2. CAPolicy2 grants access with MFA, and User3 can successfully authenticate using MFA.

So, User3 can access Site1 from Device3. The answer is Yes.



No YES YES

upvoted 5 times

  **Sunth65** 5 months ago

NB! Filter for devices: Exclude filtered devices from the policy !

upvoted 1 times

  **Tony416** 9 months, 4 weeks ago

Great explanation. 100% agreed!

upvoted 1 times

  **Kmkz83510** 1 year, 6 months ago

I think most agree that it's ?YY. The debate is regarding the first one and whether the policy is applied because the device is not registered or joined. See here:

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-registration-mfa-sspr-combined#methods-available-in-combined-registration>

It appears to depend on the rule logic that is applied. In this case, since a 'positive' operator was used, the policy is not applied and therefore access should be granted. Therefore YYY.

upvoted 3 times

  **AleFerrillo** 1 year, 1 month ago

No, in this case the EXCLUSION is not applied and the policy blocks access (NYY)

upvoted 2 times

  **Sorrynotsorry** 1 year, 7 months ago

NYY. CAP1 can't read device1 name so will block access.

upvoted 2 times

  **Nyamnyam** 1 year, 7 months ago


YYY definitely. Consider this:

CAP1 is a blocking policy, but with Exclusion condition. This is very clear: any device from Group1 will be blocked, EXCEPT the ones starting with "Device". Haha, User1 and 3 are thus always allowed no matter the device join type or compliance state.

CAP2 is a simple MFA enforcement policy for Group2. User2 will be able to access the site (once he was registered for MFA) independent from what device (1,2,3) he accesses Site2.


Trust me, I work with CAPs in real life for years.

upvoted 7 times

  **Peeeedor** 1 year, 8 months ago

I am a little confused? How can user 1 be in group 1 and successfully using MFA while not being entra ID joined or registered?

upvoted 1 times

  **Nivos300** 1 year, 7 months ago

I agree with you .



In my opinion the answer is

N

Y

Y

upvoted 1 times

  **Obyte** 1 year, 8 months ago

Hmm... NYY for me



Here is my thinking - have to say haven't tested it yet :-)

User1 will be blocked because its device is neither AzureAD-joined nor Registered and device's name cannot be evaluated. The CAPolicy1 will block it.

User2 will be allowed as it doesn't fall under any of the two policies.

User3 will be excluded from blocking by CAPolicy1 (because of device name) and will be allowed by CAPolicy2 because of membership in Group2.

upvoted 1 times

  **JckD4Ni3L** 1 year, 8 months ago

YYY, as all devices are "excluded" from CAPolicy1, and since CAPolicy2 only triggers MFA, all users can access from any devices through MFA.

upvoted 3 times

  **JckD4Ni3L** 1 year, 8 months ago

Hmm since Device1 has no Azure AD joined/Registered state it cannot report it's name and will be blocked by CAPolicy1. I would there force state NYY.

upvoted 3 times

  **MarkElliott** 1 year, 8 months ago

Wrong, look at the Syntax rule, exclude device name that starts with Device.

Correct answer given

upvoted 1 times

  **MarkElliott** 1 year, 8 months ago

Infact just checked, it says exclude devices from the rule, so it is YYY

upvoted 2 times

  **Nail** 8 months, 1 week ago

It is not excluding devices from the rule, it is excluding devices that start with "Device". The CAP can't see the name of the device because it is null so the user is not excluded from the CAP. NYY


upvoted 1 times

  **DasChi\_cken** 1 year, 8 months ago

User1 and User3 are in group1 and there devicenames Starts with "Device" --- Access blocked

User2 IS in group2 and will only ne prompt to MFA

upvoted 1 times

  **Intrudire** 1 year, 8 months ago

Devices that start with "Device" are excluded from being blocked:

Filter for devices: Exclude filtered devices from the policy

Rule syntax: device.displayName -startsWith "Device"

upvoted 2 times

  **shuhaidawahab** 1 year, 8 months ago


Explanation:

User1 is a member of Group1, which is assigned to CAPolicy1. This policy blocks access to SharePoint Online for any device that starts with "Device". Since Device1 has this prefix, User1 cannot access Site1 from Device1.

User2 is a member of Group2, which is assigned to CAPolicy2. This policy grants access to SharePoint Online with MFA for any device. Since User2 has confirmed MFA, they can access Site1 from Device2.

User3 is not a member of any group that is assigned to a Conditional Access policy. Therefore, they have the default access level to SharePoint Online, which is none. User3 cannot access Site1 from Device3.

upvoted 1 times

  **cgonIT** 1 year, 8 months ago

At the very beginning I was telling N, N, N. But then I decided to test in lab.

- Created 2 AAD Security user groups.

- Created 3 users, and added to ech group.

- Created 2 Conditional Access.

Tested with WhatIf... and that's surprised me.

Y, Y, Y.

- User 1, no Conditional Access is detected to be applied.

- User 2 and 3, MFA will be required.



So all 3 are Yes.

upvoted 2 times

  **klayytech** 1 year, 2 months ago

Microsoft Entra ID uses device authentication to evaluate device filter rules. For a device that is unregistered with Microsoft Entra ID, all device properties are considered as null values and the device attributes cannot be determined since the device does not exist in the directory.

upvoted 1 times

  **agittunc** 1 year, 8 months ago

you do realize that device 1 isnt even AD joined right?

N, Y, Y

upvoted 2 times

You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3 and a Microsoft SharePoint Online site named Site1.

The subscription contains the devices shown in the following table.

| Name    | Azure AD   | Compliance     |
|---------|------------|----------------|
| Device1 | Joined     | Noncompliant   |
| Device2 | Registered | Compliant      |
| Device3 | None       | Not applicable |

The users sign in to the devices as shown in the following table.

| User  | Device  |
|-------|---------|
| User1 | Device1 |
| User2 | Device2 |
| User3 | Device3 |

You have a Conditional Access policy that has the following settings:

- Name: CA1
- Assignments
  - o Users and groups: User1, User2, User3
  - o Cloud apps or actions: SharePoint - Site1
- Access controls
  - o Session: Use app enforced restrictions

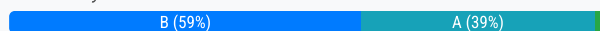
From the SharePoint admin center, you configure Access control for unmanaged devices to allow limited, web-only access.

Which users will have full access to Site1?

- A. User1 only
- B. User2 only
- C. User3only
- D. User1 and User2 only
- E. User1, User2, and User3

**Suggested Answer: B**

Community vote distribution



**vaaws** Highly Voted 1 year, 8 months ago

The users who will have full access to Site1 are User1 and User2 only. The Conditional Access policy is configured to include User1, User2, and User3, but the Access control for unmanaged devices in the SharePoint admin center allows only limited, web-only access. Therefore, only User1 and User2, who sign in from managed devices, will have full access to Site1.

The correct answer is D. User1 and User2 only.

upvoted 22 times

**Oskarma** 4 months, 3 weeks ago

I think vaaws is right.

A managed device can be registered of joined, and in the question is not said anything about compliant or not.



upvoted 4 times

**jlbrandes** Highly Voted 1 year, 7 months ago

**Selected Answer: A**

Only Joined devices are managed.

<https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-managed-unmanaged-devices?view=o365-worldwide&tabs=Managed>  
upvoted 17 times

  **Phil\_79** 6 days, 11 hours ago

Android devices managed by Intune are Registered. Joined is only for Windows Device. Here we have a compliance status for the registered device and the compliance is only evaluated by Intune... so the device is managed.

upvoted 1 times

  **armid** 4 months, 2 weeks ago

nope. The article you linked says this (and check the second bullet point/paragraph)

For their part in protecting managed devices, users can:

Use the Microsoft Authenticator app to sign in. The Microsoft Authenticator app works with all accounts that use multi-factor authentication (MFA). To learn more, see Download and install the Microsoft Authenticator app.

Join their devices to your organization's network. Users can follow a process to register their device, set up MFA, and complete the sign-in process using their account. To learn more, see Join your work device to your work or school network.

Make sure antivirus/antimalware software is installed and up to date on all devices. Once devices are onboarded, antivirus, antimalware, and other threat protection capabilities are configured for those devices. Users are prompted to install updates as they come in. To learn more, see See Keep your PC up to date.

upvoted 1 times

  **csi\_2025** 4 months ago

It's been a while since I did this but if you follow the link in the segment you mean it shows instructions which join your device, not register it.

Secondly we don't have information if the Device2 is company or privately owned since you can add register private devices too so I would default and say that Device2 is a private device and therefore does not get full access.

upvoted 1 times

  **Shaon** **Most Recent** 1 week, 3 days ago

**Selected Answer: D**

User 1 and User 2 can access Site 1 as their devices are managed by the org

upvoted 1 times

  **csi\_2025** 4 months ago

**Selected Answer: A**

Tbh we are not given enough information. According to this <https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices> devices which are not hybrid AD joined or not compliant in Intune are declared unmanaged.

We know it's a joined device but not a hybrid AD joined one -> we could assume that any type of joined device would be allowed

We know that the devices are (not) compliant but we don't know if they use Intune, the compliance state could be from Entra ID.

Therefore I stay with A unless someone can prove otherwise.

upvoted 1 times

  **YesPlease** 4 months ago

**Selected Answer: A**

Answer a) User1 will get FULL ACCESS

"Use app enforced restrictions" limits access on UNMANAGED devices. Just cause Device1 is "noncompliant" doesn't mean that they are being blocked from accessing the SharePoint site.

Device2 and Device3 are not managed devices and will not be able to get full access to the site.

upvoted 1 times

  **59e8fdb** 4 months ago

**Selected Answer: B**

Given answer is correct. Only compliant device/Entra joined device. Not compliant devices are considered unmanaged devices!

upvoted 1 times

  **Frank9020** 5 months, 1 week ago

**Selected Answer: B**

Only User2 is using a device that meets the conditions for full access (Azure AD registered and compliant). Both User1 and User3 are restricted to web-only access because their devices are either noncompliant or unmanaged.

upvoted 3 times

🗨️ 👤 **Grg433** 5 months, 2 weeks ago

**Selected Answer: B**

User Analysis:

User1 (using Device1, non-compliant):

Since the device is Azure AD joined but non-compliant, it is considered unmanaged. Therefore, User1 will have limited, web-only access to Site1.  
User2 (using Device2, compliant):

The device is Azure AD registered and compliant, which qualifies it as a managed device. Thus, User2 will have full access to Site1.  
User3 (using Device3, not Azure AD joined, compliance not applicable):

Since the device is not Azure AD joined and compliance is not applicable, it is considered unmanaged. Therefore, User3 will have limited, web-only access to Site1.

Conclusion:

Only User2 will have full access to Site1 because they are using a compliant, Azure AD registered device.

upvoted 2 times

🗨️ 👤 **Matt19** 6 months, 1 week ago

**Selected Answer: A**

Entra Joined devices are considered to be managed devices so - A

upvoted 1 times

🗨️ 👤 **Matt19** 6 months, 2 weeks ago

**Selected Answer: B**

B is correct, need a Joined device.

upvoted 3 times

🗨️ 👤 **Matt19** 6 months, 1 week ago

correction - I meant A as option A is Entra Joined

upvoted 1 times

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

**Selected Answer: B**

The key here is the compliancy status.

"you can block or limit access to SharePoint and OneDrive content from unmanaged devices (those not hybrid AD joined or compliant in Intune)" so any compliant device is considered Managed and any non-compliant is considered Unmanaged.

upvoted 8 times

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

**Selected Answer: B**

I thinks its B also.

upvoted 5 times

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

**Selected Answer: A**

<https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-managed-unmanaged-devices?view=o365-worldwide&tabs=Managed>

upvoted 1 times

🗨️ 👤 **HartMS** 1 year, 3 months ago

Option B: User2 Only

User 1 will have full access. Since this policy restricts the access for unmanaged devices.

Joined = Managed

Registered = Unmanaged

The compliance does not matter since "Device requires to be marked as Compliant" is not a criteria here.

upvoted 3 times

🗨️ 👤 **HartMS** 1 year, 3 months ago

Correcting myself: Option A: User 1 Only

upvoted 3 times

🗨️ 👤 **[Removed]** 1 year, 3 months ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

As a SharePoint Administrator or Global Administrator in Microsoft 365, you can block or limit access to SharePoint and OneDrive content from unmanaged devices (those not hybrid AD joined or compliant in Intune).

upvoted 4 times

🗨️ 👤 **[Removed]** 1 year, 3 months ago

Correct answer is definitely B:

<https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

As a SharePoint Administrator or Global Administrator in Microsoft 365, you can block or limit access to SharePoint and OneDrive content from unmanaged devices (those not hybrid AD joined or compliant in Intune).

upvoted 3 times

🗨️ 👤 **belyo** 1 year, 3 months ago

**Selected Answer: B**

User1 is using Device1, which is joined but non-compliant. Since the device is non-compliant, User1 will have limited, web-only access to Site1 due to the SharePoint Access control settings.

upvoted 5 times

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

| Name      | Description               |
|-----------|---------------------------|
| Au1       | Administrative unit       |
| CAPolicy1 | Conditional Access policy |
| Package1  | Access package            |

You create a user named Admin1.

You need to ensure that Admin1 can enable Security defaults for contoso.com.

What should you do first?

- A. Delete Package1.
- B. Delete CAPolicy1.
- C. Assign Admin1 the Authentication Administrator role for Au1.
- D. Configure Identity Governance.

**Suggested Answer: B**

Community vote distribution

B (100%)

 **YesPlease** 4 months ago

**Selected Answer: B**

Answer B) Delete CAPolicy1

To use Conditional Policies, you must first disable "security defaults". So to use the security defaults again, you will need to remove Conditional Access Policies that may conflict.

Of all the choices provided, this is the one that makes the most sense.

upvoted 2 times

 **OrangeSG** 7 months, 2 weeks ago


**Selected Answer: B**

To configure security defaults in your directory, you must be assigned at least the Security Administrator role. By default the first account in any directory is assigned a higher privileged role known as Global Administrator.

Organizations that choose to implement Conditional Access policies that replace security defaults must disable security defaults. (Imply that Conditional Access policies has conflict with security defaults)

<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>

upvoted 1 times

 **[Removed]** 8 months, 1 week ago

Answer: B is correct.

DumpsOwner : The study material that I have used has been excellent. It is well-written, organized, and informative. The material covers all of the topics that I need to know in a comprehensive and easy-to-understand way.

upvoted 1 times

 **JCKD4Ni3L** 8 months, 1 week ago

**Selected Answer: B**

B is Correct.

upvoted 1 times

 **DasChi\_cken** 8 months, 2 weeks ago

**Selected Answer: B**

To enable capolicies you need to disable Security defaults therefore you need to do it viceversa If you want to Go back to Security defaults  
upvoted 2 times

  **shuhaidawahab** 8 months, 3 weeks ago

The correct answer is B. Delete CAPolicy1.

To enable Security defaults for contoso.com, Admin1 must be assigned at least the Security Administrator role<sup>1</sup>. However, this role is not available in the list of roles for Au1, which is the only authentication method for contoso.com. This is because Au1 has a Conditional Access policy named CAPolicy1 that blocks legacy authentication protocols<sup>2</sup>. Security defaults also block legacy authentication protocols, so they cannot be enabled if there is an existing Conditional Access policy that does the same<sup>3</sup>.

Therefore, to enable Security defaults, Admin1 must first delete CAPolicy1 from Au1. This will allow Admin1 to sign in to contoso.com using a legacy authentication protocol and then assign themselves the Security Administrator role. After that, Admin1 can enable Security defaults for contoso.com.  
upvoted 1 times

  **cgonIT** 8 months, 3 weeks ago

**Selected Answer: B**

A. Delete Package1 --> no sense for me.

C. Assign Admin1 the Authentication Administrator role for Au1. --> The role needed on that case, is Security Administrator role.

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/security-defaults#enabling-security-defaults>

D. Configure Identity Governance. --> no sense for me.

So B. Delete CAPolicy1 is the correct one.

upvoted 1 times

  **LC\_90** 9 months ago

**Selected Answer: B**

Correct

upvoted 2 times

## DRAG DROP

-

You have an Azure subscription that is linked to an Azure AD tenant named contoso.com. The subscription contains a group named Group1 and a virtual machine named VM1.

You need to meet the following requirements:

- Enable a system-assigned managed identity for VM1.
- Add VM1 to Group1.

How should you complete the PowerShell script? To answer, drag the appropriate cmdlets to the correct targets. Each cmdlet may be used once, more than once or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

## Cmdlets

Get-AzADGroup

Get-AzADServicePrincipal

Get-AzVM

Update-AzADServicePrincipal

Update-AzVM

## Answer Area

```
$vm = [Cmdlet] -ResourceGroupName myResourceGroup -Name vm1
Update-AzVM -ResourceGroupName myResourceGroup -VM $vm -IdentityType SystemAssigned
$displayname = [Cmdlet] -displayname "vm1"
$group = Get-AzADGroup -searchstring "group1"
Add-AzureADGroupMember -ObjectId $group.id -RefObjectId $displayname.id
```

## Answer Area


```
$vm = Get-AzVM -ResourceGroupName myResourceGroup -Name vm1
Update-AzVM -ResourceGroupName myResourceGroup -VM $vm -IdentityType SystemAssigned
$displayname = Get-AzADServicePrincipal -displayname "vm1"
$group = Get-AzADGroup -searchstring "group1"
Add-AzureADGroupMember -ObjectId $group.id -RefObjectId $displayname.id
```

## Suggested Answer:

 **cgonIT**  1 year, 2 months ago

Seems to be correct.

- Get-AzVM  
- Get-AzADServicePrincipal  
upvoted 7 times


 **penatuna**  9 months, 1 week ago

Enable system-assigned managed identity on an existing Azure VM:

1. Retrieve the VM properties using the Get-AzVM cmdlet. Then to enable a system-assigned managed identity, use the -IdentityType switch on the Update-AzVM cmdlet:

```
$vm = Get-AzVM -ResourceGroupName myResourceGroup -Name vm1
Update-AzVM -ResourceGroupName myResourceGroup -VM $vm -IdentityType SystemAssigned
```

upvoted 3 times

 **penatuna** 9 months, 1 week ago

Add VM system assigned identity to a group:

After you have enabled system assigned identity on a VM, you can add it to a group. The following procedure adds a VM's system assigned identity to a group.

1. Retrieve and note the ObjectID (as specified in the Id field of the returned values) of the VM's service principal:



```
$displayname = Get-AzADServicePrincipal -displayname "vm1"
```

2. Retrieve and note the ObjectID (as specified in the Id field of the returned values) of the group:

```
$group Get-AzADGroup -searchstring "group1"
```

3. Add the VM's service principal to the group:

```
Add-AzureADGroupMember -ObjectId $group.id -RefObjectId $displayname.id
```



<https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/qs-configure-powershell-windows-vm#system-assigned-managed-identity>

upvoted 2 times

  **Studytime2023** 1 year ago

Correct. <https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/qs-configure-powershell-windows-vm>

upvoted 3 times

  **DasChi\_cken** 1 year, 2 months ago

Its correct, you want to save the Powershell objects in a variable first and Last step is Putting all things together

upvoted 2 times

You have an Azure AD tenant.

You deploy a new enterprise application named App1.

When users attempt to provide App1 with access to the tenant, the attempt fails.

You need to ensure that the users can request admin consent for App1. The solution must follow the principle of least privilege.


What should you do first?

- A. Enable admin consent requests for the tenant.
- B. Designate a reviewer of admin consent requests for the tenant.
- C. From the Permissions settings of App1, grant App1 admin consent for the tenant.
- D. Create a Conditional Access policy for App1.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **haazybanj** Highly Voted 1 year, 1 month ago

**Selected Answer: A**

To ensure that users can request admin consent for App1 in your Azure AD tenant, you should first enable admin consent requests for the tenant.

Enabling admin consent requests allows users to initiate the process of requesting admin consent for applications that require it. By default, users do not have the ability to grant admin consent for applications. Enabling this feature ensures that users can request admin consent for App1 without having to rely on an administrator to initiate the process.

upvoted 6 times

 **Jackdisuin** Most Recent 10 months ago

Correct Answer

upvoted 2 times

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

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

You have a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Azure Active Directory admin center, you configure the Block/unblock users settings for multi-factor authentication (MFA).

Does this meet the goal?


A. Yes

B. No

**Suggested Answer: B**

Community vote distribution

B (100%)


 **OrangeSG** 7 months, 2 weeks ago

**Selected Answer: B**

Report suspicious activity and the legacy Fraud Alert implementation can operate in parallel. You can keep your tenant-wide Fraud Alert functionality in place while you start to use Report suspicious activity with a targeted test group.

If Fraud Alert is enabled with Automatic Blocking, and Report suspicious activity is enabled, the user will be added to the blocklist and set as high-risk and in-scope for any other policies configured. These users will need to be removed from the blocklist and have their risk remediated to enable them to sign in with MFA.

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-mfasettings#report-suspicious-activity-and-fraud-alert>  
upvoted 1 times

 **haazybanj** 7 months, 3 weeks ago

**Selected Answer: B**

To meet the goal of automatically blocking users when they report an unauthorized MFA request, you would need to implement additional measures such as monitoring and alerting, conditional access policies, or security policies to detect and respond to suspicious MFA activity.


Therefore, the correct answer is B. No.  
upvoted 2 times

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1 and a Microsoft 365 group named Group1. You need to ensure that the members of Group1 can access Site1 for 90 days. The solution must minimize administrative effort.

What should you use?

- A. an access package
- B. an access review
- C. a lifecycle workflow
- D. a Conditional Access policy

**Suggested Answer: A**

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

A. an access package

For this scenario, an access package would be the most suitable. An access package in Azure Active Directory (Azure AD) entitlement management is a bundle of resources that you can give to users so they can access a set of related resources. They can be configured to expire after a certain amount of days (in this case 90 days), after which access to the resources is automatically revoked, saving administrative effort.

upvoted 7 times

 **AirSB** Most Recent 7 months ago

**Selected Answer: A**

To provide temporary access to Site1 for members of Group1 with minimal administrative effort, you can use an access package in Microsoft Entra Identity Governance. Access packages allow you to grant users access to resources (e.g., SharePoint sites, Microsoft 365 groups) for a specific duration, such as 90 days.

upvoted 1 times

 **Wazery** 1 year, 4 months ago

D. eine Richtlinie für bedingten Zugriff

Eine Richtlinie für bedingten Zugriff ermöglicht es Ihnen, den Zugriff auf SharePoint Online-Sites basierend auf bestimmten Bedingungen zu steuern, wie z. B. Standort, Gerät oder Netzwerkzugehörigkeit. In diesem Szenario können Sie eine bedingte Zugriffsrichtlinie erstellen, die sicherstellt, dass die Mitglieder der Gruppe Group1 für einen Zeitraum von 90 Tagen auf die SharePoint Online-Site Site1 zugreifen können. Diese Richtlinie würde den Verwaltungsaufwand minimieren, da sie automatisiert ist und die Zugriffssteuerung auf Gruppenebene vereinfacht.

upvoted 1 times

You have a Microsoft Entra tenant that contains the groups shown in the following table.

| Name   | Type          | Membership type |
|--------|---------------|-----------------|
| Group1 | Security      | Assigned        |
| Group2 | Security      | Dynamic         |
| Group3 | Microsoft 365 | Assigned        |
| Group4 | Microsoft 365 | Dynamic         |

You need to implement Privileged Identity Management (PIM) for the groups.

Which groups can be managed by using PIM?

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

**Suggested Answer: C**

Community vote distribution

C (100%)

 **a6792d4** Highly Voted 7 months, 2 weeks ago

Any Microsoft Entra security group and any Microsoft 365 group (except dynamic groups and groups synchronized from on-premises environment) can be enabled in PIM for Groups. So C.


upvoted 7 times

 **JanioHSilva** Most Recent 8 months, 3 weeks ago

**Selected Answer: C**

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

upvoted 3 times

 **Blakkaboy69** 8 months, 4 weeks ago

source

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

Groups in Microsoft Entra ID can be classified as either role-assignable or non-role-assignable. Additionally, any group can be enabled or not enabled for use with Microsoft Entra Privileged Identity Management (PIM) for Groups. These are independent properties of the group. Any Microsoft Entra security group and any Microsoft 365 group (except dynamic groups and groups synchronized from on-premises environment) can be enabled in PIM for Groups. The group doesn't have to be role-assignable group to be enabled in PIM for Groups.

upvoted 2 times

 **spatrick** 9 months ago

Groups in Microsoft Entra ID can be classified as either role-assignable or non-role-assignable. Additionally, any group can be enabled or not enabled for use with Microsoft Entra Privileged Identity Management (PIM) for Groups. These are independent properties of the group. Any Microsoft Entra security group and any Microsoft 365 group (except dynamic groups and groups synchronized from on-premises environment) can be enabled in PIM for Groups. The group doesn't have to be role-assignable group to be enabled in PIM for Groups.

upvoted 1 times

## HOTSPOT

-

You have a Microsoft Entra tenant that contains the users shown in the following table.

| Name  | Member of      |
|-------|----------------|
| User1 | Group1         |
| User2 | Group2         |
| User3 | Group1, Group2 |

You have a user risk policy that has the following settings:

- Assignments:
  - o Include: Group1
  - o Exclude: Group2
- Sign-in risk: Medium and above
- Access controls:
  - o Grant access: Require password change

When the users attempt to sign in, user risk levels are detected as shown in the following table.

| User  | Risk level |
|-------|------------|
| User1 | High       |
| User2 | Medium     |
| User3 | High       |

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

NOTE: Each correct selection is worth one point.

**Answer Area**

| Statements                                       | Yes                   | No                    |
|--------------------------------------------------|-----------------------|-----------------------|
| User1 must change their password during sign in. | <input type="radio"/> | <input type="radio"/> |
| User2 must change their password during sign in. | <input type="radio"/> | <input type="radio"/> |
| User3 must change their password during sign in. | <input type="radio"/> | <input type="radio"/> |

**Answer Area**

Suggested Answer:

| Statements                                       | Yes                              | No                               |
|--------------------------------------------------|----------------------------------|----------------------------------|
| User1 must change their password during sign in. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 must change their password during sign in. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User3 must change their password during sign in. | <input type="radio"/>            | <input checked="" type="radio"/> |

 **spatrick**  1 year, 3 months ago

For a CA they say:

Remember, the exclusion will take precedence. So if you select to include a user then exclude the user, the user will be excluded from the policy.  
upvoted 15 times

 **Fijii**  4 months ago

Not sure about User1 ?

User2 and User3 are clearly excluded from the policy and so are not required to change password.

User1 however has a HIGH user risk, but the policy is about sign-in, I think it is not supposed to trigger ?

I would say NNN

upvoted 1 times

  **YesPlease** 4 months ago

Yes) User1 is part of Group1 and has HIGH sign-in risk

No) User2 is excluded from risk policy because they are part of Group2

No) User3 is part of Group1 and they are HIGH risk, but they are also part of Group2 and are excluded from the risk policy. This EXCLUDE is important to understand. EXCLUDE takes precedence for any policy, just like when you want to exclude your ADMIN accounts so that you don't get locked out of a very restrictive rule/policy.

upvoted 2 times

  **Frank9020** 5 months ago

User1 must change their password? ✓ Yes

User2 must change their password? ✗ No

User3 must change their password? ✗ No

Since User3 is in both groups, exclusion takes priority, meaning User3 is excluded from the policy and does not have to change the password.

upvoted 2 times

  **penatuna** 8 months ago

When organizations both include and exclude a user or group, the user or group is excluded from the policy. The exclude action overrides the include action in policy. Exclusions are commonly used for emergency access or break-glass accounts.

User1 must change his password, cause Group1 is included in risk policy and his risk level is High.

User2 does not need to change his password, cause Group2 is excluded from risk policy.

User3 would not be required to change their password during sign-in. Here's why:

Inclusion and Exclusion: User3 is a member of both Group1 and Group2. Since Group2 is excluded from the policy, the policy does not apply to User3.

Sign-in Risk Level: Even though User3's sign-in risk level is High, the exclusion from Group2 takes precedence.

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-users-groups#exclude-users>

upvoted 4 times

  **76af099** 8 months ago

What is the precedence of Conditional Access policy?

Understanding Policy Precedence

When you have several policies enabled, the policy precedence is the following: A policy set to deny access is first priority. A policy set to allow access with MFA is second priority. A policy set to allow access without MFA is third priority.

YNY

upvoted 2 times

  **a6792d4** 1 year, 1 month ago

i' m not sure for user 3

upvoted 2 times

You have an Azure subscription that contains a resource group named RG1 and four users named User1, User2, User3, and User4.

You plan to assign the users the following roles for RG1:

- User1: Reader
- User2: Contributor
- User3: Storage Blob Data Reader
- User4: Virtual Machine Contributor

You are evaluating the use of attribute-based access control (ABAC).

Which user's role will support the use of ABAC?

- A. User1
- B. User2
- C. User3
- D. User4

**Suggested Answer: C**

Community vote distribution

C (100%)

 **YesPlease** 4 months ago


**Selected Answer: C**

Answer C) User3 (Storage Blob Data Reader) supports ABAC

Currently, conditions can be added to built-in or custom role assignments that have blob storage or queue storage data actions. These include the following built-in roles:

Storage Blob Data Contributor  
Storage Blob Data Owner  
Storage Blob Data Reader  
Storage Queue Data Contributor  
Storage Queue Data Message Processor  
Storage Queue Data Message Sender  
Storage Queue Data Reader

<https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-format#actions>  
upvoted 1 times

 **Labelfree** 7 months, 2 weeks ago

**Selected Answer: C**

C - Only User3: Storage Blob Data Reader supports ABAC.  
upvoted 1 times

 **penatuna** 1 year ago

**Selected Answer: C**

Within the roles in the question, only User3: Storage Blob Data Reader supports the use of ABAC.

You can test this yourself by adding role assignment in Azure. The Conditions tab is greyed out with all the other roles in the question. If you choose Storage Blob Data Reader, you can fill out the conditions.  
upvoted 3 times

 **RemmyT** 1 year ago



User3 : Storage Blob Data Reader

Example Azure role assignment conditions for Blob Storage

Azure attribute-based access control (Azure ABAC) is generally available (GA) for controlling access to Azure Blob Storage, Azure Data Lake Storage Gen2, and Azure Queues using request, resource, environment, and principal attributes in both the standard and premium storage account performance tiers.

<https://learn.microsoft.com/en-us/azure/storage/blobs/storage-auth-abac-examples?tabs=portal-visual-editor>

upvoted 2 times

🗲️ 👤 **klayytech** 1 year, 2 months ago

**Selected Answer: C**

Attribute-based access control (ABAC) grants access based on attributes of users, resources, and the environment.

- User roles (User1, User2, User3, User4) are a simpler form of access control.

Out of the options, only Storage Blob Data Reader and Virtual Machine Contributor roles are specific to resource types (Storage Blob and Virtual Machine). These roles suggest ABAC might be used for finer-grained control.

So, the answer is either C or D.

While both Storage Blob Data Reader and Virtual Machine Contributor roles might be used with ABAC, it's more likely for data access.

Therefore, the most likely user to benefit from ABAC is User3: Storage Blob Data Reader.

So the answer is: C. User3

upvoted 4 times

🗲️ 👤 **RASUK** 1 year, 3 months ago

C

<https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview>

upvoted 2 times

🗲️ 👤 **spatrick** 1 year, 3 months ago

Currently, conditions can be added to built-in or custom role assignments that have blob storage or queue storage data actions. Conditions are added at the same scope as the role assignment. Just like role assignments, you must have Microsoft.Authorization/roleAssignments/write permissions to add a condition.

upvoted 1 times

You have an Azure subscription. The subscription contains a virtual machine named VM1 that runs Linux.

You need to configure enhanced security for VM1. The solution must meet the following requirements:

- Ensure that users can sign in to VM1 by using their Microsoft Entra credentials.
- Ensure that users authenticate by using multi-factor out-of-band.
- Prevent users from signing in to VM1 by using passwords.

Which two authentication methods can you include in the solution? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. the Microsoft Authenticator app
- B. FIDO2 security keys
- C. Temporary Access Pass
- D. SMS
- E. Windows Hello for Business

**Suggested Answer:** BC

Community vote distribution

AB (100%)

  **59e8fdb** 4 months ago

**Selected Answer:** AB

A+B for sure!



upvoted 1 times

  **TRN80** 5 months, 3 weeks ago

**Selected Answer:** AB

Matt19 is correct the answer should be A+B



upvoted 2 times

  **Matt19** 6 months, 1 week ago

**Selected Answer:** AB

A&B - MS Authenticator app allows passwords sign-ins and FIDO2 is for sure correct.

upvoted 3 times

  **Matt19** 6 months, 1 week ago

Passwordless\*

upvoted 2 times

You have a Microsoft 365 E5 subscription.

You create an access review named Review1. Review1 requires that every six months, Microsoft 365 group owners review guest user access to their groups.

You need to ensure that if the group owners fail to review the membership of Review1, guest users are removed automatically.

Which settings should you configure for Review1?

- A. Scheduling
- B. When completed
- C. General
- D. Reviewers

**Correct Answer:** B

  **59e8fdb** 4 months ago

**Selected Answer:** B

Upon completion/When completed is correct  
upvoted 1 times

  **Shingie** 4 months, 2 weeks ago

**Selected Answer:** B

Correct Answer: B. When completed

In Microsoft Entra ID (Azure AD) Access Reviews, the "When completed" setting defines what happens if reviewers do not take action before the access review period ends.

Since you want to automatically remove guest users if group owners fail to review, you must configure the "When completed" setting to "Remove access".

Why Not the Other Options?

A. Scheduling – Incorrect

The scheduling settings determine how often the review occurs (e.g., every six months), but do not control what happens if a review is not completed.

C. General – Incorrect

The General settings include details like the name and description of the access review but do not impact automatic removal of guests.

D. Reviewers – Incorrect

The Reviewers setting defines who conducts the review (in this case, group owners). However, it does not control what happens if they fail to review.  
upvoted 3 times

## SIMULATION

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 Password: =1122334455667788

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 99999999

-

You need to enforce multi-factor authentication (MFA) for users in the Executives group when they connect to Microsoft Office 365 apps. The solution must affect only the users in the Executives group.

To complete this task, sign in to the appropriate admin center.

**Correct Answer:**

enforce multi-factor authentication connect Microsoft Office 365 apps

Set up multifactor authentication for Microsoft 365

Use Conditional Access policies

If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.

Part 1:

First, create a Conditional Access policy and assign your test group of users as follows:


Step 1: Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.


Step 2: Browse to Protection > Conditional Access, select + New policy, and then select Create new policy.


[Home](#) > [Security | Conditional Access](#) >

## Conditional Access | Overview ...

Microsoft Entra ID

 + Create new policy + Create new policy from templates Refresh Got feedback?

 Overview

 Policies

Getting started **Overview** Coverage Monitoring (Preview) Tutorials

Step 3: Enter a name for the policy, such as MFA Pilot.

Step 4: Under Assignments, select the current value under Users or workload identities.

[Home](#) > [Conditional Access](#) >

**New** ...  
Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

Assignments

Users or workload identities ⓘ  
0 users or workload identities selected

Cloud apps or actions ⓘ  
No cloud apps, actions, or authentication contexts selected

Step 5: Under What does this policy apply to?, verify that Users and groups is selected.

Step 6: Under Include, choose Select users and groups, and then select Users and groups.

[Home](#) > [Contoso](#) > [Security](#) > [Conditional Access](#) >

**New** ...  
Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

What does this policy apply to?

**Include** Exclude

Users or workload identities ⓘ  
Specific users included

\*Select users and groups\* must be configured

Cloud apps or actions ⓘ  
No cloud apps, actions, or authentication contexts selected

Conditions ⓘ  
0 conditions selected

Access controls

☐ None

☐ All users

☒ Select users and groups

☐ All guest and external users ⓘ

☐ Directory roles ⓘ

☒ Users and groups

Select  
0 users and groups selected  
\*Select at least one user or group

Since no one is assigned yet, the list of users and groups (shown in the next step) opens automatically.

Step 7: Browse for and select your Microsoft Entra group, such as MFA-Test-Group, then choose Select. [Select the Executives group]

**Select** ×  
Users and groups

MFA-Test-Group

Control access based on who the policy will apply to, such as users and groups, workload

identities, directory roles, or external guests.  
[Learn more](#)

What does this policy apply to?

Users and groups

Include Exclude

- ☐ None
- ☐ All users
- ☒ Select users and groups

☐ All guest and external users ⓘ

☐ Directory roles ⓘ

☒ Users and groups

Select

0 users and groups selected

✖ Select at least one user or group

MF Selected

Selected items

MF MFA-Test-Group

Remove

Select

We've selected the group to apply the policy to. In the next section, we configure the conditions under which to apply the policy.

## Part 2: Configure the conditions for multifactor authentication

Now that the Conditional Access policy is created and a test group of users is assigned, define the cloud apps or actions that trigger the policy.

### Configure which apps require multifactor authentication

Step 1: Select the current value under Cloud apps or actions, and then under Select what this policy applies to, verify that Cloud apps is selected.

Step 2: Under Include, choose Select apps.

Since no apps are yet selected, the list of apps (shown in the next step) opens automatically.

Step 3: Browse the list of available sign-in events that can be used. [Select Microsoft Office 365 apps]

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps

Include Exclude

- ☐ None
- ☐ All cloud apps
- ☒ Select apps

Select

None

✖ Select at least one app.

Select

Cloud apps

Search

- ☐ Office 365 ⓘ
- ☐ AC Azure Credential Configurati  
ea890292-c3c8-4433-b5ea-b09d06...
- ☐ D3 Dynamics 365 Business Cent  
996de73d-b36c-4153-8607-a9fd3c...
- ☒ MA Microsoft Azure Managemer  
7974846-ba00-4fd7-ba43-dac1f8f...
- ☐ Microsoft Cloud App Security  
05a55629-4c1b-48c1-a78b-804c4a...
- ☐ MI Microsoft Information Protec  
870c4f2e-85b6-4d43-bdda-6ed9a5...

Selected items

MA Microsoft Azure I  
7974846-ba00-4fd...

Remove

Select

### Reference:

<https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-azure-mfa>

<https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication>

Currently there are no comments in this discussion, be the first to comment!

## SIMULATION

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 Password: =1122334455667788

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 99999999

-

You need to ensure that users in the sg-Legal group must reauthenticate every 12 hours when they access any cloud apps managed by the tenant.

To complete this task, sign in to the appropriate admin center.



## Correct Answer:

Microsoft Entra, Microsoft Entra ID, Conditional Access, Configure adaptive session lifetime policies

Sign-in frequency control

Step 1: Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.

Step 2: Browse to Protection > Conditional Access.

Step 3: Select Create new policy.

Step 4: Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

Step 5: Choose all required conditions for customer's environment, including the target cloud apps.

Step 6: Under Access controls > Session.

Step 6a: Select Sign-in frequency.

Step 6b: Choose Periodic reauthentication and enter a value of hours or days [Specify 12 hours: 12 + Hours as Unit] or select Every time.

Home > Contoso | Security > Security | Conditional Access > Conditional Access | Policies >

## New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more](#)

Name \*

Sign-in frequency ✓

### Assignments

Users or workload identities ⓘ

[Specific users included](#)

Cloud apps or actions ⓘ

[1 app included](#)

Conditions ⓘ

[0 conditions selected](#)

Access controls

Grant ⓘ

[0 controls selected](#)

Session ⓘ

[0 controls selected](#)

Enable policy

Report-only On Off

Create

Step 6c: For Assignments, User or workload identities, specify the sg-Legal group

Step 6d: For Cloud apps or actions, specify any/all cloud apps.

Step 7: Click Create, and save your policy.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-session-lifetime>

## Session

Control access based on session controls to enable limited experiences within specific cloud applications.  
[Learn more](#)

☐ Use app enforced restrictions ⓘ

☐ Use Conditional Access App Control ⓘ

☒ Sign-in frequency ⓘ

☒ Periodic reauthentication

0

Select units ▼

☐ Every time

⚠ Some of the applications currently selected are not compatible with the "Sign-in frequency" option of "Every time"

☐ Persistent browser session ⓘ

☐ Customize continuous access evaluation ⓘ

☐ Disable resilience defaults ⓘ

Select

👤 Giuseppe\_Geraci 1 month, 1 week ago

Protection – Conditional access + new policy

User = sg-legal group

Target = allcloudapps

Session = Sign-Frequency = 12h

upvoted 2 times

## SIMULATION

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 Password: =1122334455667788

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 99999999

-

You need to configure Microsoft Entra Identity Protection to meet the following requirements:

- Require multi-factor authentication (MFA) for any sign-ins at the high risk level.
- Apply the configuration to all users except for Mod Administrator.

To complete this task, sign in to the appropriate admin center.

#### Correct Answer:

Microsoft Entra Identity Protection multi-factor authentication (MFA) for any sign-ins at the high risk level

Enable sign-in risk policy for MFA

Most users have a normal behavior that can be tracked. When they fall outside of this norm, it could be risky to allow them to successfully sign in. Instead, you might want to block that user, or ask them to perform a multifactor authentication. If the user successfully completes the MFA challenge, you can consider it a valid sign-in attempt and grant access to the application or service.

To enable this policy, complete the following steps:

Step 1: Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.

Step 2: Browse to Protection > Conditional Access.

Step 3: Select New policy.

Step 4: Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

Step 5: Under Assignments, select Users or workload identities

Step 5a: Under Include, select All users.

Step 5b: Under Exclude, select Users and groups and choose your organization's emergency access or break-glass accounts.  
[Select Mod Administrator]

Step 6: Under Cloud apps or actions > Include, select All cloud apps.

Step 7: Under Conditions > Sign-in risk, set Configure to Yes. Under Select the sign-in risk level this policy will apply to.

- a. Select High.
- b. Select Done.

Step 8: Under Access controls > Grant.

- a. Select Grant access, Require multifactor authentication.
- b. Select Select.

Step 9: Under Session. [Skip, do not need to specify sign-in frequency]

Step 10: Confirm your settings and set Enable policy to On.

Step 11: Select Create to create to enable your policy.

Note: Use risk detections for user sign-ins to trigger Microsoft Entra multifactor authentication or password changes

To protect your users, you can configure risk-based Microsoft Entra Conditional Access policies that automatically respond to risky behaviors. These policies can automatically block a sign-in attempt or require extra action, such as require a secure password change or prompting for Microsoft Entra multifactor authentication. These policies work with existing Microsoft Entra Conditional Access policies as an extra layer of protection for your organization. Users might never trigger a risky behavior in one of these policies, but your organization is protected if an attempt to compromise your security is made.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-risk-based-sspr-mfa>

 **Giuseppe\_Geraci** 1 month, 1 week ago

Entra > Identity Protection > Sign-in risk policy

Assignments : Include All Users, Exclude Mod Administrator

Sign-in risk : High - Access : allow access, require multifactor authentication

upvoted 1 times

 **Fijii** 4 months ago

Entra > Identity > Protection > Identity Protection > Sign-in risk policy

- Create a new policy

- Assignments : Include All Users, Exclude Mod Administrator

- Sign-in risk : High

- Access : allow access, require multifactor authentication

upvoted 1 times

 **Oskarma** 4 months, 3 weeks ago

I think is easier (and possible) to use the sign-in policy in Identity Protection.

I saw it in my tenant.

upvoted 1 times